

Utilizar vRealize Log Insight

24 de mayo de 2022

vRealize Log Insight 8.0

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

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

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

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

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

Contenido

Acerca de Utilizar vRealize Log Insight	6
1 Información general de las funciones de vRealize Log Insight	7
2 Descripción general de la interfaz de usuario web de vRealize Log Insight	10
3 Buscar y filtrar eventos de registro	11
Agrupación de tipos de eventos	12
Información en eventos de registro	13
Filtrar eventos del registro por intervalo de tiempo	14
Buscar eventos del registro que contengan una palabra clave completa	15
Buscar eventos de registro por operaciones de campo	15
Excluir la extracción de campos de paquete de contenido de la búsqueda de eventos de registro	17
Buscar eventos que se produjeron antes, después o cercanos a un evento	18
Ver evento en contexto	19
Analizar tendencias de eventos	19
Borrar todas las reglas de filtrado	20
Ejemplos de consultas de búsqueda	20
Ejemplos de expresiones regulares	22
4 Uso del gráfico Análisis interactivo para analizar registros	26
Tipos de gráficos	26
Gráficos de múltiples funciones	27
Función de agregación	27
Trabajar con gráficos	28
Cambiar el tipo del gráfico de análisis interactivo	29
5 Extracción dinámica de campos	31
Extraer campos con extracción en un clic	31
Modificar un campo extraído	33
Duplicar un campo extraído	33
Eliminar un campo extraído	35
6 Administrar consultas de búsqueda	36
Guarde una consulta en vRealize Log Insight	36
Cambie el nombre de una consulta en vRealize Log Insight	37
Cargar una consulta en vRealize Log Insight	37

- Eliminar una consulta de vRealize Log Insight 38
- Comparta la consulta actual 38
- Exportar la consulta actual 39
- Tomar una instantánea de una consulta 40
- Solución de problemas de los resultados de la consulta de vRealize Log Insight 40

7 Trabajar con paneles de control 42

- Administrar paneles de control 43
- Añadir un widget de lista de consultas al panel 45
- Añadir una consulta a un widget de lista de consultas en un panel 46
- Añadir un widget de tabla de campos a un panel de control 47
- Agregar un widget Tipos de eventos al panel de control 47
- Agregar un widget Tendencias de eventos al panel de control 48
- Filtrar usando valores de campo de gráficos 48

8 Trabajar con paquetes de contenido 50

- Utilizar paquetes de contenido 50
 - Instalar un paquete de contenido del Catálogo de paquetes de contenido 51
 - Actualizar un paquete de contenido instalado a partir del mercado del paquete de contenido 52
 - Importar un paquete de contenido 52
 - Exportar un paquete de contenido 55
 - Visualización de detalles de los elementos del paquete de contenido 56
 - Desinstalar un paquete de contenido 57
 - Extraer campos de paquete de contenido seleccionados para las consultas 57
- Crear paquetes de contenidos 58
 - Términos de paquetes de contenido 58
 - Consultas 60
 - Prácticas recomendadas de paneles de control 67
 - Errores de importación de paquetes de contenidos 69
 - Requisitos para publicar paquetes de contenidos 70
 - Enviar paquete de contenido 74
- Alias de almacén de datos a identificador de dispositivo para almacenes de datos de vSphere 75

9 Consultas de alerta en vRealize Log Insight 82

- Definir una consulta de alerta 84
- Agregar una consulta de alerta para enviar notificaciones por correo electrónico 86
- Acerca de usar webhooks para enviar alertas a productos de terceros 87
 - Agregar una consulta de alerta para enviar notificaciones de webhook 87
 - Acerca de Escribir shims de traducción para alertas de vRealize Log Insight 88
- Agregar una consulta de alerta para enviar notificaciones a vRealize Operations Manager 91

Ver consultas de alerta	94
Modificar consultas de alerta	96
Habilitar consultas de alerta	98
Eliminar consultas de alerta	100

Acerca de Utilizar vRealize Log Insight

Los temas sobre *Utilizar vRealize Log Insight* proporcionan información acerca de los procedimientos para el filtrado y la búsqueda de mensajes de registro, el análisis y la visualización de los resultados de búsqueda, el trabajo con consultas de alertas y la extracción dinámica de campos desde mensajes de registro a partir de consultas personalizadas.

Esta información está destinada a quienes desean utilizar vRealize Log Insight.

Información general de las funciones de vRealize Log Insight

1

vRealize Log Insight proporciona agregación e indexación de registros escalable para vCloud Suite, incluidas todas las ediciones de vSphere, con capacidad de análisis y búsqueda en tiempo casi real.

vRealize Log Insight recopila, importa y analiza registros para proporcionar respuestas a problemas relacionados con los sistemas, servicios y aplicaciones y obtener perspectivas importantes.

Consumo de alto rendimiento

vRealize Log Insight puede procesar cualquier tipo de datos generados por equipos o por registros. Admite tasas de rendimiento elevadas y una baja latencia, además de aceptar datos a través de syslog y la API de consumo.

Escalabilidad

vRealize Log Insight puede escalar horizontalmente utilizando varias instancias del dispositivo virtual, lo que permite el escalado lineal del rendimiento de consumo, aumenta el rendimiento de la consulta y permite la alta disponibilidad de consumo. En el modo de clúster, vRealize Log Insight proporciona los nodos principal y de trabajador. Los nodos principal y de trabajador son responsables de un subconjunto de datos. Los nodos principal y de consulta pueden consultar todos los subconjuntos de datos y añadir los resultados.

Búsqueda en tiempo casi real

Los datos consumidos por vRealize Log Insight están disponibles para la búsqueda en cuestión de segundos. Además, los datos históricos pueden buscarse desde la misma interfaz con la misma baja latencia.

vRealize Log Insight admite consultas completas de palabra clave. Las palabras clave son cualquier combinación de caracteres alfanuméricos, guiones o guiones bajos. Además de las consultas de palabra clave completa, vRealize Log Insight admite consultas con globs (por ejemplo, `erro? o vm*`) y filtros basados en campos (por ejemplo, el nombre del host NO coincide con prueba*, la IP incluye "10.64"). Además, los campos de mensajes de registro que contienen valores numéricos pueden utilizarse para definir filtros de selección (por ejemplo, `CPU>80, 10<threads<100`, y así sucesivamente).

Los resultados de la búsqueda se presentan como eventos individuales. Cada evento proviene de un único origen, pero los resultados de la búsqueda pueden provenir de varios orígenes. Puede utilizar vRealize Log Insight para correlacionar los datos en una o varias dimensiones (por ejemplo, los identificadores de hora y solicitud) proporcionando una vista coherente en toda la agrupación. De esta manera, el análisis de la causa de raíz se facilita mucho.

Agentes de Linux y Windows

vRealize Log Insight incluye agentes que recopilan eventos y archivos en los equipos Windows y Linux.

Agrupación inteligente

vRealize Log Insight utiliza una nueva tecnología de aprendizaje de la máquina. La agrupación inteligente escanea los datos no estructurados entrantes y agrupa los mensajes por tipo de problema para darle la capacidad de entender rápidamente los problemas que pueden abarcar sus entornos físicos, virtuales y de nube híbridos.

Agregación

Los campos que se extraen de los datos del registro pueden utilizarse para agregación. Esta funcionalidad es similar a la funcionalidad que proporcionan las consultas GROUP BY en una base de datos de relaciones o en tablas de pivote en Microsoft Excel. La diferencia es que no hay necesidad de extraer, transformar y cargar (ETL) procesos y escalas de vRealize Log Insight a cualquier tamaño de datos.

Puede generar vistas agregadas de datos e identificar errores o eventos específicos sin acceder a varios sistemas y aplicaciones. Por ejemplo, al visualizar una métrica importante del sistema, por ejemplo, la cantidad de errores por minuto, puede obtener información detallada de un intervalo específico de eventos y analizar los errores que se produjeron en el entorno.

Extracción de campos en tiempo de ejecución

Los datos del registro sin procesar no son siempre fáciles de entender y es posible que necesite procesar algunos para identificar los campos que son importantes para la búsqueda y la agregación. vRealize Log Insight proporciona extracción de campos en tiempo de ejecución para abordar este problema. Puede extraer dinámicamente cualquier campo de los datos proporcionando una expresión regular. Los campos extraídos se pueden utilizar para la selección, proyección y agregación, en forma similar a la manera en que se utilizan los campos que se extraen en el intervalo de análisis.

Nota Un nombre de campo extraído puede contener caracteres diferentes. Sin embargo, el nombre de campo de un evento consumido debe comenzar solo con una letra o un carácter de subrayado y contener solo letras, dígitos o el carácter de subrayado.

Paneles de control

Puede crear paneles de control de métrica útil que desee supervisar de cerca. Cualquier consulta puede transformarse en un widget del panel de control y resumir cualquier intervalo en el tiempo. Puede elegir el rendimiento de su sistema de los últimos cinco minutos, hora o día. Puede visualizar el desglose de los errores por hora y observar las tendencias en los eventos del registro.

Consideraciones de seguridad

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

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

Descripción general de la interfaz de usuario web de vRealize Log Insight

2

La funcionalidad a la que puede acceder depende de la cuenta de usuario que utiliza para iniciar sesión en la interfaz de usuario web de vRealize Log Insight.

Pestaña Paneles de control

La pestaña **Paneles de control** contiene los paneles de control personalizados y los paneles de control del paquete de contenido. En la pestaña **Paneles de control** puede visualizar los gráficos de los eventos de registro de su entorno o bien crear grupos personalizados de widgets para acceder a la información que más le interesa.

La pestaña Análisis interactivo

En la pestaña **Análisis interactivo** puede buscar y filtrar los eventos del registro y crear consultas para extraer eventos basados en la marca de tiempo, el texto, el origen y los campos de los eventos del registro. vRealize Log Insight presenta los gráficos de los resultados de la consulta. Puede guardar estos gráficos para buscarlos más adelante en la pestaña **Paneles de control**.

Paquetes de contenido

Los paquetes de contenido incluyen paneles, campos extraídos, consultas almacenadas y alertas relacionados con un producto específico o grupos de registros. Puede acceder a los paquetes de contenido en el menú desplegable de la esquina superior derecha de la interfaz de usuario web de vRealize Log Insight.

Los usuarios de vRealize Log Insight pueden importar o crear los paquetes de contenido. Consulte [Utilizar paquetes de contenido](#).

La interfaz de usuario de Administración

Los administradores de vRealize Log Insight pueden administrar las cuentas de usuario, configurar la ubicación del almacenamiento y el archivo, configurar un servidor SMTP saliente para las notificaciones de correo electrónico y modificar otros parámetros. El formato URL de la UI de Administración es `https://host-log_insight/admin/`, donde *host-log_insight* es la dirección IP o el nombre de host del dispositivo virtual de vRealize Log Insight.

Buscar y filtrar eventos de registro

3

Puede buscar y filtrar los eventos de registro en la pestaña **Análisis interactivo**.

Para buscar solo los eventos que contengan las palabras clave especificadas, introduzca las frases, globos o palabras clave completas en el cuadro de texto de búsqueda y haga clic en **Buscar**.

Puede especificar el intervalo en cualquiera de las páginas **Paneles de control** o **Análisis interactivo** de la interfaz de usuario web. Los intervalos son inclusivos al aplicar el filtro.

Puede buscar eventos de registro que coincidan con determinados valores de campos específicos. El uso de texto entre comillas en el campo de búsqueda principal permite la correspondencia de frases exactas. Introducir un espacio en el campo de búsqueda principal es un operador AND lógico. La búsqueda solo usa tokens completos. Por ejemplo, la búsqueda de "err" no encuentra "error" como una coincidencia.

Nota El nombre de campo de un evento consumido debe comenzar solo con una letra o un carácter de subrayado y contener solo letras, dígitos o el carácter de subrayado.

Puede introducir los criterios, o filtros, de búsqueda de campos, usando los menús desplegables y el cuadro de texto que se encuentra arriba de la lista de eventos de registro.

En un filtro de una sola línea, puede usar valores separados por comas para listar filtros OR. Por ejemplo, seleccione **hostname contains** y escriba **127.0.0.1, 127.0.0.2**. La búsqueda devuelve eventos con el nombre de host 127.0.0.1 o 127.0.0.2.

Nota El filtro **text contains** trata cada valor separado por comas como una palabra clave completa.

Las consultas con campos en los que se usan nombres de sintaxis del lenguaje de consulta interno (por ejemplo, `from` o `in`) no se pueden procesar y no deben utilizarse.

Para combinar filtros de varios campos, cree una línea de filtro para cada campo. Puede cambiar el operador que se aplica a filtros de varias líneas.

- Para aplicar el operador AND, seleccione **all**.
- para aplicar el operador OR, seleccione **any**.

Nota Independientemente del valor cambiado, el operador para los valores separados por comas en una línea de filtro sencillo siempre es OR.

Puede usar globs en los términos de búsqueda. Por ejemplo, **vm*** o **vmw?re**.

- Para 0 o mas caracteres, use *****.
- Para un carácter, use **?**.

Nota No se pueden usar globs como el primer carácter de un término de búsqueda. Por ejemplo, puede usar 192.168.0.*, pero no puede usar *.168.0.0 en sus consultas de filtrado.

Este capítulo incluye los siguientes temas:

- [Agrupación de tipos de eventos](#)
- [Información en eventos de registro](#)
- [Filtrar eventos del registro por intervalo de tiempo](#)
- [Buscar eventos del registro que contengan una palabra clave completa](#)
- [Buscar eventos de registro por operaciones de campo](#)
- [Excluir la extracción de campos de paquete de contenido de la búsqueda de eventos de registro](#)
- [Buscar eventos que se produjeron antes, después o cercanos a un evento](#)
- [Ver evento en contexto](#)
- [Analizar tendencias de eventos](#)
- [Borrar todas las reglas de filtrado](#)
- [Ejemplos de consultas de búsqueda](#)
- [Ejemplos de expresiones regulares](#)

Agrupación de tipos de eventos

vRealize Log Insight resume un gran número de eventos individuales en un número menor de tipos de eventos amplios. vRealize Log Insight utiliza el aprendizaje automático para agrupar eventos similares, donde cada grupo muestra el número aproximado de eventos en el grupo. La agrupación de eventos ayuda a identificar los eventos más y menos comunicativos; ambos son fundamentales para la solución de problemas.

La pestaña **Tipos de eventos** de la página Análisis interactivo, bajo la barra de búsqueda, proporciona una vista agregada de los eventos para el intervalo de tiempo especificado de la consulta. Se selecciona un evento en un grupo como evento representativo. Puede hacer clic en el vínculo **Expandir** de cada evento representativo para ver los eventos en el grupo.

Como resultado de la agrupación de eventos, se asigna un tipo de evento a cada evento. Se crea un campo *event_type* apropiado, que posteriormente se puede utilizar en consultas regulares.

vRealize Log Insight no documenta el mecanismo exacto para agrupar eventos. Intenta detectar automáticamente grupos de eventos similares en función del número de partes comunes que tienen los eventos. Por ejemplo, supongamos que tenemos los siguientes eventos:

- [2019-05-20 06:41:24.291+0000] ["SearchWorker-thread-12999"/10.113.164.150 INFO] [com.company.product.analytics.distributed.LogSearchWorkerService] [Worker fully completed query (token=5f6e5e1faf93e4ce) in 11 msec]
- [2019-05-20 06:41:24.284+0000] ["SearchWorker-thread-11961"/10.113.164.167 INFO] [com.company.product.analytics.distributed.SearchWorkerService] [Worker fully completed query (token=3b247b2ba6057c47) in 24 msec]

Estos eventos tienen ocho partes comunes: marca de tiempo, nombre de subprocesso, IP de host, nivel de registro, nombre de clase, texto de mensaje, número de token y duración.

Ahora, vamos a considerar los siguientes eventos:

- [2019-05-20 06:41:24.291+0000] ["LogSearchWorker-thread-12999"/10.113.164.150 INFO] [com.vmware.loginsight.analytics.distributed.LogSearchWorkerService] [Worker finished search (wait=59500 token=5f6e5e1faf93e4ce) in 12 msec]
- [2019-05-20 06:41:20.136+0000] ["AliasStudentStudyPool-thread-1"/192.168.110.24 INFO] [com.vmware.loginsight.analytics.alias.AliasStudent] [looking for alias due to rule DatastoreFromVmFileSystem]

Estos eventos solo tienen tres partes comunes: marca de tiempo, IP de host y nivel de registro.

Además de agrupar los eventos de forma conjunta, vRealize Log Insight identifica campos útiles en cada evento del grupo, conocidos como campos inteligentes. Cada campo inteligente aparece dentro del evento representativo como un hipervínculo con un icono de menú desplegable junto a él. Puede hacer clic en el icono para ver un histograma de los valores del campo o para definir un campo extraído en función del campo inteligente.

Información en eventos de registro

vRealize Log Insight recopila y analiza todos los tipos de datos de registro generados por una máquina, incluidos los registros de aplicaciones, los rastreos de redes, los archivos de configuración, los mensajes, los datos de rendimiento y los volcados de estados del sistema.

Puede conectar vRealize Log Insight a cualquier elemento de su entorno (sistemas operativos, aplicaciones, almacenamiento, firewalls, dispositivos de red u otros elementos) para obtener visibilidad de toda la empresa con el análisis de registros.

Cuando vRealize Log Insight se ha configurado y está listo para recopilar registros, existen varias formas en las que se pueden recopilar datos de registro, entre ellas:

- vSphere Integration: vRealize Log Insight se puede integrar con vSphere para recopilar automáticamente eventos de un servidor vCenter Server y registros de hosts ESXi.

- Integración con vRealize Operations Manager: vRealize Log Insight puede integrarse con vRealize Operations Manager para permitir que diversas alertas envíen eventos de notificación en vRealize Operations Manager y correos electrónicos a los administradores.
- Agentes: vRealize Log Insight cuenta con agentes de recopilación disponibles para enviar registros de eventos y archivos de Linux o Windows a vRealize Log Insight
- Syslog: vRealize Log Insight puede recopilar datos de varios orígenes mediante syslog. Solamente configure el servidor vRealize Log Insight como su destino de syslog.
- CFAPI: los eventos se envían en su formato original a vRealize Log Insight mediante cfapi. Los eventos enviados por medio de cfapi no tienen que seguir las directrices de un evento de syslog y no se modifican para cumplir con los estándares de RFC de syslog.

Cada evento incluye la siguiente información.

Tipo	Descripción
Marca de tiempo	La hora en que sucedió el evento.
Origen	El punto en el que se originó el evento. Este puede ser el originador de mensajes de syslog, tal como un host ESXi, o un reenviador, tal como una agregación de syslog.
Texto	El texto sin procesar del evento.
Campos	Un par de nombre y valor extraído del evento. Los campos se entregan al servidor como campos estáticos solo cuando un agente utiliza el protocolo CFAPI.

Nota vRealize Log Insight no es responsable del contenido de los mensajes de registro de otros productos de VMware. Si tiene una pregunta sobre el contenido del registro, comuníquese con el equipo de productos que generó el mensaje de registro.

Filtrar eventos del registro por intervalo de tiempo

Puede filtrar eventos del registro para ver solo los eventos de un período determinado.

Puede especificar el intervalo en cualquiera de las páginas **Paneles de control** o **Análisis interactivo** de la interfaz de usuario web. Los intervalos son inclusivos al aplicar el filtro.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En el menú desplegable a la izquierda del botón **Buscar**, seleccione uno de los períodos predefinidos.

- 2 (opcional) Para establecer los puntos inicial y final del intervalo de tiempo, seleccione **Intervalo de tiempo personalizado**.

Buscar eventos del registro que contengan una palabra clave completa

Puede buscar eventos del registro que contengan una palabra clave completa. Las palabras clave contienen caracteres alfanuméricos, guion y guion bajo.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.
- 2 En el cuadro de texto de la búsqueda, escriba la palabra clave completa que desea buscar en los eventos del registro y haga clic en el botón **Buscar**.

Resultados

Los eventos del registro que contienen la palabra clave completa especificada se muestran en la lista.

La cadena que buscó se destaca en amarillo.

Pasos siguientes

Puede almacenar la consulta actual para cargarla posteriormente.

Buscar eventos de registro por operaciones de campo

Puede usar la lista de campos existentes para buscar eventos de registro con valores específicos para un campo.

Importante vRealize Log Insight conforma un índice de caracteres completos, alfanuméricos, guion y guion bajo.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.

2 Haga clic en **Añadir filtro**.

3 En la fila de filtro debajo del cuadro de texto de búsqueda, use el primer menú desplegable para seleccionar cualquier campo definido en vRealize Log Insight.

Por ejemplo, **hostname**.

La lista incluye todos los campos definidos disponibles estáticamente, en paquetes de contenido y en contenido personalizado. Los campos se clasifican por nombre, excepto por el campo **texto**. Dado que **texto** es un campo especial que hace referencia al texto del mensaje, **texto** aparece en la parte superior de la lista y está seleccionado de forma predeterminada.

Nota Los campos numéricos incluyen operadores adicionales de los que carecen los campos de cadena: **=**, **>**, **<**, **>=**, **<=**. Estos operadores realizan comparaciones numéricas y su uso genera resultados diferentes que al usar operadores de cadena. Por ejemplo, el filtro **response_time=02** coincidirá con un evento que incluya un campo **response_time** con un valor 2. El filtro **response_timecontains02** no tendrá la misma concordancia.

4 En la fila de filtro debajo del cuadro de texto de búsqueda, use el segundo menú desplegable para seleccionar la operación que se debe aplicar al campo seleccionado en el primer menú desplegable.

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

5 En el cuadro de texto a la derecha del menú desplegable de filtros, escriba el valor que desee usar como filtro.

Puede enumerar varios valores separados por comas. El operador entre estos valores es OR.

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

6 (opcional) Para añadir más filtros, haga clic en **Añadir filtro**.

Aparece un botón de alternancia por encima de las filas de filtro.

7 (opcional) Para múltiples filas de filtro, seleccione el operador entre los filtros.

Opción	Descripción
todo	Seleccionar para aplicar la operación AND entre filas de filtros
cualquiera	Seleccionar para aplicar la operación OR entre filas de filtros

De forma predeterminada, se selecciona **todo**.

8 Haga clic en el botón **Buscar**.

Ejemplo: Buscar un grupo de hosts que tengan una cadena común en el nombre

Suponga que tiene varios hosts con un host con el siguiente nombre: w1-stvc-205-prod3 y otro host denominado w1-stvc-206-prod5.

Para buscar todos los registros de ambos hosts, cree la siguiente consulta.

- 1 1. Deje vacío el cuadro de texto de la búsqueda.
- 2 Defina el filtro.
 - a Seleccione **hostname** (nombre del host) en el menú desplegable del campo.
 - b Seleccione **empieza con** en el menú desplegable del operador.
 - c Escriba **w1-stvc** en el cuadro de texto del valor.

Como opción, puede utilizar el operador **contains** pero entonces debe usar un glob en el valor de búsqueda. En este ejemplo, debe escribir **w1-stvc-*** en el cuadro de texto del valor.

- 3 Haga clic en el botón **Buscar**.

Pasos siguientes

Puede almacenar la consulta actual para cargarla posteriormente.

Excluir la extracción de campos de paquete de contenido de la búsqueda de eventos de registro

Puede excluir los campos de paquete de contenido de la extracción al buscar eventos de registro, para aumentar el rendimiento de la consulta.

Importante Solo se deben excluir los paquetes de contenido que no se deban extraer como parte de la búsqueda específica.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://log_insight-host`, donde `log_insight-host` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.
- 2 Haga clic en **Paquetes de contenido** para abrir el menú desplegable.
 - a Seleccione **Todos** para seleccionar todos los paquetes de contenido de la búsqueda de registros.
 - b Seleccione solo los paquetes de contenido que desea incluir en los resultados de la búsqueda de registros.

3 Haga clic en **Buscar**.

Nota Si el campo extraído participa en el filtro de consulta y su paquete de contenido se excluye de la búsqueda, el campo extraído se utiliza para crear los resultados de la consulta. Sin embargo, el campo extraído no aparece en los resultados de la búsqueda.

Resultados

Solo se extraen los campos de paquete de contenido seleccionados durante la búsqueda de eventos de registro.

Pasos siguientes

Puede guardar esta consulta de búsqueda para utilizarla en el futuro.

Buscar eventos que se produjeron antes, después o cercanos a un evento


Puede buscar la lista de eventos de registro que se produjeron antes, después o cerca de un evento de la lista.

Si desea más información acerca del estado de su entorno antes y después de un evento, puede verificar los eventos cercanos.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En la pestaña **Análisis interactivo**, ubique el evento en la lista.
- 2 A la izquierda de la fila de eventos, haga clic en  y seleccione **Establecer intervalo desde este evento**.
- 3 En el cuadro de diálogo Configurar intervalo de tiempo desde evento, use los menús desplegables para seleccionar el período y la dirección del intervalo de tiempo.
Puede seleccionar de una lista de períodos predefinidos de 1 segundo a 10 minutos.
- 4 Haga clic en **Establecer intervalo**.

Resultados

En la lista se muestran los eventos que rodean al evento seleccionado.

Nota Esta operación borra todos los parámetros de búsqueda y los filtros que ha especificado anteriormente.

Ver evento en contexto



Puede visualizar el contexto de un evento de registro y buscar los eventos de registro que llegaron antes y después del evento.

Si desea más información acerca del estado de su entorno antes y después de un evento, puede verificar los eventos cercanos.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En la pestaña **Análisis interactivo**, ubique el evento en la lista.
- 2 A la izquierda de la fila de eventos, haga clic en  y seleccione **Ver evento en contexto**.
- 3 (opcional) Desplácese hacia arriba o hacia abajo hasta el borde de la ventana para cargar más eventos.
- 4 (opcional) Haga clic en la marca de tiempo color lila para volver al mensaje resaltado.
- 5 (opcional) Para añadir filtros, haga clic en **Añadir filtro** en la parte superior o haga clic en un campo dentro del evento resaltado.
- 6 (opcional) Para agregar tipos de eventos específicos, señale un evento y haga clic en .

Analizar tendencias de eventos

Puede analizar eventos de registro para tendencias y anomalías.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.
- 2 Elabore y ejecute la consulta usando el cuadro de texto de búsqueda y aplicando los filtros.
- 3 En el cuadro de diálogo Configurar intervalo de tiempo desde evento, use los menús desplegables para seleccionar el período y la dirección del intervalo de tiempo.
- 4 Haga clic en la pestaña **Tendencias de eventos**.

vRealize Log Insight compara su consulta con el mismo período inmediatamente anterior y muestra los resultados.

Borrar todas las reglas de filtrado

Puede borrar los resultados de filtrado y de búsqueda para ver la lista de todos los eventos de registro.

Después de llevar a cabo una búsqueda en la lista de eventos, los resultados de la búsqueda permanecerán en la pantalla hasta que borre todas las consultas.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En la pestaña **Análisis interactivo**, elimine todos los filtros.
- 2 Si aparece texto en el cuadro de texto de búsqueda, bórralo.
- 3 Haga clic en el botón **Buscar**.

Ejemplos de consultas de búsqueda

Puede usar estos ejemplos al crear sus consultas en la pestaña **Análisis interactivo** de vRealize Log Insight.

Ejemplo: Consultar todos los eventos notificados por el proceso ESX/ESXi hostd ayer entre las 9 y las 10 a.m.

Importante vRealize Log Insight conforma un índice de caracteres completos, alfanuméricos, guion y guion bajo.

Para consultar todos los eventos notificados por el proceso ESX/ESXi hostd:

- 1 En el cuadro de texto de búsqueda, escriba **heartbeat***.
- 2 Defina un filtro.
 - a Seleccione **appname** en el primer menú desplegable.
 - b Seleccione **contains** en el segundo menú desplegable.
 - c Escriba **hostd** en el cuadro de texto de valor.
- 3 Defina el intervalo de tiempo.
 - a En el menú desplegable **Intervalo de tiempo**, seleccione **Personalizado**.
 - b En el primer cuadro de texto, introduzca la fecha de ayer y 9 a.m.
 - c En el segundo cuadro de texto, introduzca la fecha de ayer y 10 a.m.
- 4 Haga clic en el botón **Buscar**.

Ejemplo: Buscar un grupo de hosts que tengan una cadena común en el nombre

Suponga que tiene varios hosts con un host con el siguiente nombre: w1-stvc-205-prod3 y otro host denominado w1-stvc-206-prod5.

Para buscar todos los registros de ambos hosts, cree la siguiente consulta.

- 1 1. Deje vacío el cuadro de texto de la búsqueda.
- 2 Defina el filtro.
 - a Seleccione **hostname** (nombre del host) en el menú desplegable del campo.
 - b Seleccione **empieza con** en el menú desplegable del operador.
 - c Escriba **w1-stvc** en el cuadro de texto del valor.

Como opción, puede utilizar el operador **contains** pero entonces debe usar un glob en el valor de búsqueda. En este ejemplo, debe escribir **w1-stvc-*** en el cuadro de texto del valor.

- 3 Haga clic en el botón **Buscar**.

Ejemplo: Consulte todos los errores notificados por tareas, eventos y alarmas de vCenter Server.

Para consultar todos los errores notificados por tareas, eventos y alarmas de vCenter Server:

- 1 En el cuadro de texto de búsqueda, escriba **error**.
- 2 Defina un filtro.
 - a Seleccione **vc_event_type** en el primer menú desplegable.
 - b Seleccione el operador **exists** en el segundo menú desplegable.
- 3 Haga clic en el botón **Buscar**.

Ejemplo: Consultar la latencia SCSI durante un segundo tal como la notificó ESX/ESXi

Para consultar la latencia SCSI durante un segundo tal como la notificó ESX/ESXi

- 1 En el cuadro de texto de búsqueda, escriba **scsi latency "performance has"**.
- 2 Defina un filtro.
 - a Seleccione **vmw_vob_component** en el primer menú desplegable.
 - b Seleccione el operador **contains** en el segundo menú desplegable.
 - c Escriba **scsiCorrelator** en el cuadro de texto.
- 3 Defina un segundo filtro.
 - a Seleccione **vmw_latency_in_micros** en el primer menú desplegable.
 - b Seleccione el operador **>** en el segundo menú desplegable.

c Escriba **1000000** en el cuadro de texto.

4 Haga clic en el botón **Buscar**.

Ejemplos de expresiones regulares

Puede escribir expresiones regulares en cuadros de texto para valores de campos a fin de extraer campos de eventos de registro.

Las expresiones que escriba deben usar la sintaxis de expresiones regulares de Java.

Tabla 3-1. Operadores de caracteres

Expresión regular	Descripción
\	Es el carácter de escape para los caracteres especiales.
\b	Límite de palabra
\B	No es límite de palabra
\d	Un dígito
\D	Un carácter que no es dígito
\n	Nueva línea
\r	Carácter de retorno
\s	Un espacio
\S	Cualquier carácter, excepto espacio en blanco
\t	Tabulador
\w	Un carácter alfanumérico o guion bajo
\W	Un carácter no alfanumérico o guion bajo

Por ejemplo, si tiene la cadena `1234-5678` y aplica las siguientes expresiones regulares, obtendrá:

Expresión regular	Resultado
\d	1
\d+	1234
\w+	1234
\S	1234-5678

Tabla 3-2. Operadores cuantificadores

Expresión regular	Descripción
.	Cualquier carácter, excepto una línea nueva
*	Cero o más con la máxima extensión posible
?	Cero o un carácter OR lo más corto posible
+	Uno o más
{<n>}	Exactamente <n> veces
{<n>,<m>}	<n> a <m> veces

Por ejemplo, si tiene la cadena `aaaaa` y aplica las siguientes expresiones regulares

Expresión regular	Resultado
.	a
*	aaaaa
.*?	aaaaa
.{1}	a
.{1,2}	aa

Tabla 3-3. Operadores de combinación

Expresión regular	Descripción
.*	Cualquier cosa
.*?	Cualquier cosa lo más breve posible antes de

Por ejemplo, si tiene la cadena `a b 3 hi d hi` y aplica las siguientes expresiones regulares

Expresión regular	Resultado
a.* hi	b 3 hi d
a .*? hi	b 3

Tabla 3-4. Operadores lógicos

Expresión regular	Descripción
^	Comienzo de una línea OR no si está entre corchetes
\$	Fin de una línea
()	Encapsulación
[]	Un carácter entre corchetes
	OR

Tabla 3-4. Operadores lógicos (continuación)

Expresión regular	Descripción
-	Intervalo
\A	Comienzo de una cadena
\Z	Fin de una cadena

Por ejemplo, si aplica las siguientes expresiones regulares

Expresión regular	Resultado
(hola)?	Contiene hola OR no contiene hola
(a b c)	a OR b OR c
[a-cp]	a OR b OR c OR p
palabra \$	Finaliza con palabra seguido por nada más

Tabla 3-5. Operadores de lectura previa

Expresión regular	Descripción
?=	Lectura previa positiva (incluye)
?!=	Lectura previa negativa (no incluye)

Por ejemplo, si aplica las siguientes expresiones regulares

Expresión regular	Resultado
is (?=\w+)\w{2} primario	es FT primario? falso
opid=(?!WFU-1fecf8f9)\S+	WFU-3c9bb994

Tabla 3-6. Otros ejemplos de expresiones regulares

Expresión regular	Descripción
[xyz]	x, y, o z
(información advertencia error)	información, advertencia o error
[a-z]	Una letra minúscula
[^a-z]	No una letra minúscula
[a-z]+	Una o más letras minúsculas
[a-z]*	Cero o más letras minúsculas
[a-z]?	Cero o una letra minúscula
[a-z]{3}	Exactamente tres letras minúsculas
[\d]	Un dígito

Tabla 3-6. Otros ejemplos de expresiones regulares (continuación)

Expresión regular	Descripción
\d+\$	Uno o más dígitos seguidos por fin del mensaje
[0-5]	Un número de 0 a 5
\w	Un carácter de palabra (letra, dígito o guion bajo)
\s	Espacio en blanco
\S	Cualquier carácter, excepto espacio en blanco
[a-zA-Z0-9]+	Uno o más caracteres alfanuméricos
([a-z] {2,} [0-9] {3,5})	Dos o más letras seguidas por tres a cinco números

Uso del gráfico Análisis interactivo para analizar registros

4

El gráfico que aparece en la parte superior de la página **Análisis interactivo** le permite llevar a cabo análisis visuales de los resultados de la consulta.

Los gráficos representan instantáneas gráficas de consultas de búsqueda de registros. Puede usar los menús desplegables que están debajo del gráfico para cambiar el tipo de gráfico.

Puede usar el primer menú desplegable que está a la izquierda para controlar el nivel de agregación del gráfico. La función **Cantidad** se selecciona de manera predeterminada.

Este capítulo incluye los siguientes temas:

- [Tipos de gráficos](#)
- [Gráficos de múltiples funciones](#)
- [Función de agregación](#)
- [Trabajar con gráficos](#)
- [Cambiar el tipo del gráfico de análisis interactivo](#)

Tipos de gráficos

Puede seleccionar diferentes tipos de gráficos para cambiar el modo en que se visualizan los datos en la página Análisis interactivo.

Los diferentes tipos de gráficos requieren de diferentes funciones de agregación; el uso de series temporales y campos por grupos. Las visualizaciones de los gráficos se limitan a los 2.000 resultados más recientes.

tipos de gráfico	Función de agregación	Requisito de serie temporal	Requisito de campo por grupos
Columna	Cualquiera	Serie temporal	No procede
Línea	Cualquiera	Serie temporal	No procede
Área	Cualquiera	Serie temporal	No procede
Barra	Cualquiera	Serie no temporal	Al menos un campo
Circular	Cantidad o Cantidad única	Serie no temporal	Al menos un campo
Burbuja	Cualquiera	Serie no temporal	Dos campos
Indicador	Cantidad	Serie no temporal	No procede

tipos de gráfico	Función de agregación	Requisito de serie temporal	Requisito de campo por grupos
Escalar	Cantidad	Serie no temporal	No procede
Tabla	Cualquiera	Cualquiera	No procede

Gráficos de múltiples funciones

Puede utilizar gráficos de múltiples funciones para comparar variables que no se encuentran en la misma escala.

Con los gráficos de múltiples funciones, puede asignar un eje y a cada serie o un eje x si desea comparar los conjuntos de datos de distintas categorías. Cada eje puede colocarse a la derecha o a la izquierda del gráfico. Puede intercambiar las funciones para intercambiar el eje y sobre el cual se trazan de derecha a izquierda.

Por ejemplo, puede realizar un gráfico de la cantidad de eventos agrupados por canal y nivel además del promedio de tareas agrupadas por canal y nivel.

Función de agregación

vRealize Log Insight ofrece varias funciones de agregación.



Tipo	Campo	Descripción
Cantidad	Eventos únicamente	Crea un gráfico de la cantidad de eventos para una consulta específica.
Cantidad única	Cualquier campo	Crea un gráfico de la cantidad de valores únicos para un campo.
Mínimo	Campos numéricos únicamente	Crea un gráfico del valor mínimo para un campo.
Máxima	Campos numéricos únicamente	Crea un gráfico del valor máximo para un campo.
Promedio	Campos numéricos únicamente	Crea un gráfico del valor promedio para un campo.
Desv est	Campos numéricos únicamente	Crea un gráfico de la desviación estándar para los valores de un campo.
Suma	Campos numéricos únicamente	Crea un gráfico de la suma de valores únicos para un campo.
Varianza	Campos numéricos únicamente	Crea un gráfico de la varianza para los valores de un campo.

Puede modificar el modo en que visualiza los resultados de la consulta.

Vista	Descripción
Para agrupar los resultados de las consultas por valores de campos específicos	Use el segundo menú desplegable del gráfico para agrupar los resultados de las consultas por valores de campos específicos en lugar de, o además de, series temporales.
Para ver la cantidad de eventos para un campo	Por ejemplo, para la cantidad de eventos por host, anule la selección de la casilla de verificación Serie temporales y marque la casilla de verificación para ese campo.
Para ver un gráfico de barras apiladas para un campo con distribuciones en grupo a través del tiempo	Seleccione la casilla de verificación Serie temporal y la casilla de verificación del campo.

Trabajar con gráficos

Puede modificar la manera en que se muestran los gráficos en la pestaña **Análisis interactivo**, añadir gráficos a sus paneles de control personalizados y administrar los gráficos del panel de control.

Tarea	Procedimiento
Modificar el intervalo de un gráfico	En la pestaña Análisis interactivo , use el menú desplegable de la izquierda del botón Buscar para cambiar el período que se muestra en el gráfico.
Modificar la granularidad de un gráfico	En la pestaña Análisis interactivo , use los botones de la esquina superior derecha para cambiar entre los distintos intervalos para cada punto que se representa en el gráfico. Los rangos disponibles dependen del intervalo especificado para la consulta.
Cargar un gráfico del panel de control en la pestaña Análisis interactivo	En la pestaña Paneles , ubique el gráfico y haga clic en el icono Abrir en Análisis interactivo  . El intervalo se fija con el intervalo actual del panel de control. Puede modificar el intervalo si es necesario.
Guardar un gráfico en el panel personalizado	<ol style="list-style-type: none"> En la esquina superior izquierda de la pestaña Análisis interactivo, haga clic en Añadir al panel. Como alternativa, desde el menú a la derecha del botón Buscar, seleccione Añadir consulta actual al panel. Escriba un nombre, seleccione el panel de destino en el menú desplegable, seleccione el tipo de widget, añada información sobre el widget y haga clic en Añadir.
Guardar una consulta como un gráfico en el panel de control personalizado	<ol style="list-style-type: none"> Haga clic en Añadir consulta actual al panel de control junto al botón Buscar. Escriba un nombre, seleccione el panel de control de destino en el menú desplegable, asegúrese de establecer el tipo de widget en Gráfico, añada información sobre el widget y haga clic en Añadir.
Guardar una consulta como una tabla de campos en el panel de control personalizado	<ol style="list-style-type: none"> Haga clic en Añadir consulta actual al panel de control junto al botón Buscar. Escriba un nombre, seleccione el panel de control de destino en el menú desplegable, asegúrese de establecer el tipo de widget en Tabla de campos, añada información sobre el widget y haga clic en Añadir.
Eliminar un widget del panel de control personalizado	<ol style="list-style-type: none"> En la pestaña Paneles de control, seleccione el panel de control personalizado que incluye el widget que desea eliminar. En la esquina superior derecha del widget, haga clic en el icono Otras acciones , y seleccione Eliminar. En el cuadro de diálogo Eliminar widget, haga clic en Eliminar para confirmar.

Cambiar el tipo del gráfico de análisis interactivo

Puede cambiar la agregación y el agrupamiento de los resultados de las consultas que aparecen en el gráfico para analizar gráficamente los eventos de registro.

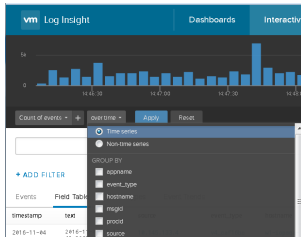
La cantidad de menús desplegables que ve debajo del gráfico depende de la función de agregación seleccionada.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 Use los menús desplegables debajo del gráfico Análisis interactivo para cambiar la función de agregación y el tipo de agrupamiento.



- Para consultar la cantidad de eventos a través del tiempo, seleccione el botón **Serie temporal**.
- Para consultar únicamente valores de eventos, seleccione el botón **Serie no temporal** y seleccione al menos un campo.

- 2 Haga clic en **Actualizar**.

Ejemplo: Agregación y agrupamiento en el gráfico Análisis interactivo

La siguiente tabla contiene ejemplos que ilustran la agregación y el agrupamiento en los gráficos de vRealize Log Insight.

Tabla 4-1. Ejemplo de agregación y agrupamiento en el gráfico Análisis interactivo

Selección en el primer menú desplegable	Selección en el segundo menú desplegable	Selección de serie temporal	Texto que aparece en la pantalla	Resultado
Cantidad	Serie temporal	Serie temporal	Cantidad de eventos a través del tiempo	El gráfico muestra un gráfico de barras con la cantidad de eventos para la consulta actual a través del tiempo.
Promedio	vmw_op_latency (VMware - vSphere)	Serie temporal	Promedio de vmw_op_latency (VMware - vSphere) a través del tiempo	El gráfico muestra un gráfico de líneas con un valor promedio de latencia de operaciones a través del tiempo.
Cantidad	vmw_esx_problem Nota El campo vmw_esx_problem no aparece de forma predeterminada. Debe extraer el campo vmw_esx_problem y guardar la consulta para que vmw_esx_problem aparezca en el menú desplegable.	Serie no temporal	Cantidad de eventos agrupados por vmw_esx_problem	El gráfico muestra un gráfico de barras de la cantidad de eventos para contener el campo vmw_esx_problem.
Cantidad	Serie temporal, vmw_esx_problem	Serie temporal	Cantidad de eventos a través del tiempo agrupados por vmw_esx_problem	El gráfico muestra un gráfico de barras apiladas agrupadas por vmw_esx_problem a través del tiempo.

Extracción dinámica de campos

5

En un entorno grande con numerosos eventos de registro, no siempre es posible localizar los campos de datos que consideramos importantes.

vRealize Log Insight proporciona extracción de campos en tiempo de ejecución para abordar este problema. Puede extraer cualquier campo de forma dinámica desde los datos proporcionando una expresión regular. Consulte [Ejemplos de expresiones regulares](#).

Nota Las consultas genéricas podrían ser lentas. Por ejemplo, si intenta extraer un campo utilizando la expresión `\(\d+\)`, la consulta devolverá todos los eventos de registro que contienen números entre paréntesis. Compruebe que sus consultas contengan tanto contexto textual como sea posible. Por ejemplo, una mejor consulta de extracción de campos es `Event for vm\(\d+\)`.

Puede usar los campos extraídos para buscar y filtrar la lista de eventos de registro, o para añadir eventos en el gráfico Análisis interactivo.

Nota Un nombre de campo extraído puede contener caracteres diferentes. Sin embargo, el nombre de campo de un evento consumido debe comenzar solo con una letra o un carácter de subrayado y contener solo letras, dígitos o el carácter de subrayado.

Este capítulo incluye los siguientes temas:

- [Extraer campos con extracción en un clic](#)
- [Modificar un campo extraído](#)
- [Duplicar un campo extraído](#)
- [Eliminar un campo extraído](#)

Extraer campos con extracción en un clic

En lugar de escribir los valores de contexto para extraer los campos en forma dinámica, puede utilizar la función de extracción en un clic.

La extracción en un clic completa todos los valores de contexto que corresponden al campo que seleccionó en un evento de registro.

Nota La opción de extracción en un clic está disponible solamente en la pestaña Eventos.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.
- 2 En la lista de eventos de registro, resalte el texto que representa el campo que desea extraer. Arriba del grupo de nombres del campo presentes en ese evento se muestra un menú de acción.
- 3 Haga clic en **Extraer campo**.
Los valores de contexto previo y posterior del panel Campos se completan automáticamente con el contexto que se necesita para extraer el campo resaltado.
- 4 (opcional) Modifique la expresión regular del valor Extraído en el panel Campos.
- 5 (opcional) Modifique las expresiones regulares del contexto previo y posterior en el panel Campos.
- 6 (opcional) Haga clic en **+ Añadir contenido adicional** para añadir más palabras clave y filtros. Se pueden añadir una o más palabras clave y utilizar un campo estático simple como filtro.
- 7 Si es un usuario administrador, seleccione qué usuarios pueden acceder al campo desde el menú desplegable.

Opción	Descripción
Todos los usuarios	Todos los usuarios verán el campo en sus eventos y en el menú desplegable del filtro.
Solo yo	Solo el creador del campo verá el campo en sus eventos y en el menú desplegable del filtro.

- 8 (opcional) En la parte superior del panel Campos, haga clic en **i** y, a continuación, en **Editar** para agregar notas a este campo. Agregue notas en la ventana **Editar notas** y haga clic en **Aceptar**.
- 9 Haga clic en **Guardar**.

Pasos siguientes

Es posible usar el campo extraído para buscar y filtrar la lista de eventos de registro o para sumar eventos en el gráfico de Análisis interactivo.

Puede modificar las definiciones de campos almacenadas o eliminarlas si ya no las necesita.

Modificar un campo extraído

Puede modificar las definiciones de los campos extraídos.

vRealize Log Insight crea copias de los campos que utiliza cuando crea gráficos, consultas o alertas. Si modifica la definición de un campo, todos los gráficos, consultas y alertas que utilizan el campo modificado se actualizan para reflejar la nueva definición.



Los usuarios normales solo pueden modificar su propio contenido. Los usuarios administradores pueden modificar su propio contenido y su contenido compartido.

Los campos del paquete de contenido son de solo lectura.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.
- 2 En la parte superior del panel Campos, haga clic en **Administrar campos extraídos**  y seleccione un campo extraído de la lista.
- 3 Modifique los valores y haga clic en **Actualizar**.
Un cuadro de diálogo muestra una lista del contenido que se verá afectado con el campo actualizado. Si el campo se comparte entre varios usuarios, el cuadro de diálogo muestra además una lista de los usuarios afectados.
- 4 (opcional) En la parte superior del panel Campos, haga clic en  y, a continuación, en **Editar** para agregar notas a este campo. Agregue notas en la ventana **Editar notas** y haga clic en **Aceptar**.
- 5 Haga clic en **Actualizar** para confirmar sus cambios.

Resultados

vRealize Log Insight actualiza todas las consultas, alertas y gráficos que usan el campo que ha modificado.

Duplicar un campo extraído

Puede duplicar un campo extraído.



Puede usar la opción **Duplicar** cuando desea extraer más de un campo de un evento o cuando ambos campos aparecen en un contexto similar. Después de extraer un campo y guardarlo, abra la definición del campo extraído y use la opción **Duplicar**. El campo duplicado tiene exactamente la misma definición que el campo extraído original. Puede modificar la definición del campo duplicado para que coincida con otro valor en caso de que le interese.

Los usuarios normales solo pueden duplicar su propio contenido. Los usuarios administradores pueden modificar su propio contenido y su contenido compartido.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.
- 2 En la parte superior del panel Campos, haga clic en **Administrar campos extraídos**  y seleccione un campo extraído de la lista.
- 3 Haga clic en **Duplicar** para crear una copia del campo.
- 4 (opcional) Modifique la expresión regular del valor Extraído en el panel Campos.
- 5 (opcional) Modifique las expresiones regulares del contexto previo y posterior en el panel Campos.
- 6 (opcional) Haga clic en  **Añadir contenido adicional** para añadir más palabras clave y filtros.
Se pueden añadir una o más palabras clave y utilizar un campo estático simple como filtro.
- 7 Si es un usuario administrador, seleccione qué usuarios pueden acceder al campo desde el menú desplegable.

Opción	Descripción
Todos los usuarios	Todos los usuarios verán el campo en sus eventos y en el menú desplegable del filtro.
Solo yo	Solo el creador del campo verá el campo en sus eventos y en el menú desplegable del filtro.

- 8 Haga clic en **Guardar**.

Pasos siguientes


Es posible usar el campo extraído para buscar y filtrar la lista de eventos de registro o para sumar eventos en el gráfico de Análisis interactivo.

Puede modificar las definiciones de campos almacenadas o eliminarlas si ya no las necesita.

Eliminar un campo extraído

Puede eliminar campos extraídos que ya no se necesitan.

vRealize Log Insight crea copias de los campos que usted utiliza cuando crea widgets, consultas o alertas. Si elimina un campo que se utiliza en widgets, consultas o alertas, vRealize Log Insight crea una copia temporal del campo eliminado para cada widget, consulta o alerta que utiliza ese campo.



Puede eliminar únicamente los campos que tienen el icono **Editar este campo**  junto a sus nombres. Los usuarios normales pueden eliminar únicamente sus propios contenidos. Los usuarios administradores pueden eliminar sus propios contenidos y sus contenidos compartidos.

Los campos del paquete de contenido son de solo lectura.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.
- 2 En la parte superior del panel Campos, haga clic en **Administrar campos extraídos**  y pase el cursor sobre un campo extraído de la lista.
- 3 Haga clic en .

Un cuadro de diálogo muestra una lista de contenidos que usa el campo que desea eliminar. Si usted es el usuario administrador y el campo está compartido por múltiples usuarios, el cuadro de diálogo también mostrará una lista de los usuarios afectados.
- 4 Haga clic en **Eliminar** para confirmar.

Resultados

Si se usa un campo eliminado en consultas existentes, vRealize Log Insight crea una copia temporal del campo y la muestra cuando usted carga una consulta que utiliza el campo eliminado.

Si exporta contenido que contiene campos temporales, vRealize Log Insight crea los campos en el paquete de contenidos exportado para evitar archivos temporales.

Administrar consultas de búsqueda

6

Puede exportar resultados de consultas; compartir consultas con otros usuarios; y guardar, eliminar, cambiar el nombre y cargar consultas existentes. Puede tomar instantáneas de las consultas y guardarles en paneles.

Este capítulo incluye los siguientes temas:

- Guarde una consulta en vRealize Log Insight
- Cambie el nombre de una consulta en vRealize Log Insight
- Cargar una consulta en vRealize Log Insight
- Eliminar una consulta de vRealize Log Insight
- Comparta la consulta actual
- Exportar la consulta actual
- Tomar una instantánea de una consulta
- Solución de problemas de los resultados de la consulta de vRealize Log Insight


Guarde una consulta en vRealize Log Insight

Puede guardar su consulta actual e intervalo de tiempo en vRealize Log Insight para revisarla con posterioridad. Las consultas almacenadas solo pueden cargarse desde la página **Análisis interactivo**.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En la pestaña **Análisis interactivo**, realice la consulta que desea guardar.
- 2 Haga clic y seleccione el icono **Añadir consulta actual a favoritos** .

- 3 Escriba un nombre y haga clic en **Guardar**.

Nota Las consultas almacenadas incluyen un intervalo fijo y no se actualizan. Al guardar una consulta, toma una instantánea de los mensajes de registro disponibles dentro del intervalo en el momento en que guarda.

Resultados

La consulta se añade a la lista de consultas favoritas.

Todos los usuarios, incluso los administradores, tienen una lista individual de consultas almacenadas.



Cambie el nombre de una consulta en vRealize Log Insight

Puede cambiar el nombre de una consulta que almacenó en vRealize Log Insight.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.
- 2 Haga clic en el icono Consultas favoritas .
- 3 Señale la consulta a la cual desea cambiar el nombre y haga clic en el icono **Editar esta consulta almacenada** .
- 4 Escriba el nombre nuevo y haga clic en **Guardar**.

Cargar una consulta en vRealize Log Insight

Puede cargar consultas de paquetes de contenido o consultas que ha guardado para verlas en la pestaña **Análisis interactivo**.


Las consultas guardadas se separan de elementos del panel de control. No aparecen en ningún panel personalizado. Si desea ver una consulta guardada, debe cargarla.

Todos los usuarios, incluso los administradores, tienen una lista individual de consultas almacenadas.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.
- 2 Haga clic en el icono Consultas favoritas 
- 3 En la lista Consultas favoritas, haga clic en la consulta que desea ver en la pestaña **Análisis interactivo**.

La consulta se carga en la pestaña **Análisis interactivo**. El intervalo de tiempo de la consulta se muestra por encima de la lista de eventos.

Pasos siguientes

Puede añadir la consulta a un panel de control, cambiar la granularidad del gráfico, o aplicar otros filtros a los resultados de consulta.



Eliminar una consulta de vRealize Log Insight

Puede eliminar las consultas guardadas de vRealize Log Insight.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.
- 2 En el menú desplegable que se encuentra a la derecha del botón **Buscar**, seleccione **Cargar consulta**.
- 3 Haga clic en el icono Consultas favoritas 
- 4 En la lista Consultas favoritas, haga clic en  junto a la consulta que desea eliminar.
- 5 Haga clic en **Eliminar** para confirmar.


Comparta la consulta actual

Puede enviar a sus pares un vínculo a la consulta actual.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En la pestaña **Análisis interactivo**, realice la consulta que desea compartir.
- 2 Haga clic en  y seleccione **Compartir consulta**.
vRealize Log Insight crea y muestra una dirección URL abreviada para la consulta. Antes de eliminarla, esta se conserva durante 93 días desde su último uso.
- 3 Copie la URL y envíela a la persona con la cual desea compartirla.


Exportar la consulta actual

Puede exportar los resultados de una consulta de registro para compartirlos con otros sistemas, o reenviarlos a su contacto de soporte.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En la pestaña **Análisis interactivo**, realice la consulta que desea exportar.
- 2 Haga clic en  y seleccione **Exportar resultados del evento**.
- 3 Seleccione el formato para guardar la consulta y haga clic en **Exportar**.

Elemento de menú	Descripción
Eventos sin procesar	Seleccione esta opción para guardar los resultados en formato TXT.
JSON	Seleccione esta opción para guardar los resultados en formato JSON.
CSV	Seleccione esta opción para guardar los resultados en formato CSV.

- 4 Si la consulta de registro tiene más de 20.000 resultados, introduzca la ubicación del recurso compartido de NFS al que desea exportar los resultados y haga clic en **Exportar**.

La exportación tarda algún tiempo en finalizar, según el volumen de los resultados de la consulta de registro. El progreso se muestra como una notificación en la parte superior de la ventana. No se puede exportar otro conjunto de resultados de consulta durante este proceso, pero se pueden usar otras funciones de vRealize Log Insight. Una vez finalizada la exportación, puede acceder al recurso compartido de NFS para abrir el archivo que contiene los resultados.

Nota Para asegurarse de poder ver el progreso de la exportación, acceda a la interfaz de usuario de vRealize Log Insight desde un nodo y no utilice la dirección VIP.

Tomar una instantánea de una consulta



Puede tomar una instantánea de su rango de tiempo y consulta actual en vRealize Log Insight para una visualización rápida o para guardarla en un panel. Las instantáneas pueden tomarse desde la página **Análisis interactivo**.

Una instantánea guarda los mensajes de registro disponibles dentro del intervalo en el momento en el que tomó la instantánea. Después de tomar la instantánea, haga clic en la imagen para volver a la consulta en el momento en que la tomó. Si desea guardar al menos una instantánea, añádala en un panel existente o cree un panel nuevo.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En la pestaña **Análisis interactivo**, realice la consulta que desea guardar como instantánea.
- 2 Haga clic en el icono de instantánea.
La instantánea se muestra en la parte inferior de la pantalla.
- 3 (opcional) Modifique la consulta y tome otras instantáneas.
Las instantáneas se muestran en la parte inferior de la pantalla.
- 4 (opcional) En la parte inferior de la pantalla, haga clic en  y seleccione **Guardar todos en el panel**.
 - a Seleccione un panel existente o cree un panel nuevo.
 - b Haga clic en **Añadir**.
La instantánea se añade en el panel seleccionado o en el nuevo.
- 5 (opcional) Haga clic en la "X" de la instantánea para eliminarla.
- 6 (opcional) Haga clic en  y seleccione **Borrar todos** para eliminar las instantáneas.

Solución de problemas de los resultados de la consulta de vRealize Log Insight

Un icono de advertencia junto a un widget del panel de control o en la página de análisis interactivo indica que los resultados de la consulta pueden estar incompletos.

Una causa es un agotamiento del tiempo de espera durante la extracción de campos dinámicos mientras se ejecuta la consulta. Puede producirse un agotamiento del tiempo de espera cuando vRealize Log Insight se sobrecarga al procesar demasiados eventos de registro, demasiadas consultas o contenido complejo. Los tiempos de espera agotados pueden tener como resultado que se omita una pequeña parte de los registros recopilados. Un icono de advertencia y el mensaje de advertencia detallado le informa acerca de estos tiempos de espera.

Nota Los resultados de las consultas afectadas por los tiempos de espera agotados no se han solucionado y pueden variar, según la carga de vRealize Log Insight en el momento preciso y la cantidad de registros que se están procesando para la consulta.

Para resolver el problema, intente llevar a cabo las siguientes acciones.

- Asegúrese de que el dimensionamiento de vRealize Log Insight sea correcto para la carga de consumo. Para obtener más información acerca del dimensionamiento, consulte
 - a Vaya a la página **Supervisión de sistema** del menú Administración para comprobar la carga de consumo.

Nota Para acceder al menú Administración, se necesitan privilegios de administrador.

- b Vaya a la pestaña **Consultas activas** de la página **Supervisión del sistema** para comprobar el número de consultas activas y el tiempo necesario para ejecutarlas.
 - c Asegúrese de que el dimensionamiento de vRealize Log Insight sea correcto para la tasa de consumo actual.
- Revise su consulta. En algunos casos, las consultas que tienen tiempos de procesamiento prolongados y probabilidad de que se agote el tiempo de espera contienen una cláusula de agrupamiento, cubren un número importante de registros o devuelven una cantidad relativamente elevada de resultados.

En lugar de una consulta cuyo resultado es un valor único, sustitúyala por una consulta que genere resultados de series temporales. Este tipo de consulta no se ve afectado por el volumen del registro durante el procesamiento de la consulta.

Trabajar con paneles de control

7

Los paneles de control en vRealize Log Insight son colecciones de widgets de gráficos, tablas de campos y listas de consultas.

Paneles de control personalizados

Los paneles de control personalizados son creados por los usuarios de la instancia actual de vRealize Log Insight. Los paneles de control personalizados se organizan en dos categorías, Mis paneles de control y Paneles compartidos. Los paneles de control compartidos están visibles para todos los usuarios de la instancia de vRealize Log Insight.

Mis paneles de control son específicos del usuario.

Los usuarios normales pueden modificar únicamente los paneles de control de la sección Mi panel de control.

Los usuarios administradores pueden modificar los paneles de control de la sección Mis paneles de control y los paneles de control que crearon en la sección Paneles de control compartidos.

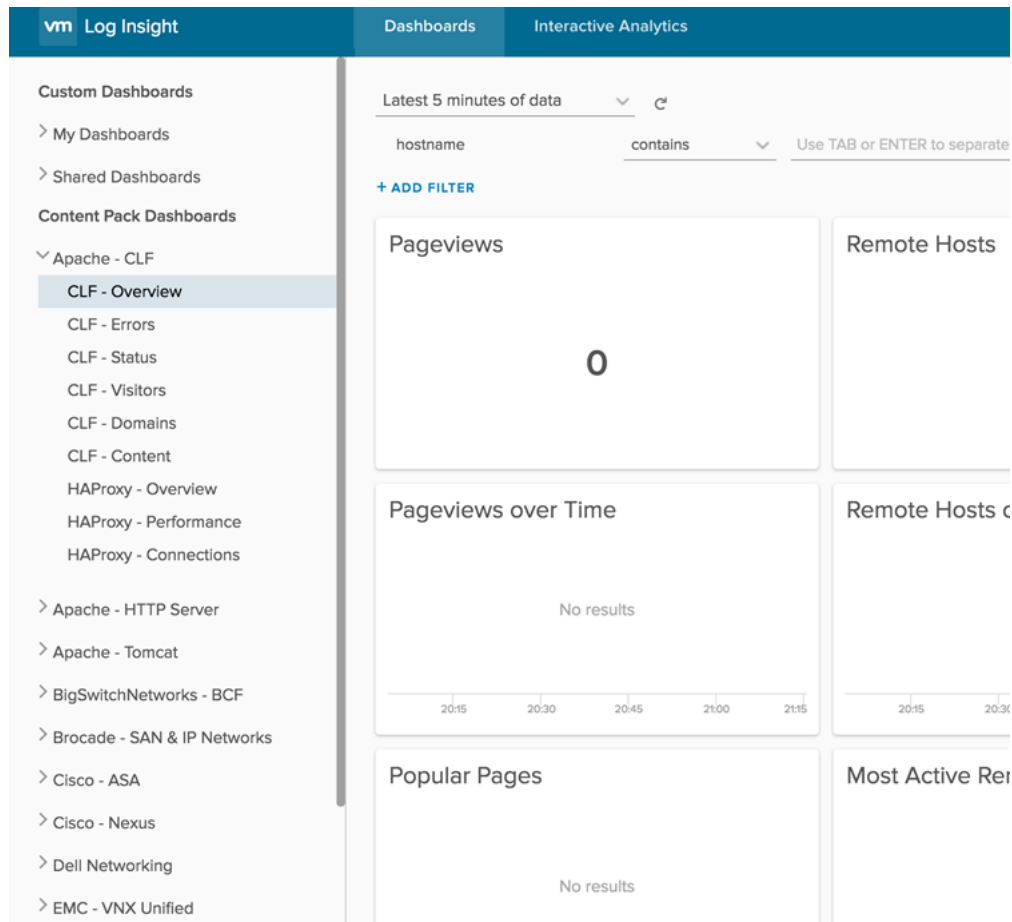
Paneles de control de paquetes de contenidos

Los paneles de control de paquetes de contenidos se importan con los paquetes de contenidos y están visibles para todos los usuarios de la instancia de vRealize Log Insight.

Nota Los paneles del paquete de contenido son de solo lectura. No es posible eliminarlos ni cambiarles el nombre. No obstante, es posible clonar los paneles del paquete en su panel personalizado. Es posible clonar paneles completos o widgets individuales.

Para ver los paneles de control que están disponibles en su instancia de vRealize Log Insight, haga clic en **Paneles de control** en la esquina superior izquierda de la interfaz de usuario de vRealize Log Insight. El panel que aparece a la izquierda muestra todos los paneles de control a los que tiene acceso, agrupados por Paneles personalizados y Paneles de paquetes de contenido. Haga clic en > que aparece junto a cada subgrupo para mostrar los paneles de control asociados. Puede abrir un grupo de paneles de control al mismo tiempo haciendo clic en > que aparece junto al nombre de grupo. Haga clic en > junto a otro nombre de grupo para abrir un nuevo grupo y para cerrar el anterior. Solo se puede abrir un grupo al mismo tiempo.

Para ver los contenidos de un panel de control, haga clic en el nombre del panel de control que se encuentra en la lista a la izquierda.



Este capítulo incluye los siguientes temas:

- [Administrar paneles de control](#)
- [Añadir un widget de lista de consultas al panel](#)
- [Añadir una consulta a un widget de lista de consultas en un panel](#)
- [Añadir un widget de tabla de campos a un panel de control](#)
- [Agregar un widget Tipos de eventos al panel de control](#)
- [Agregar un widget Tendencias de eventos al panel de control](#)
- [Filtrar usando valores de campo de gráficos](#)

Administrar paneles de control




Puede añadir, modificar y eliminar paneles de control en su espacio Paneles de control personalizados.


Los paneles de control de Paquete de contenido, que son los paneles de control de serie que se descargan, no pueden modificarse, pero puede clonar estos paneles de control a su espacio Paneles de control personalizados y modificar los clones.

Importante vRealize Log Insight no comprueba la existencia de nombres duplicados en los paneles de control, las consultas y las alertas que guarde o clone. El nombre mostrado no es un identificador único cuando vRealize Log Insight guarda consultas. Por lo tanto, puede guardar varios gráficos, alertas y paneles de control con el mismo nombre. Para facilitar la recuperación de los datos, no duplique nombres cuando guarde gráficos, alertas o paneles de control.

Trabajar con paneles de control personalizados

La siguiente tabla enumera las capacidades del producto que puede utilizar para crear o modificar un panel de control personalizado.

Tarea	Procedimiento
Crear un panel de control personalizado.	En la pestaña Paneles de control , seleccione Mis paneles de control , y haga clic en Nuevo panel de control en la parte inferior izquierda.
Editar el nombre de un panel de control personalizado.	En la pestaña Paneles de control , apunte al nombre del panel de control, haga clic en el icono de menú  y seleccione Cambiar nombre . Introduzca un nuevo nombre y haga clic en Guardar .
Eliminar un panel de control personalizado.	En la pestaña Paneles de control , apunte al nombre del panel de control, haga clic en el icono de menú  y seleccione Eliminar . En el cuadro de diálogo de confirmación, seleccione Eliminar .
Clonar un panel de control a partir de un paquete de contenido a su panel de control personalizado.	<ol style="list-style-type: none"> 1 En la pestaña Paneles de control, seleccione un paquete de contenido e indique el panel de control que desea clonar. 2 Haga clic en el icono de menú  y seleccione Clonar en el menú desplegable. 3 Escriba un nombre y haga clic en Guardar. <p>Si es un usuario administrador, puede seleccionar si compartir su panel de control con otros usuarios.</p>
Añadir un widget de gráfico a un panel de control.	<ol style="list-style-type: none"> 1 En la esquina superior izquierda de la pestaña Análisis interactivo, haga clic en Añadir al panel. Como alternativa, desde el menú a la derecha del botón Buscar, seleccione Añadir consulta actual al panel. 2 Escriba un nombre, seleccione el panel de destino en el menú desplegable, seleccione el tipo de widget, añada información sobre el widget y haga clic en Añadir.
Añadir un widget de lista de consultas al panel de control.	Consulte Añadir un widget de lista de consultas al panel .
Añadir una consulta a un widget de lista de consultas en un panel de control.	Consulte Añadir una consulta a un widget de lista de consultas en un panel .

Tarea	Procedimiento
Añadir una consulta a un widget de tabla de campos en un panel de control.	Consulte Añadir un widget de tabla de campos a un panel de control
Agregar un widget de tipos de eventos al panel de control.	Agregar un widget Tipos de eventos al panel de control
Agregar un widget de tendencias de eventos al panel de control.	Agregar un widget Tendencias de eventos al panel de control
Eliminar un widget de un panel de control.	<ol style="list-style-type: none"> 1 En la pestaña Paneles de control, seleccione el panel de control personalizado que incluye el widget que desea eliminar. 2 En la esquina superior derecha del widget, haga clic en el icono Otras acciones  y seleccione Eliminar. 3 En el cuadro de diálogo Eliminar widget, haga clic en Eliminar para confirmar.
Mostrar datos sincronizados en el tiempo para todos los widgets.	<p>De forma predeterminada, puede mostrar una etiqueta de leyenda para un punto de datos determinado en un widget, pasando el cursor por encima del punto. También puede mostrar etiquetas de leyenda para todos los widgets para el mismo momento en el tiempo, habilitando el ajuste Mostrar leyenda en todos los widgets, que se aplica a todos los paneles. Este ajuste se basa en cookies y se conserva en posteriores sesiones de explorador.</p> <ol style="list-style-type: none"> 1 En la pestaña Paneles de control, seleccione un panel de control. 2 En la esquina superior izquierda del panel de control, establezca el conmutador Mostrar leyenda en todos los widgets en la posición activada.
Solucionar problemas de un widget que muestra el símbolo de advertencia.	Consulte Solución de problemas de los resultados de la consulta de vRealize Log Insight .


Añadir un widget de lista de consultas al panel

Puede guardar listas de consultas de búsqueda en sus paneles personalizados creando widgets de lista de consultas.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En la pestaña **Análisis interactivo**, ejecute la consulta que desea añadir al panel.
- 2 Haga clic en el icono **Añadir consulta actual al panel** .
- 3 En el menú desplegable **Panel**, seleccione el panel donde desea añadir la consulta.

- 4 En el menú desplegable **Tipo de widget**, seleccione **Lista de consultas**.
- 5 En el menú desplegable **Lista de consultas**, seleccione **Nueva lista de consultas**, escriba un nombre para la lista y haga clic en **Guardar**.
- 6 Haga clic en **Añadir**.

Resultados

El widget de lista de consultas aparece en el panel que especificó.

Pasos siguientes

Puede añadir consultas al widget de lista de consultas creado. Consulte [Añadir una consulta a un widget de lista de consultas en un panel](#).

Añadir una consulta a un widget de lista de consultas en un panel


Los widgets de lista de consultas proporcionan rápido acceso a una o más consultas guardadas desde el panel.

Puede modificar o personalizar widgets de lista de consultas para añadir nuevas consultas.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En la pestaña **Análisis interactivo**, ejecute la consulta que desea añadir al widget de lista de consultas.
- 2 Haga clic en el icono **Añadir consulta actual al panel** .
- 3 En el menú desplegable **Panel**, seleccione el panel que contiene el widget de lista de consultas.
- 4 En el menú desplegable **Tipo de widget**, seleccione **Lista de consultas**.
- 5 En el menú desplegable **Lista de consultas**, seleccione el nombre del widget al que desea añadir la consulta y haga clic en **Guardar**.
- 6 Haga clic en **Añadir**.

Resultados

vRealize Log Insight añade la consulta al widget seleccionado.

Nota Los widgets de lista de consultas utilizan consultas de mensajes. Si utiliza la misma consulta de mensaje en un widget de gráfico y escoge un grupo por campo que no existe en ninguno de los mensajes, el cuadro no mostrará resultados.


Añadir un widget de tabla de campos a un panel de control

Los widgets de tabla de campos proporcionan rápido acceso a uno o más campos guardados desde el panel de control.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En la pestaña **Análisis interactivo**, ejecute la consulta que desea añadir al widget de tabla de campos.
- 2 Haga clic en el icono **Añadir consulta actual al panel** .
- 3 En el menú desplegable **Panel de control**, seleccione el panel de control donde desea añadir la tabla de campos.
- 4 En el menú desplegable **Tipo de widget**, seleccione **Tabla de campos**.
- 5 Seleccione los campos que desea incluir en la tabla de campos.
- 6 Haga clic en **Añadir**.

Resultados

El widget de tabla de campos aparece en el panel de control especificado.


Agregar un widget Tipos de eventos al panel de control

Los widgets Tipos de eventos proporcionan acceso a los grupos de tipos de eventos (creados mediante aprendizaje automático para agruparlos).

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En la pestaña **Análisis interactivo**, ejecute la consulta que desea añadir al widget.
- 2 Haga clic en el icono **Añadir consulta actual al panel** .
- 3 En el menú desplegable **Panel**, seleccione el panel donde desea añadir el widget.
- 4 En el menú desplegable **Tipo de widget**, seleccione Tipos de eventos.
- 5 Haga clic en **Añadir**.

Resultados

El widget aparece en el panel que especificó.


Agregar un widget Tendencias de eventos al panel de control

Los widgets Tendencias de eventos proporcionan acceso a la información sobre tendencias de eventos. Esta información muestra el análisis de dichas tendencias durante un periodo de tiempo específico.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En la pestaña **Análisis interactivo**, ejecute la consulta que desea añadir al widget.
- 2 Haga clic en el icono **Añadir consulta actual al panel** .
- 3 En el menú desplegable **Panel**, seleccione el panel donde desea añadir el widget.
- 4 En el menú desplegable **Tipo de widget**, seleccione Tendencias de eventos.
- 5 Haga clic en **Añadir**.

Resultados

El widget aparece en el panel que especificó.

Filtrar usando valores de campo de gráficos

Puede usar un valor de campo en un gráfico como filtro en el panel que incluye el gráfico, en un panel diferente que usa el campo y en Análisis interactivo.

Si advierte un problema con un valor de campo en un gráfico, puede usar rápidamente el valor de campo como entrada e ir a otro panel que use ese campo. Si ningún otro panel usa el campo, puede usar el valor de campo como filtro en el mismo panel o ejecutarlo en Análisis interactivo.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En el menú desplegable **Panel**, seleccione el panel que incluye un widget de gráfico.
- 2 En el widget de gráfico, desplácese sobre los datos del gráfico y vea los valores de campo que aparecen como información de herramienta.
- 3 Haga clic en el valor de campo que desea usar como filtro.
Aparece el menú **Añadir valor como filtro**.
- 4 Seleccione dónde desea usar el valor de campo como filtro.

Opción	Acción
Análisis interactivo	La página Análisis interactivo se abre y muestra los resultados de la consulta de gráfico. El valor de campo seleccionado en el Paso 3 se usa como filtro.
Este panel	El valor de campo seleccionado en el Paso 3 se usa como filtro en el mismo panel.
Otro panel	El valor de campo seleccionado en el Paso 3 se usa como filtro en otro panel que incluye el campo.

Trabajar con paquetes de contenido



Los paquetes de contenido incluyen paneles, campos extraídos, consultas almacenadas y alertas relacionados con un producto específico o grupos de registros.

vRealize Log Insight viene instalado con paquetes de contenido de tipo general, de vSphere, VMware vSAN y vRealize Operations Manager. También puede instalar paquetes de contenido desde el catálogo de Content Pack, o puede crear y exportar sus propios paquetes de contenido para uso individual o en equipo.

Este capítulo incluye los siguientes temas:

- [Utilizar paquetes de contenido](#)
- [Crear paquetes de contenidos](#)
- [Alias de almacén de datos a identificador de dispositivo para almacenes de datos de vSphere](#)

Utilizar paquetes de contenido

Los paquetes de contenido incluyen paneles, campos extraídos, consultas almacenadas y alertas relacionados con un producto específico o grupos de registros.

Para ver los paquetes de contenido cargados en el sistema, seleccione **Paquetes de contenido** en el menú desplegable de la esquina superior derecha de la interfaz de usuario de vRealize Log Insight.

Para ver el contenido de un paquete de contenido, haga clic en el paquete de contenido de la lista que se encuentra a la izquierda.

Paquetes de contenido

La categoría Paquetes de contenido incluye los grupos de paneles de control importados, los campos extraídos, las consultas y alertas. Los paquetes de contenido General y VMware - vSphere se importan de manera predeterminada.

Nota Los paneles del paquete de contenido son de solo lectura. No es posible eliminarlos ni cambiarles el nombre. No obstante, es posible clonar los paneles del paquete en su panel personalizado. Es posible clonar paneles completos o widgets individuales.

Contenido personalizado

La categoría Contenido personalizado incluye paneles, campos extraídos y consultas en la instancia actual de vRealize Log Insight. La sección Mi contenido incluye el contenido personalizado del usuario que está conectado al sistema. La sección Contenido compartido incluye el contenido que se comparte entre todos los usuarios de vRealize Log Insight.

Solo los usuarios administradores pueden compartir contenido con otros usuarios. Solo los usuarios administradores pueden administrar el contenido compartido.

Nota No es posible desinstalar contenido de la sección Contenido personalizado. Si desea eliminar la información almacenada de la sección Contenido personalizado, debe eliminar los elementos individuales, como paneles de control, consultas, alertas y campos.

Instalar un paquete de contenido del Catálogo de paquetes de contenido

Puede instalar paquetes de contenido del Catálogo de paquetes de contenido sin abandonar la UI de vRealize Log Insight.

Si su servidor de vRealize Log Insight no tiene acceso a Internet, puede descargar e instalar paquetes de contenido por separado, como se describe en [Importar un paquete de contenido](#).

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight como usuario con permiso **Editar administrador**. El formato URL es `https://host-log-insight`, donde *host-log-insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En el menú desplegable de la esquina superior derecha, seleccione **Paquetes de contenido**.
- 2 Haga clic en **Catálogo** que aparece en **Catálogo de paquetes de contenido** en la parte izquierda.
- 3 Haga clic en el paquete de contenido que desee instalar.
- 4 Seleccione la casilla de verificación para aceptar los términos del contrato de licencia.
- 5 Haga clic en **Instalar**.

Resultados

Cuando se completa la instalación, el paquete de contenido aparece a la izquierda, en la lista Paquetes de contenido instalados.

Actualizar un paquete de contenido instalado a partir del mercado del paquete de contenido

Puede actualizar los paquetes de contenido que ya están instalados desde el catálogo de paquetes de contenido sin salir de vRealize Log Insight.

Nota Cuando las alertas de los paquetes de contenido están habilitadas, estas se copian en un perfil de usuario. Los usuarios pueden modificar las condiciones o la descripción de la copia. A partir de las definiciones de alertas instanciadas en 4.0, al actualizar un paquete de contenido y, por extensión, las definiciones de sus alertas, se actualizan o se eliminan las copias que coincidan con el paquete de contenido en cuestión. Si desea conservar las modificaciones de los usuarios, expórtelas como paquete de contenido antes de aplicar la actualización y vuelva a importar los cambios al perfil de usuario tras la actualización.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight como usuario con permiso **Editar administrador**. El formato URL es `https://host-log-insight`, donde *host-log-insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En el menú desplegable de la esquina superior derecha, seleccione **Paquetes de contenido**.
- 2 Desde el menú de la izquierda, seleccione **Actualizaciones** para ver una lista de los paquetes de contenido para los que están disponibles las actualizaciones.
 - Para actualizar un único paquete de contenido, haga clic en su icono para abrir una ventana informativa. Haga clic en **Actualizar** para empezar la importación. Dependiendo del paquete de contenido, después de completarse la importación es posible que se muestren instrucciones adicionales. Si aparecen, siga los pasos de configuración para finalizar la actualización correctamente.
 - Para actualizar de forma silenciosa todos los paquetes de contenido con actualizaciones pendientes, haga clic en **Actualizar todo**. Lea las instrucciones incluidas en la ventana emergente de información y haga clic en **Actualizar** para continuar. Tras la actualización, haga clic en cada paquete de contenido para ver si deben realizarse pasos adicionales para finalizar la importación. Si ha exportado un paquete de contenido para conservar las modificaciones de los usuarios, vuelva a importarlo al perfil de usuario.

Resultados

El paquete de contenido disponible se muestra a la izquierda en el listado de paquetes de contenido instalados.

Importar un paquete de contenido

Puede importar paquetes de contenido para intercambiar información definida por el usuario con otras instancias de vRealize Log Insight.

Únicamente puede importar archivos de paquete de contenido (VLCP).

Puede descargar paquetes de contenido desde VMware Solutions Exchange, en <https://marketplace.vmware.com>.

Si utiliza un servidor de vRealize Log Insight con acceso a Internet, también puede instalar o actualizar paquetes de contenido desde dentro de vRealize Log Insight. Consulte [Instalar un paquete de contenido del Catálogo de paquetes de contenido](#).

Nota Al actualizar un paquete de contenido que tenga alertas habilitadas, la actualización sobrescribe las modificaciones que haya realizado en las condiciones o las descripciones de alerta.

Las modificaciones se mantienen en el perfil de usuario. Para conservar estas modificaciones, expórtelas como paquete de contenido antes de la actualización y vuelva a importarlo al perfil de usuario tras la actualización.

Requisitos previos

- Si desea utilizar **Instalar como paquete de contenido** como método de importación, verifique que tenga la sesión iniciada en la interfaz web de usuario de vRealize Log Insight como un usuario con el permiso **Editar administrador**. El formato URL es `https://host-log-insight`, donde *host-log-insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.
- Si desea utilizar **Importar en Mi contenido**, puede iniciar sesión en la interfaz web de usuario de vRealize Log Insight con cualquier nivel de permiso.

Procedimiento

- 1 En el menú desplegable de la esquina superior derecha, seleccione **Paquetes de contenido**.
- 2 En la esquina superior izquierda, haga clic en **Importar paquete de contenido**.

3 Seleccione el método de importación.

Elemento de menú	Descripción
instalar como paquete de contenido	<p>El contenido se importa como un paquete de contenido de solo lectura visible para todos los usuarios de la instancia de vRealize Log Insight.</p> <p>Nota Los paneles del paquete de contenido son de solo lectura. No es posible eliminarlos ni cambiarles el nombre. No obstante, es posible clonar los paneles del paquete en su panel personalizado. Es posible clonar paneles completos o widgets individuales.</p>
Importar en Mi contenido	<p>El contenido se importa como contenido personalizado a su espacio de usuario, y solo usted puede verlo. Puede editar el contenido importado sin necesidad de clonarlo.</p> <p>Nota Los metadatos de paquetes de contenido, tal como nombre, autor, icono y demás, no se muestran en este modo.</p> <p>Una vez importado en Mi contenido, el paquete de contenido no puede desinstalarse como paquete. Si desea eliminar un paquete de contenido de Mi contenido, debe eliminar individualmente cada uno de sus elementos, tales como tableros, consultas, alertas y campos.</p>

Los usuarios normales pueden importar paquetes de contenido solo en sus propios espacios de usuario.

- 4 Examine el paquete de contenido que desea importar, y haga clic en **Abrir**.
- 5 Haga clic en **Importar**.
- 6 (opcional) Si seleccionó importar el paquete de contenido como contenido personalizado, aparece un cuadro de diálogo y se le solicita que seleccione el contenido que desea importar. Seleccione los elementos de contenido y haga clic en **Importar** de nuevo.

Observe que los campos que se usan en consultas, gráficos y alertas importados también se importan.
- 7 (opcional) Algunos paquetes de contenido requieren pasos de configuración adicionales. Las instrucciones para estos pasos aparecen una vez finalizada la importación. Complete estos pasos antes de usar el paquete de contenido.

Resultados

El paquete de contenido importado ya se puede usar y aparece en Paquetes de contenido o en la lista Contenido personalizado situada a la izquierda.

Nota Las alertas importadas están deshabilitadas de forma predeterminada. Consulte [Habilitar consultas de alerta](#).

Exportar un paquete de contenido


Puede exportar sus paneles personalizados, consultas guardadas, alertas y campos extraídos como un paquete de contenido, para compartir contenido entre instancias de vRealize Log Insight o con usuarios de vRealize Log Insight en la comunidad.

Los paquetes de contenido se guardan como archivos vCenter vRealize Log Insight Content Pack (VLCP).

Todos los campos que se usan en consultas, gráficos y alertas que exporta están incluidos en el paquete de contenido exportado.

Si exporta contenido que incluye campos temporales, vRealize Log Insight crea estos campos dentro del paquete de contenido durante la exportación.

Procedimiento

- 1 En el menú desplegable de la esquina superior derecha, seleccione **Paquetes de contenido**.
- 2 Haga clic en el paquete de contenido que desea exportar y seleccione **Exportar** en el menú desplegable  junto al nombre del paquete de contenido.
- 3 (opcional) Seleccione el contenido que desee incluir en el paquete de contenido.

Nota No puede anular la selección de campos que se usan en paneles, consultas o alertas seleccionados para exportar.

- 4 En los campos de texto a la derecha, complete los metadatos para su paquete de contenido.

Opción	Descripción
Nombre	El nombre se muestra cuando importa el paquete en una instancia de vRealize Log Insight. El nombre del archivo del paquete de contenido se deriva del cuadro de texto Nombre . El formato es <i>Proveedor - Producto</i> . Por ejemplo, VMware - vSphere.
Versión	Si tiene planes de actualizar este paquete de contenido, escriba una versión. vRealize Log Insight muestra la versión cuando intenta instalar un paquete de contenido que ya está en la lista Paquetes de contenido.
Espacio de nombres	El espacio de nombres es un identificador único para el paquete de contenido. Use la asignación de nombres DNS inversa, por ejemplo, com.companyname.contentpackname .
Autor	Opcionalmente, puede escribir su nombre o el nombre de su empresa.
Sitio web	Opcionalmente, puede proporcionar un vínculo al sitio web asociado al paquete de contenido. Todos los usuarios que pueden ver el paquete de contenido también pueden ver el vínculo del sitio web.

Opción	Descripción
Descripción	Opcionalmente, puede proporcionar información sobre el contenido y propósito del paquete.
Icono	Opcionalmente, puede explorar en busca de un icono para mostrar junto al nombre del paquete de contenido. Nota El formato del archivo de icono debe ser PNG o JPG, y se escala a 144 por 144 píxeles.

Nota Estos datos pueden verse solo si importa el paquete de contenido utilizando la opción **Instalar como paquete de contenido**. No puede ver esta información si elige importar el paquete de contenido como contenido personalizado.

- Haga clic en **Exportar**, desplácese hasta la ubicación donde desea guardar el archivo y haga clic en **Guardar**.

Resultados

El archivo VLCP exportado se descarga en la ubicación seleccionada.

Visualización de detalles de los elementos del paquete de contenido

Puede abrir las consultas que compilan los paneles o puede abrir las definiciones de los campos, consultas y alertas directamente desde la vista de los paquetes de contenido.

Puede usar las definiciones de los elementos del paquete de contenido como planillas para sus definiciones personalizadas.

Procedimiento

- En el menú desplegable de la esquina superior derecha, seleccione **Paquetes de contenido**.
- Seleccione el paquete de contenido que incluye el elemento que desea revisar.
- Haga clic en el botón que corresponde al tipo de elemento que desea revisar.

Por ejemplo, haga clic en **Alertas** para visualizar todas las alertas que incluye el paquete de contenido.

- En la lista de elementos, haga clic en el nombre del elemento que desee revisar.

Resultados

Se abre la página **Análisis interactivo** y muestra la consulta que corresponde al elemento seleccionado.

Pasos siguientes

Puede modificar la consulta o la definición del elemento del paquete de contenido y guardarla en su contenido personalizado.

Desinstalar un paquete de contenido

Es posible desinstalar paquetes de contenido. La desinstalación de paquetes de contenido elimina los paneles personalizados, las consultas almacenadas, las alertas y los campos extraídos.


Los paquetes de contenido se guardan como archivos vCenter vRealize Log Insight Content Pack (VLCP).

La desinstalación de un paquete de contenido hace que deje de estar disponible en forma permanente para todos los usuarios. Realice una copia de seguridad exportando el paquete de contenido como archivo VLCP en primer lugar. Consulte [Exportar un paquete de contenido](#).

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight como usuario con permiso **Editar administrador**. El formato URL es `https://host-log-insight`, donde *host-log-insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 En el menú desplegable de la esquina superior derecha, seleccione **Paquetes de contenido**.
- 2 Haga clic en el paquete de contenido que desea desinstalar y seleccione **Desinstalar** en el menú desplegable  junto al nombre del paquete de contenido.
- 3 Haga clic en **Desinstalar**.

Resultados

El paquete de contenido se elimina de la lista de paquetes de contenido instalados.

Extraer campos de paquete de contenido seleccionados para las consultas

Al ejecutar consultas que utilizan campos extraídos, puede especificar los paquetes de contenido en los que se ejecutará la consulta.

De forma predeterminada, todos los campos de paquete de contenido se extraen después de ejecutar una consulta. Sin embargo, es posible que algunos de los paquetes de contenido no sean relevantes para la información deseada y que, como resultado, los campos extraídos generen una eficacia nula y sobrecarga durante el procesamiento de consultas.

Para ejecutar la consulta de forma más eficaz y reducir los tiempos de espera de extracción de los campos de paquete de contenido, puede seleccionar solo los paquetes de contenido que contengan los campos relevantes para la extracción. Para especificar los paquetes de contenido, selecciónelos en el menú desplegable Paquetes de contenido de la pestaña Análisis interactivo.

Crear paquetes de contenidos

Cualquier usuario de Log Insight puede crear un paquete de contenidos para uso privado o público.

Los paquetes de contenidos son complementos inmutables o de solo lectura para vRealize Log Insight, que proporcionan información predefinida acerca de tipos específicos de eventos, tales como los mensajes de registro. La finalidad de un paquete de contenidos es proporcionar información acerca de un conjunto específico de eventos en un formato que sea de fácil comprensión para los administradores, ingenieros, equipos de supervisión y ejecutivos.

Los paquetes de contenidos brindan información sobre el estado de mantenimiento de un producto o una aplicación. Además, un paquete de contenidos le ayuda a comprender el modo en que funciona un producto o una aplicación.

Puede guardar la información desde un paquete de contenidos usando las páginas Paneles de control o Análisis interactivo en vRealize Log Insight. La información de un paquete de contenidos incluye:

- Consultas: generalmente un paquete de contenido contiene al menos tres consultas y tres widgets de gráficos para cada panel, lo que implica más de nueve consultas en total.
- Campos: los campos pueden utilizarse de varias formas para agregaciones y filtros. Por ejemplo, las funciones y las agrupaciones se pueden aplicar a campos, y las operaciones también se pueden realizar en campos. Un campo debe incluir tantas palabras clave como sea posible para mejorar el rendimiento.
- Agregaciones
- Alertas: un paquete de contenido contiene al menos cinco alertas.
- Paneles de control: un paquete de contenido contiene al menos tres paneles de control.
- Filtros de panel de control: consulte [Capítulo 3 Buscar y filtrar eventos de registro](#).
- Visualizaciones: consulte [Capítulo 4 Uso del gráfico Análisis interactivo para analizar registros](#)
- Grupos de agentes: agentes de vRealize Log Insight que se utilizan como mecanismo de recopilación de registros.

De forma predeterminada, vRealize Log Insight incluye los paquetes de contenido VMware - vSphere, VMware - vRealize Operations Manager, VMware vSAN y General. Puede importar paquetes de contenidos adicionales si es necesario.

Términos de paquetes de contenido

El flujo de trabajo de creación de paquetes de contenido está basado en varios conceptos y términos. Debe familiarizarse con ellos para crear y mantener paquetes de contenido de manera eficaz.

Instance (Instancia)

Solamente los administradores de vRealize Log Insight pueden importar un archivo de paquete de contenido como un paquete de contenido. Si se importa un paquete de contenido como paquete de contenido, no puede editarse.

Todos los usuarios pueden importar un archivo de paquete de contenido a un espacio de usuario. Si importa un archivo de paquete de contenido a un espacio de usuario, la operación importa selectivamente los objetos en Mi contenido. Cuando importa un paquete de contenido a un espacio de usuario, puede editar los paquetes de contenido en una instancia de vRealize Log Insight. Si desea publicar o modificar un paquete de contenido, es necesario un paquete de contenido exportado.

User (Usuario)

Los paquetes de contenido se crean en parte a partir del contenido guardado en Paneles de control personalizados, también conocidos como espacio de usuario, o más específicamente Mis paneles de control o Paneles de control compartidos en la página Paneles de control. Si bien los objetos de un panel de control personalizado pueden exportarse selectivamente, se recomienda que cada paquete de contenido individual se cree por una entidad de usuario individual en vRealize Log Insight para garantizar un espacio de usuario limpio por paquete de contenido.

Para obtener información sobre cómo crear usuarios en vRealize Log Insight, consulte [Administrar cuentas de usuario de vRealize Log Insight](#).

Para obtener información sobre cómo crear usuarios en vRealize Log Insight, consulte la *Guía de administración de vRealize Log Insight*.

Use un usuario autor de paquete de contenido individual en vRealize Log Insight para cada paquete de contenido que cree.

Eventos

Es fundamental recopilar eventos relevantes antes de intentar crear un paquete de contenido para garantizar que un paquete de contenido cubra todos los eventos relevantes para un producto o una aplicación. Una forma común de recopilar eventos relevantes es preguntar a los equipos de control de calidad y soporte, dado que estos equipos por lo general tienen acceso y conocen los eventos comunes.

Los intentos de generar eventos al crear un paquete de contenido requieren mucho tiempo y generan la omisión de eventos importantes. Si los equipos de control de calidad y soporte no pueden suministrar eventos, puede simular eventos y usarlos en su lugar si los eventos de productos o aplicaciones son conocidos y están documentados.

Una vez que recopile los registros correspondientes, deben consumirse en vRealize Log Insight.

Autores

Los autores de un paquete de contenido deben tener las siguientes calificaciones:

- Experimente el uso de VMware vRealize Log Insight.

- Conocimientos operativos del mundo real del producto o de la aplicación.
- Comprensión y habilidad para generar expresiones regulares optimizadas.
- Experiencia en la depuración de diferentes problemas de productos o aplicaciones con registros.
- Experiencia en soporte, con exposición a una amplia variedad de problemas.
- Experiencia como administrador del sistema, con experiencia previa en syslog.

Flujo de trabajo

El enfoque recomendado para la creación de paquetes de contenido es comenzar en la página Análisis interactivo y comenzar las consultas de tipos específicos de eventos, tales como error o advertencia. Observe los resultados de las consultas y analice y extraiga posibles candidatos de campos según corresponda. Con algo de entendimiento de los tipos de eventos e información útil disponible en los eventos, cree y guarde consultas relevantes según corresponda. Para consultas que destacan un problema que requiere una acción rápida, cree y guarde alertas. A medida que guarde consultas, elimínelas de la lista de resultados usando un filtro para mostrar otros eventos que puedan ser posibles candidatos para nuevas consultas guardadas. Una vez que guarde todas las consultas relevantes, organícelas y muéstrelas de manera lógica en la página Paneles de control.

Consultas

Las consultas en vRealize Log Insight pueden recuperar y resumir eventos.

Puede crear y guardar consultas desde la página Análisis interactivo. Una consulta consta de al menos uno de los siguientes elementos:

Palabras clave

Coincidencias completas, de texto completo, alfanuméricas, con guion y con guion bajo.

Globs

Coincidencias completas, de texto completo, alfanuméricas, con guion y con guion bajo.

Expresiones regulares

Coincidencia de patrón de cadena sofisticado a partir de expresiones regulares de Java.

Operaciones de campo

Coincidencias de palabra clave, expresión regular y patrón aplicadas a los campos extraídos.

Incorporaciones

Funciones que se aplican a uno o más subgrupos de los resultados.

vRealize Log Insight admite los siguientes tipos de consultas:

- Mensaje. Una consulta formada por palabras clave, expresiones regulares u operaciones de campo.

- Expresión regular o campo. Una consulta formada por palabras clave o expresiones regulares.
- Agregación. Una consulta formada por una función, una o más agrupaciones y cualquier número de campos.

Es posible definir alertas personalizadas en vRealize Log Insight y activarlas desde las consultas programadas de cualquier tipo.

Prácticas recomendadas para crear consultas de mensajes

Conceptos básicos para crear consultas de mensajes.

Puede introducir consultas de mensajes usando la barra de búsqueda o aplicando filtros.

Use la barra de búsqueda para refinar los resultados para eventos en una instancia de vRealize Log Insight. Si bien puede usar un filtro en lugar de la barra de búsqueda, con frecuencia es más fácil comprender una consulta que aprovecha la barra de búsqueda que un filtro equivalente. La práctica recomendada es usar la barra de búsqueda en lugar de un filtro equivalente cuando sea posible.

Un filtro le permite crear consultas usando una expresión regular, un campo, una operación OR lógica o una combinación de una barra de búsqueda y consultas de filtro.

Cuando crea consultas usando la barra de búsqueda y filtros, se aplican las siguientes prácticas recomendadas:

- Asegúrese de que las consultas no sean específicas del entorno. Los paquetes de contenido públicos deben ser genéricos para cualquier entorno y, como tales, no deben depender de información específica del entorno. Ejemplos de información específica del entorno incluyen origen, nombre de host y potencialmente la instalación si esta usa *local*.*.
- Al crear una consulta, use palabras clave cuando sea posible; cuando las palabras clave no sean suficientes, use globs, y cuando los globs no sean suficiente, use expresiones regulares. Las consultas de palabras clave son el tipo de consulta que requiere menos recursos. Los globs son una versión simple de expresión regular y son el siguiente tipo de consulta que requiere menos recursos. Las expresiones regulares son el tipo de consulta más costoso.
- Proporcione tantas palabras clave como sea posible cuando use expresiones regulares o campos. Si una expresión regular incluye un OR lógico, por ejemplo, *this/that*, no incluya palabras clave. vRealize Log Insight está optimizado para realizar consultas de palabras clave antes que las expresiones regulares para minimizar la sobrecarga de expresiones regulares.

Consultas de campo

Los campos son una forma eficaz de añadir estructura a eventos no estructurados y permitir la manipulación de la representación textual y visual de los datos.

Los campos son uno de los elementos más importantes en un paquete de contenido, dado que pueden usarse de formas diferentes, incluidas agregaciones y filtros. Las agregaciones le permiten aplicar funciones y agrupaciones a campos. Los filtros le permiten realizar operaciones a través de campos.

Debe extraer cualquier parte de un mensaje de registro que pueda aplicarse a una consulta o agregación. Los campos son un tipo de consulta de expresión regular y son útiles para la coincidencia de patrones complejos de modo que no sea necesario conocer, recordar o conocer expresiones regulares complicadas.

Valor de contexto de campo	Definición
Regex antes del valor	Incluya tantas palabras clave como sea posible. Si este campo está vacío o solo incluye caracteres especiales, la Regex después del valor debe incluir palabras clave.
Regex después del valor	Incluya tantas palabras clave como sea posible. Si este campo está vacío o solo incluye caracteres especiales, la Regex antes del valor debe incluir palabras clave.
Nombre	Use solo caracteres alfanuméricos. Asegúrese de que todos los caracteres estén en minúscula y use guiones bajos en lugar de espacios, dado que esto facilita la visualización de los campos. Tenga en cuenta que los nombres de campos de paquetes de contenido y campos de usuario pueden ser los mismos, si bien los campos de paquetes de contenido tendrán un espacio de nombres entre paréntesis a la derecha del nombre del campo. Incluya un prefijo en los campos de paquetes de contenido con una abreviatura como, por ejemplo, vmw_, para evitar confusión.
Términos de búsqueda de palabras clave	Una o más palabras clave, separadas por espacio, que aparecen dentro de eventos que incluyen el campo.
Filter (Filtrar)	Un campo estático, operador y un valor posible que aparece dentro de eventos que contienen el campo. Es común usar esto junto con el agente de vRealize Log Insight y etiquetas para eventos que no contienen palabras clave.
Información (botón "i")	Se usa para proporcionar información sobre el campo, incluido su significado, los valores posibles que pueden devolverse y posiblemente una asignación fácil de usar de los valores para información comprensible para las personas.

Prácticas recomendadas

Además de los distintos componentes que conforman un campo, se aplican varias prácticas recomendadas.

- Solo cree campos para patrones de expresiones regulares. Si se puede consultar un campo usando consultas de palabras clave, o solo devolverá alguna vez un valor único, use consultas de palabras clave en lugar de un campo predefinido. Si un campo solo devolverá dos valores, considere la posibilidad de construir consultas individuales en lugar de extraer un campo. Los campos tienen como objetivo añadir estructura a datos no estructurados además de proporcionar una forma de consultar partes específicas de un evento.
- Solo cree campos para patrones de expresión regular que devuelvan una fracción del total de eventos. Los campos que coincidirán con la mayoría de los eventos o devolverán una gran cantidad de resultados no son buenas opciones para la extracción de campos. La expresión regular deberá aplicarse a una gran cantidad de eventos, lo que dará lugar a una operación que requiera el uso de muchos recursos. Si es posible, añada palabras clave adicionales para reducir la cantidad de resultados devueltos y optimizar la consulta.

- Si un campo incluye palabras clave dentro de la sintaxis de la expresión regular, añada estas palabras clave como filtro sin sintaxis de la expresión regular. Por ejemplo, si el valor o el contexto de un campo incluye palabras clave dentro de la sintaxis de una expresión regular, tal como *this/that*, añada las palabras clave como un filtro de texto para optimizar la consulta como **text contains this, that**.
- El uso de contexto adicional con una o más palabras clave es preferible al uso de expresiones regulares complejas en los valores de contexto previo o posterior.
- Añada contexto adicional a todos los campos extraídos a fin de optimizar el rendimiento de la consulta.

Campos temporales

Un campo temporal es un campo que existe como parte de una consulta pero que no se almacena globalmente dentro de una instancia vRealize Log Insight ni como parte de un paquete de contenido instalado.

vRealize Log Insight reduce las posibilidades de crear un campo temporal actualizando automáticamente la consulta que se basa en un campo que se está modificando.

Nota Si elimina un campo sobre el cual depende una consulta almacenada, la consulta almacenada contiene un campo temporal.

Puede ver los campos temporales cuando ejecuta una consulta almacenada en la página Análisis interactivo y un campo usando en la consulta almacenada contiene el espacio de nombres Temporal a la derecha del nombre del campo.

Las consultas tienen uno o más campos. Para las consultas de vRealize Log Insight, se modifica la definición del campo utilizada cuando se almacena una consulta si se modifica el campo. Las modificaciones del campo incluyen

- Cambiar el valor del campo
- Cambiar Regex antes del valor y Regex después del valor del campo
- Cambiar el nombre del campo
- Eliminar el campo

Cuando exporta un paquete de contenido, vRealize Log Insight convierte todos los campos temporales a los campos del paquete de contenido. Si ve un campo temporal en un paquete de contenido, es posible que esté frente a un paquete de contenido de una versión anterior del producto que se exporta con campos temporales o que el paquete de contenido se edite en forma manual.

Si existe un campo temporal con el mismo nombre que un campo extraído existente, el campo temporal que se muestra termina en {n}. Por ejemplo, si tiene un campo denominado `product_test_field`, es posible que durante la exportación también vea `product_test_field {2}`. Si ve este comportamiento, existe un campo temporal. Para tratar este tema, seleccione la opción **Seleccionar ninguno** en la parte inferior del cuadro de diálogo Exportar y seleccione cada

panel o alerta hasta que se marquen los campos extraídos con la marca final {n}. Busque los paneles y alertas y edite cada consulta. Cuando encuentre una consulta usando el campo extraído, modifique el filtro o la agregación para usar el filtro sin la terminación {n}, ejecute la consulta y guárdela. Después de completar estos pasos para todas las consultas usando un campo con la terminación {n}, el campo ya no se muestra durante la exportación.

Consultas de agregación

vRealize Log Insight le permite manipular la representación visual de los eventos usando consultas de agregación.

Las consultas de agregación están formadas por estos dos atributos:

- Funciones
- Agrupaciones

Una consulta de agregación requiere una función y al menos una agrupación. Las agrupaciones son parte importante de los paquetes de contenidos. Las funciones y las agrupaciones afectan el modo en que se visualizan los gráficos.

Las visualizaciones de los gráficos se limitan a los 2.000 resultados más recientes.

Gráficos de barras

De forma predeterminada, el gráfico de descripción general en la página Análisis interactivo de vRealize Log Insight muestra una cantidad de eventos a través del tiempo. Si utiliza la función de cantidad junto con la agrupación de series temporales, vRealize Log Insight crea un gráfico de barras.

Si utiliza la función de cantidad junto con una única agrupación de campos en vez de una serie temporal, vRealize Log Insight crea gráficos de barras con cantidades listadas de mayor a menor.

Gráficos de líneas

Todas las funciones, excepto la función de cantidad, son matemáticas. Requieren de un campo en función del cual se aplica la ecuación. Cuando se realiza una función matemática en un campo y agrupaciones por serie temporal, vRealize Log Insight crea un gráfico de líneas.

Gráficos apilados

De forma predeterminada, el gráfico de descripción general en la página Análisis interactivo de vRealize Log Insight es una cantidad de eventos a través del tiempo. Si añade un campo a la agrupación de serie temporal, entonces vRealize Log Insight crea un gráfico apilado.

Si utiliza la agrupación por serie temporal más un campo y utiliza cualquier función excepto la cantidad, vRealize Log Insight crea un gráfico de líneas apiladas. Los gráficos apilados son eficaces cuando se intenta encontrar anomalías para un objeto.

Debe decidir qué tipo de gráfico apilado utilizar basado en el número de objetos que puede devolver la consulta de agregación. Mostrar más objetos requiere de más recursos, los cuales son necesarios para analizar y mostrar información. Además, la cantidad de colores es fija, y distinguir entre objetos puede ser un desafío dependiendo de la cantidad de objetos devueltos. En general se aplican las siguientes prácticas recomendadas

- Si la cantidad de objetos devueltos en cada barra es menor de 10, es preferible usar gráficos apilados.
- Si la cantidad de objetos devueltos en cada barra está, o podría estar, entre 10 y 20, se recomienda el uso de gráficos apilados. Debe tener en cuenta el modo de representar visualmente el gráfico en un paquete de contenidos.
- Si la cantidad de objetos devueltos en cada barra es, o podría ser, mayor de 20, no se recomienda el uso de gráficos apilados.

Gráficos multicolores

Si va a crear una agrupación usando más de un campo y serie temporal, vRealize Log Insight crea un gráfico multicolor. El gráfico está compuesto por dos colores que se intercambian. Cada intercambio representa un nuevo intervalo. Los gráficos multicolores pueden ser difíciles de interpretar; por eso debe tener en cuenta el valor de dicho gráfico antes de incluirlo en un paquete de contenidos.

Cuando agrupa por campos múltiples, tenga en cuenta el uso de series no temporales. Eliminar series temporales facilita la comprensión del gráfico de barras.

Si muchos campos son importantes en un intervalo de tiempo determinado, se pueden crear múltiples gráficos para cada campo individualmente durante el intervalo de tiempo. Puede visualizar los gráficos en la misma columna de un grupo de paneles en un paquete de contenidos.

Otros gráficos

Hay otros tipos de gráficos disponibles, incluidos los gráficos circulares, de burbujas y de tablas. Para utilizarlos se requiere un tipo específico de consulta. Si está disponible la opción para estos gráficos, entonces ya posee la consulta correcta. Si no está disponible la opción para estos gráficos, pase el cursor por el nombre del gráfico que desea utilizar. Un mensaje emergente describe el tipo de consulta requerida para el tipo de gráfico.

Consultas de mensajes

Cuando se elabora una consulta de agregación, la consulta de mensaje debe devolver únicamente los resultados que sean relevantes para la consulta de agregación. Esto facilita el análisis y garantiza que los resultados muestren únicamente los campos relevantes. Para garantizar que la consulta de mensaje devuelva los mismos resultados que la consulta de agregación, debe añadir filtros usando el operador *exists* para cada campo que se utiliza en la consulta de agregación.

Cambiar el tipo de gráfico

Si desea cambiar el tipo de gráfico de un widget en un panel, haga clic en el icono de engranaje del widget y seleccione **Editar tipo de gráfico**. Si desea cambiar un tipo de widget, guarde el widget nuevo y elimine el anterior.

Alertas

Las alertas proporcionan un modo de activar una reacción cuando ocurre un determinado tipo de eventos.

vRealize Log Insight admite dos tipos de alertas

- Correo electrónico
- vRealize Operations Manager

Puede guardar alertas únicamente en el espacio de un usuario. De forma predeterminada, todas las alertas de paquetes de contenidos se deshabilitan. Si crea una alerta habilitada y la exporta como parte de un paquete de contenidos, la alerta se deshabilitará en el paquete de contenidos.

Los paquetes de contenidos no contienen parámetros de correo electrónico ni de vRealize Operations Manager. Tampoco puede añadir estos parámetros a un paquete de contenidos.

Umbrales

Los umbrales establecen un límite para la cantidad de alertas que se activan.

Es importante entender cómo funcionan los umbrales para asegurarse de que, si están habilitados, no se genere una alerta de paquete no deseada para un usuario. Cuando se considera el uso de un umbral, hay dos preguntas que deben tenerse en cuenta

- ¿Con qué frecuencia activar la alerta? Log Insight tiene frecuencias predefinidas. Las alertas solo se activan una vez para un espacio de umbral dado.
- ¿Con qué frecuencia revisar si se produjo un estado de alerta? Una alerta se activa con una consulta. Las alertas, al igual que las consultas, no son en tiempo real en la versión actual. Para cada espacio de umbral, se asigna una frecuencia de consulta predeterminada. Si se modifica el umbral, se modifica el tiempo de consulta.

Agrupaciones

Cuando cree una alerta de correo electrónico, es importante agrupar por un campo que identifique el origen de la alerta.

El correo electrónico que la alerta envía incluye una tabla de resultados para una consulta de agregación en particular. Puede ver la representación visual de la consulta en la página Análisis interactivo.

Sin un identificador único para usar como criterio de agrupación, no sabrá si el resultado es relevante para uno o más sistemas en su entorno. Debe agrupar por campo de nombre de host y no por campo de origen. También puede añadir un campo cualquiera que identifique de forma única el lugar de proveniencia del evento.

Prácticas recomendadas de paneles de control

Los paneles de control forman parte de los paquetes de contenidos. Existen algunas prácticas recomendadas que se aplican al crear paneles de control.

Al crear paneles de control, se aplican las siguientes prácticas recomendadas

- Los paquetes de contenidos generalmente contienen un mínimo de tres paneles de control. La práctica recomendada consiste en comenzar con un panel de control de generalidades que brinde información de alto nivel acerca de los eventos para un producto o aplicación en particular. Además de los paneles de control de generalidades, se deben crear paneles de control basados en las agrupaciones lógicas de los eventos. Las agrupaciones lógicas son específicas de los productos o específicas de las aplicaciones, aunque algunos enfoques comunes son el rendimiento, los errores y las auditorías. También es común crear paneles de control para un componente, como un disco o una controladora. Con el enfoque en los componentes, es importante notar que resulta efectivo únicamente si las consultas se pueden elaborar para que devuelvan resultados de componentes específicos. Si esto no es posible, se recomienda el enfoque lógico.
- Al nombrar los paneles de control, otorgue títulos genéricos y evite añadir nombres específicos a los productos o las aplicaciones a menos que se utilicen de una manera específica para los componentes. Por ejemplo, en el paquete de contenidos VMware - vSphere, hay un grupo de paneles de control llamado ESX/ESXi en vez de VMware ESX/ESXi.
- Los paneles de control deben contener un mínimo de tres widgets de paneles de control y un máximo de seis. Con menos de tres widgets de paneles de control, la cantidad de información que los paneles pueden obtener es mínima. Además, tener muchos paneles de control con solo una cantidad limitada de widgets de paneles obliga al usuario a alternar entre diferentes páginas y no proporciona información de un modo coherente.

En cambio, más de seis widgets de paneles pueden tener consecuencias negativas. Podría obtener demasiada información que podría resultar confusa. Demasiados widgets requieren del uso intensivo de los recursos del sistema, ya que cada widget es una consulta que debe ejecutarse en función del sistema.

Cuando incluye más de seis widgets de panel en los paneles, debe separar la información y crear múltiples paneles de control. Si un widget de panel se puede aplicar a uno o más paneles, cree el widget en cada panel correspondiente.

Filtros de panel de control

Los filtros de panel de control se pueden usar para obtener información detallada de eventos específicos. Los filtros funcionan de modo similar a los filtros en la página Análisis interactivo y aprovechan los campos a desglosar. Cada panel de control debe tener al menos un filtro, normalmente con el campo de nombre de host, pero se pueden añadir hasta cinco campos a cada panel.

El campo que se añade debe ser utilizado por la mayoría de los widgets en un panel determinado, de modo que, si se utiliza el filtro del panel, la mayoría de los widgets devolverán resultados. Ejemplos de filtros de panel pueden incluir un campo de gravedad, un campo de usuarios o incluso un campo de componentes.

Nota El campo y el operador usados por el filtro del panel de control se guardarán en un paquete de contenidos exportado. Cualquier valor utilizado por un filtro de panel de control no se guardará durante la exportación ya que el valor posiblemente será específico a un entorno y no genérico a todos los entornos.

Widgets de paneles de control

Los widgets de paneles de control lo ayudan a visualizar información.

Existen varios tipos de widgets en vRealize Log Insight que puede agregar a un panel de control. Entre ellos se incluyen:

- Un widget de gráficos que contiene una representación visual de los eventos con un vínculo a una consulta guardada.
- Un widget de lista de consultas que contiene vínculos de títulos a consultas guardadas.
- Un widget de tabla de campos que contiene eventos donde cada campo representa una columna.
- Un widget de la tabla de tipos de eventos simplificada que contiene eventos similares combinados en grupos simples.
- Un widget de la tabla de tendencias de eventos que muestra una lista de tipos de eventos que se encuentran en la consulta, ordenada por número de apariciones. De esta forma, se puede observar de forma rápida qué tipo de eventos aparecen con frecuencia en una consulta.

Gráfico

Un widget de gráfico de panel contiene una representación visual de eventos. Puede representar un gráfico como un gráfico de barras o de líneas, y cualquiera de ellos se puede mostrar como una pila.

Existen varias formas de representar gráficos:

- Los gráficos pueden contener mucha información. Evite tener más de dos widgets de gráfico en una misma fila. En algunos casos excepcionales, es posible utilizar tres widgets de gráfico de manera eficaz, pero es desaconsejable usar más de tres. Al determinar si los widgets de gráfico son o no legibles, asegúrese de usar la resolución mínima que admite vRealize Log Insight, que es de 1024 x 768 píxeles.
- Si cualquier fila excepto la última tiene un widget con un solo gráfico, haga que ese widget tenga el ancho completo.
- Al nombrar un widget de gráfico, use un título descriptivo y evite nombres de campo crípticos. Por ejemplo, un campo extraído se denomina `vmw_error_message`. En vez de llamar a un gráfico Cantidad de `vmw_error_message`, llámelo Cantidad de mensajes de error.

- Puede guardar gráficos similares y apilarlos en la misma columna de un grupo de paneles para comparación visual. Por ejemplo:
 - Promedio X de eventos a través del tiempo + Máximo X de eventos a través del tiempo. Según las diferentes funciones que se utilizan, el eje Y de los gráficos puede tener una escala diferente.
 - Cantidad de eventos a través del tiempo agrupados por X + cantidad de eventos a través del tiempo agrupados por Y.

Lista de consultas

Un widget de la lista de consultas del panel contiene al menos un vínculo a las consultas predefinidas.

Es posible utilizar los widgets de la lista de consultas para lo siguiente

- Cuando un widget del gráfico no proporciona un valor significativo pero la consulta subyacente sí lo hace.
- Para guardar consultas complejas como las que utilizan expresiones regulares.
- Para utilizar distintas agregaciones en una misma consulta subyacente dentro de un grupo del panel de control.

Tabla de campos

Una tabla de campos que contiene eventos donde cada campo representa una columna.

Un widget de tabla de campos del panel incluye los últimos eventos para una consulta determinada en un formato de tabla en el que cada campo representa una columna.

Puede usar un widget de tabla de campos por los siguientes motivos.

- Para ver los últimos eventos de la consulta determinada. Esto puede resultar útil para el control de cambios o por motivos de seguridad.
- Para ver solo los campos que le interesan para una consulta determinada. Esto puede resultar útil para limitar la salida de eventos.

Errores de importación de paquetes de contenidos

Cuando importe un paquete de contenidos, es posible que reciba algunas advertencias o mensajes de error.

Actualización

Es posible que reciba un mensaje de actualización. Significa que otro paquete de contenidos está instalado en el sistema que tiene el mismo espacio de nombres. En este caso, puede actualizar y reemplazar el paquete de contenidos existente o cancelar el proceso de actualización y conservar el paquete de contenidos existente.

Formato no válido

Posiblemente recibirá un mensaje que afirma que el formato no es válido. Esto significa que el archivo VLCP está editado manualmente y contiene errores de sintaxis. Los errores de sintaxis se deben reparar antes de importar el paquete de contenidos.

Versión más reciente

Este tipo de mensaje implica que el paquete de contenidos está creado y es compatible únicamente con una versión más reciente de Log Insight. En las versiones de producto posteriores a Log Insight 1.5, este tipo de mensajes significa que el archivo VLCP está editado manualmente.

Versión no reconocida

Cuando el archivo VLCP se edita manualmente y contiene errores de sintaxis, es posible que vea este tipo de mensaje. Debe reparar los errores de sintaxis antes de intentar importar el paquete de contenidos.

Nota No debe editar los archivos VLCP de forma manual. Como resultado, resulta difícil localizar y reparar los errores de sintaxis.

Requisitos para publicar paquetes de contenidos

Cuando cree y desee publicar un paquete de contenido, asegúrese de que los paquetes de contenido cumplan con los requisitos de publicación básica.

Debe revisar los requisitos del paquete de contenido y los requisitos de publicación.

Requisitos del paquete de contenido

Los paquetes de contenido deben cumplir algunos requisitos de contenido, calidad y estándares.

Los requisitos de contenido incluyen:

- Un mínimo de tres paneles
- Un mínimo de uno (en forma ideal, tres) y hasta cinco filtros de panel de control por panel de control
- Un mínimo de tres widgets de panel de control por panel de control
- Un máximo de seis widgets de panel de control por panel de control
- Un máximo de tres widgets de panel de control por fila
- Un mínimo de cinco alertas
- Un mínimo de 20 campos extraídos

Los requisitos de calidad para un paquete de contenido son los siguientes:

Alertas

Use períodos de tiempo significativos para las alertas.

Grupos de paneles de control

- Considere la opción de empezar con un grupo de paneles de control de descripción general.
- Cree grupos de paneles basados en tipos de mensaje (por ejemplo, descripción general o rendimiento) y no en tipos de componente (por ejemplo, recursos informáticos, redes o almacenamiento).
- Duplique el mismo widget de panel de control en varios grupos de paneles de control si el widget de panel de control puede aplicarse en cada grupo de paneles de control.
- Establezca como destino al menos tres grupos de paneles de control en un paquete de contenido.
- No puede reordenar los grupos de paneles de control y los widgets de panel de control, excepto con contenido de usuario.
- Al asignar nombres a grupos de paneles de control, aplique un título genérico y evite agregar nombres específicos de producto o específicos de aplicación, a menos que se utilicen de forma específica para los componentes.

Widgets de panel de control

- No ponga más de tres widgets de panel de control en la misma fila.
- Al mostrar información similar en formatos distintos, asegúrese de que cada formato aporte valor.
- Apile los paneles de control relacionados para facilitar su visualización.
- Asigne nombres descriptivos a los widgets de panel de control. No utilice nombres de campo en los títulos de los widgets.
- Asegúrese de que cada widget de panel de control contenga información o vínculos sobre lo que muestra el gráfico y el motivo de su importancia. Las notas deben responder a preguntas como: "¿Por qué es importante el widget?" y "¿Dónde se puede encontrar información adicional?".

Consultas

- Cada consulta tiene al menos una palabra clave de texto completo y, en forma ideal, tres o más palabras clave.
- Las consultas no están basadas en atributos específicos de entorno, como origen, nombre de host o instalación.
- Use expresiones regulares en las consultas solo si las palabras clave y los comodines no son suficiente. Cuando utilice expresiones regulares, proporcione tantas palabras clave como sea posible.

- Realice consultas lo más específicas posible. Las consultas de paquete de contenido solo deben coincidir con los eventos aplicables al producto o a la aplicación para los que se diseñó el paquete de contenido.

Extracción de campos

- Utilice filtros de contexto adicionales en los campos para mejorar el rendimiento del campo en las consultas.
- Cuando sea posible, reduzca al mínimo el número de expresiones regulares que se utilizan.
- Compruebe que un valor de expresión regular coincida con todos los mensajes de registro aplicables.
- Proporcione la mayor cantidad posible de contexto antes y después de las palabras clave.
- Cada campo tiene al menos una palabra clave de texto completo y, en forma ideal, tres o más palabras clave.
- Los campos son específicos de un producto o aplicación y no devuelven resultados para otros registros de producto o aplicación
- Siempre que sea posible, utilice agentes para la recopilación de registros. Utilice agentes para el análisis de campos en lugar de la extracción de campos tras el consumo.

Nomenclatura de campos

- Utilice el siguiente estándar de nomenclatura: *Prefijo_Campo_Nombre*. El prefijo debe ser aplicable al paquete de contenido.
- Utilice solo letras minúsculas.
- Use palabras clave en el contexto adicional del campo para mejorar el rendimiento del campo en las consultas.

Filtros

- Al utilizar filtros, no utilice el operador de coincidencia "any" a menos que se definan una o más palabras clave en la barra de búsqueda. "any" significa que cada filtro es una consulta independiente. Por ejemplo, cuando se utilizan tres filtros con el operador "any" en una consulta, la consulta se trata como tres consultas. Un número superior de consultas supondrá la ralentización de la obtención de resultados. Puede pensar en "any" como el operador "or", y en "all" como el operador "and".
- Cuando utilice el filtro de texto con varios valores diferentes, asegúrese de que se definan una o varias palabras clave en la barra de búsqueda.

Información del paquete de contenido

- Al exportar un paquete de contenido, utilice el formato de nomenclatura *Compañía – Producto v Versión*. Lo ideal es que el nombre del paquete de contenido tenga menos de 30 caracteres, para evitar saltos de línea.

- Al exportar con un espacio de nombres, utilice el formato de espacio de nombres *Ext.Dominio.Producto*.
- Al exportar un paquete de contenido, hágalo con una descripción detallada del producto que corrige el paquete de contenido y cómo el paquete de contenido ayuda a supervisar el producto.
- Agregue información a la sección de instrucciones de configuración de un paquete de contenido. Estas instrucciones ayudan al usuario final a configurar y utilizar el paquete de contenido.
- Agregue información a la sección de instrucciones de actualización de un paquete de contenido. Estas instrucciones ayudan al usuario final a comprender y utilizar todas las funciones de la versión actualizada del paquete de contenido.
- Proporcione información detallada sobre las versiones probadas del producto o dispositivo para el que está diseñado el paquete de contenido.
- De forma predeterminada, se asume que los paquetes de contenido son compatibles con versiones anteriores del producto o del dispositivo, y que las nuevas versiones del paquete de contenido no presentan conflictos con las configuraciones anteriores tras actualizar un paquete de contenido desde Marketplace. De lo contrario, asegúrese de proporcionar un paquete de contenido independiente.
- Al separar un paquete de contenido, asegúrese de que los paquetes de contenido tengan diferentes espacios de nombres y que no haya posibilidad de actualizar del paquete de contenido antiguo al nuevo. Además, admita el uso de soluciones antiguas y nuevas en paralelo, sin confundir a los usuarios con datos incorrectos o alertas adicionales. Agregue las excepciones a las secciones Notas de la versión y Problemas conocidos de ambos paquetes de contenido.
- Asigne un número de versión al paquete de contenido con el formato *Principal.Secundaria.Revisión*. La versión principal es para varios cambios en el paquete de contenido, por ejemplo, uno o varios paneles de control nuevos. La versión secundaria es para un pequeño cambio, como una corrección de errores, un cambio de tipo de widget o la adición de uno o dos widgets. La revisión es opcional y pueden utilizarla los autores del paquete de contenido cuando se prepara una nueva versión para enviarla a VMware con el conjunto de revisiones, pero se puede omitir después de publicar la versión finalizada. Utilice únicamente números de versión de dos dígitos para los paquetes de contenido.

Grupos de agentes

vRealize Log Insight es compatible con configuraciones reenviadas de syslog y sus propios agentes para la entrega de registros. Los paquetes de contenido diseñados para su uso con plantillas de grupos de agentes y agentes incluyen las configuraciones sugeridas. Para obtener más información, consulte las instrucciones de cada paquete de contenido.

Requisitos de publicación

Antes de publicar un paquete de contenido, revise si cumple con los requisitos de publicación. Use el publicador del paquete de contenido en Developer Center para obtener las sugerencias del paquete de contenido y para cargar una versión para revisión en VMware. <https://developercenter.vmware.com/web/loginsight>

Requisito de publicación	Descripción
Formato del archivo del paquete de contenido	Un archivo VLCP.
Eventos	Los eventos apropiados necesarios para validar el paquete de contenido.
Descripción general	Una descripción general de uno o dos párrafos del paquete de contenido.
Destacados	Tres destacados que demuestren el valor del paquete de contenido.
Descripción	Una descripción de dos a tres párrafos del paquete de contenido y de su valor.
Especificaciones técnicas	Describen los requisitos mínimos del sistema con la configuración y versiones de producto y la configuración y versión de Log Insight. Además, brinda todas las instrucciones necesarias para configurar el producto para registrar Log Insight y completar el paquete de contenido.
Capturas de pantalla	Tres o más capturas de pantalla que muestren el paquete de contenido con datos reales.
Video (opcional)	Ejemplo de cómo el paquete de contenido aporta valor.
Informe técnico (opcional)	Cómo configurar el producto o la aplicación para enviar registros a vRealize Log Insight.

Enviar paquete de contenido

Envíe el paquete de contenido que creó en VMware Solutions Exchange.

Requisitos previos

- Verifique que su paquete de contenido cumpla con [Requisitos para publicar paquetes de contenidos](#).
- Si no tiene una cuenta en <http://solutionexchange.vmware.com>, haga clic en **Registro** y seleccione **Partner**. Complete el formulario de solicitud de registro como partner y envíelo. Recibirá una notificación por correo electrónico si se aprueba su inicio de sesión.

Procedimiento

- 1 Vaya a <http://solutionexchange.vmware.com> y haga clic en **Iniciar sesión ahora** en la esquina superior derecha de la página.
- 2 Introduzca su nombre de usuario y contraseña y haga clic en **Iniciar sesión ahora**.
- 3 Haga clic en **Administración** y seleccione **Administrar soluciones** para añadir o editar una solución.

- 4 Haga clic en **Añadir solución** y complete la información requerida.

Use el botón **Guardar borrador** frecuentemente para asegurarse de no perder su trabajo.

- 5 Haga clic en **Enviar para aprobación**.

Su solución se envía al equipo VMware Solution Exchange Alliance Team para su revisión y aprobación.

Resultados

Recibirá un correo electrónico con el estado de aprobación de su solución.

Pasos siguientes

Para más información sobre cómo completar un listado de solución, haga clic en el vínculo **Sitio del partner** en la parte superior de la página. Si no encuentra la información que necesita, por cualquier pregunta, comuníquese con VSXAlliance@vmware.com.

Alias de almacén de datos a identificador de dispositivo para almacenes de datos de vSphere

vRealize Log Insight asigna los nombres de los almacenes de datos de vSphere predefinidos a los identificadores de dispositivo. Debido a esta asignación, puede utilizar nombres de almacenes de datos que sean alias para los identificadores de dispositivo en las consultas. La consulta busca mensajes con el nombre del almacén de datos o el identificador de dispositivo para el que tiene un alias asignado. vRealize Log Insight debe recibir la clave (nombre del almacén de datos) y su valor (identificador de almacén de datos) en los mensajes antes de que se pueda habilitar el alias.

Los alias se definen en el paquete de contenido (Content Pack) de VMware-vSphere. Los alias pueden ser estáticos o dinámicos.

Alias estáticos

Los alias estáticos se configuran mediante los siguientes campos:

Campo	Descripción
<i>aliasFields</i>	La asignación estática de un valor (<i>value</i>) a una clave (<i>key</i>) para un campo de búsqueda (<i>searchField</i>) determinado.
<i>name</i>	El nombre del campo de alias.
<i>searchField</i>	El nombre del campo para el que se desea un alias.
<i>value</i>	El valor de <i>searchField</i> para el que se debe encontrar la coincidencia.

Campo	Descripción
<i>key</i>	El alias que se muestra con eventos que contienen <i>searchField</i> .
<i>definition</i>	<p>Un alias estático se define de la siguiente manera:</p> <pre> "aliasFields": [{ "name": "vmw_esxi_scsi_host_status", "searchField": "vmw_esxi_scsi_host_status_label", "aliases": [{ "key": "OK", "value": "0x0"}, { "key": "NO_CONNECT", "value": "0x1"}, { "key": "BUS_BUSY", "value": "0x2"}, { "key": "TIME_OUT", "value": "0x3"}, { "key": "BAD_TARGET", "value": "0x4"}, { "key": "ABORT", "value": "0x5"}, { "key": "PARITY", "value": "0x6"}, { "key": "ERROR", "value": "0x7"}, { "key": "RESET", "value": "0x8"}, { "key": "BAD_INTR", "value": "0x9"}, { "key": "PASSTHROUGH", "value": "0xa"}, { "key": "SOFT_ERROR", "value": "0xb" }] }, { "name": "vmw_esxi_scsi_device_status", "searchField": "vmw_esxi_scsi_device_status_label", "aliases": [{ "key": "GOOD", "value": "0x0"}, { "key": "CHECK_CONDITION", "value": "0x2"}, { "key": "CONDITION_MET", "value": "0x4"}, { "key": "BUSY", "value": "0x8"}, { "key": "RESERVATION_CONFLICT", "value": "0x18"}, { "key": "TASK_SET_FULL", "value": "0x28"}, { "key": "ACA_ACTIVE", "value": "0x30"}, { "key": "TASK_ABORTED", "value": "0x40" } }, { "name": "vmw_esxi_scsi_sense_code", "searchField": "vmw_esxi_scsi_sense_label", "aliases": [{ </pre>

Campo	Descripción
	<pre> "key": "NO_SENSE", "value": "0x0"}, { "key": "RECOVERED_ERROR", "value": "0x1"}, { "key": "NOT_READY", "value": "0x2"}, { "key": "MEDIUM_ERROR", "value": "0x3"}, { "key": "HARDWARE_ERROR", "value": "0x4"}, { "key": "ILLEGAL_REQUEST", "value": "0x5"}, { "key": "UNIT_ATTENTION", "value": "0x6"}, { "key": "DATA_PROTECT", "value": "0x7"}, { "key": "BLANK_CHECK", "value": "0x8"}, { "key": "VENDOR_SPECIFIC", "value": "0x9"}, { "key": "COPY_ABORTED", "value": "0xA"}, { "key": "ABORTED_COMMAND", "value": "0xB"}, { "key": "VOLUME_OVERFLOW", "value": "0xD"}, { "key": "MISCOMPARE", "value": "0xE" } } </pre> <p>Para cada campo existente, esta definición agrega otro campo con valores que tienen nombres descriptivos:</p> <ul style="list-style-type: none"> ■ Para el campo <i>vmw_esxi_scsi_host_status</i>, la definición agrega un campo <i>vmw_esxi_scsi_host_status_label</i> con un valor que es un nombre descriptivo. Por ejemplo, un valor de campo de "0x1" para <i>vmw_esxi_scsi_host_status</i> produce un valor de "NO_CONNECT" para <i>vmw_esxi_scsi_host_status_label</i>. ■ Para el campo <i>vmw_esxi_scsi_device_status</i>, la definición agrega un campo <i>vmw_esxi_scsi_device_status_label</i> con un valor que es un nombre descriptivo. Por ejemplo, un valor de campo de "0x2" para <i>vmw_esxi_scsi_device_status</i> produce un valor de "CHECK_CONDITION" para <i>vmw_esxi_scsi_device_status_label</i>. ■ Para el campo <i>vmw_esxi_scsi_sense_code</i>, la definición agrega un campo <i>vmw_esxi_scsi_device_sense_label</i> con un valor que es un nombre descriptivo. Por ejemplo, un valor de campo de "0x3" para <i>vmw_esxi_scsi_sense_code</i> produce un valor de "MEDIUM_ERROR" para <i>vmw_esxi_scsi_device_sense_label</i>.

Alias dinámicos

Los alias dinámicos se configuran mediante los siguientes campos:

Campo	Descripción
<i>aliasRules</i>	La asignación dinámica de un campo de valor (<i>valueField</i>) a un campo de clave (<i>keyField</i>) para campos asociados (<i>associatedFields</i>).
<i>name</i>	Un nombre único para identificar el alias (solo interno).
<i>keyField</i>	El campo al que se debe asignar un alias dinámico.
<i>valueField</i>	Un segundo campo en el mismo evento que el campo <i>keyField</i> que proporciona el valor de alias.
<i>aliasFieldName</i>	El nombre del campo de alias que se mostrará junto a los eventos que contienen <i>keyField</i> .

Campo	Descripción
<i>associatedFields</i>	El campo o los campos para los que debe aparecer <i>aliasFieldName</i> .
<i>definition</i>	<p>Un alias dinámico se define de la siguiente manera:</p> <pre> "aliasRules": [{ "name": "DatastoreFromVmFileSystem", "filter": "hostd VmFileSystem Label headExtent naa*", "keyField": "vmw_esxi_device_id", "valueField": "vmw_esxi_vmfs_label", "aliasFieldName": "vmw_esxi_vmfs_name", "associatedFields": ["vmw_esxi_device_id"] }, { "name": "DatastoreFromScsiCorrelator", "filter": "scsiCorrelator storage Datastores naa*", "keyField": "vmw_esxi_device_id", "valueField": "vmw_esxi_datastore", "aliasFieldName": "vmw_esxi_datastore_name", "associatedFields": ["vmw_esxi_device_id"] }] </pre> <p>Para que los campos de alias dinámico funcionen, vRealize Log Insight requiere que se registren mensajes específicos para crear los alias.</p> <ul style="list-style-type: none"> ■ Para que el campo <i>vmw_esxi_vmfs_name</i> funcione correctamente, vRealize Log Insight primero debe recibir un mensaje de registro similar al siguiente: <pre> 016-10-22T00:50:00.042Z host001.corp.local Hostd: info hostd[5179FB70] [Originator@6876 sub=Libs] VmFileSystem: uuid:57925c06-0a8a627e-9f0b- b82a72d50b06, Label:datastore001,logicalDevice:57925c05 -63b188db-37da-b82a72d50b06, headExtent:naa.6b083fe0c212bd001f22e05d07 099022:1 </pre> <p>La consulta utilizada para encontrar la coincidencia con este evento es <code>hostd VmFileSystem Label headExtent naa*</code>. Para cada valor del campo <i>vmw_esxi_device_id</i> encontrado, vRealize Log Insight asigna el valor del campo <i>vmw_esxi_vmfs_label</i> al campo <i>vmw_esxi_vmfs_name</i>. En este ejemplo, el campo <i>vmw_esxi_device_id</i> es "naa.6b083fe0c212bd001f22e05d07099022" y el campo <i>vmw_esxi_vmfs_label</i> es "datastore001". Tras registrarse este evento, la ejecución de una consulta con un filtro en el</p>

Campo	Descripción
	<p>cual el campo <code>vmw_esxi_vmfs_name</code> contiene un nombre de almacén de datos devuelve los mensajes de registro que contienen "naa.6b083fe0c212bd001f22e05d07099022".</p> <ul style="list-style-type: none"> ■ Para que el campo <code>vmw_esxi_datastore_name</code> funcione correctamente, vRealize Log Insight primero debe recibir un mensaje de registro similar al siguiente: <pre>2016-11-24T03:56:47.738Z host002.corp.local vobd: [scsiCorrelator] 4851129307827us: [esx.clear.storage.redundancy.restored] Path redundancy to storage device naa.6006016006502a004b1c42e756fbe411 (Datastores: "datastore002") restored. Path vmhba39:C0:T1:L2 is active again.</pre> <p>La consulta utilizada para encontrar la coincidencia con este evento es <code>scsiCorrelator storage Datastores naa*</code>. Para cada valor único que se encuentre en el campo <code>vmw_esxi_device_id</code>, vRealize Log Insight asigna el valor del campo <code>vmw_esxi_datastore</code> al campo <code>vmw_esxi_datastore_name</code>. En este ejemplo, el campo <code>vmw_esxi_device_id</code> es "naa.6006016006502a004b1c42e756fbe411" y el campo <code>vmw_esxi_datastore</code> es "datastore002". Tras registrarse este evento, la ejecución de una consulta con un filtro en el cual el campo <code>vmw_esxi_datastore_name</code> contiene un nombre de almacén de datos devuelve los mensajes de registro que contienen "naa.6006016006502a004b1c42e756fbe411".</p>

Requisitos para los alias

Para utilizar alias, asegúrese de que:

- Está utilizando vRealize Log Insight 4.0 o una versión posterior.
- Está utilizando el paquete de contenido (Content Pack) 4.0 de VMware - vSphere o una versión posterior. vRealize Log Insight incluye este paquete de contenido.
- ESXi está configurado para enviar registros a vRealize Log Insight.
- Hay un intervalo mínimo de cinco minutos después de que el primer evento que contiene la clave y el valor pase por la canalización de consumo.

Restricciones para los alias

Se aplican las siguientes restricciones al uso de alias:

- No puede utilizar alias con funciones matemáticas, por ejemplo, avg, min, max, etc.

- No puede utilizar alias con los operadores "exist" y "does not exist".
- Los alias no se reenvían como parte del reenvío de eventos.
- Se pueden aprender hasta 100.000 alias por nodo, tras lo cual se rotan al estilo FIFO.

Consultas de alerta en vRealize Log Insight

9

Puede configurar vRealize Log Insight para que ejecute consultas específicas a intervalos programados.

Si la cantidad de eventos que coinciden con la consulta supera los valores umbral que ha establecido, vRealize Log Insight puede enviar notificaciones por correo electrónico o de webhook y activar eventos de notificación en vRealize Operations Manager.

Para ver la lista de alertas disponibles, desplácese hasta la página Análisis interactivo y seleccione **Administrar alertas...** en el menú desplegable **Crear y administrar alertas...** que está junto al campo **Buscar**. El estado de cada alerta aparecerá bajo el nombre de la alerta.

Nota Las consultas de alerta son específicas para el usuario. El usuario solo puede administrar sus propias alertas. Debe tener asignada un rol de superadministrador para poder administrar las alertas de otros usuarios.

Tipos de alertas que puede crear en vRealize Log Insight

Puede controlar los intervalos a los que se ejecutan las consultas de alerta, y las condiciones cuando vRealize Log Insight envía notificaciones de alerta seleccionando uno de los tipos de alerta.

Alerta para cualquier coincidencia

La consulta de alerta se ejecuta automáticamente cada cinco minutos. Una notificación se activa cuando al menos un evento dentro de los últimos 5 minutos coincide con la consulta.

Alerta basada en Tipos de eventos

La consulta de alerta se ejecuta automáticamente cada cinco minutos. Se activa una notificación cuando aparece un tipo de evento especificado.

Alerta basada en cantidad de eventos dentro de un período de tiempo personalizado

Los intervalos de consulta de alerta dependen de los parámetros que configure. Una notificación se activa de acuerdo con los parámetros cuando ocurren más o menos de *X* eventos coincidentes en los últimos *Y* minutos.

Si se activa este tipo de alerta, esta se repite por la duración de su intervalo de tiempo para evitar que se emitan alertas duplicadas para los mismos grupos de eventos. Si desea habilitar una alerta mientras se está repitiendo, puede deshabilitarla y luego volver a habilitarla.

Alertas basadas en consultas de agregación

La alerta de consultas de agregación activa una notificación si un valor de una función que se encuentre en una agrupación supera un valor que defina. Esto se puede ver en un gráfico donde al menos una de sus barras esté por encima o por debajo del valor umbral establecido dentro de un periodo especificado.

Este tipo de alerta se puede configurar para los gráficos que no visualizan **Cantidad de eventos a través del tiempo**.

Alertas de paquetes de contenidos

Los paquetes de contenidos pueden contener consultas de alertas. El paquete de contenidos vSphere que se incluye en vRealize Log Insight de forma predeterminada contiene varias consultas de alerta predefinidas. Pueden activar alertas si un host ESXi deja de enviar datos de syslog, si vRealize Log Insight ya no puede recopilar datos de eventos, tareas y alarmas desde un vCenter Server, o cuando el estado de una alarma cambia a rojo. Puede utilizar estas consultas de alerta como plantillas para crear alertas que sean específicas a su entorno.

Todas las alertas de paquetes de contenidos se deshabilitan de forma predeterminada.

Habilitar la alerta **vCenter Server: ESX/ESXi dejó de registrar** constituye una buena práctica, porque determinadas versiones de hosts ESXi podrían dejar de enviar datos de syslog al reiniciar vRealize Log Insight. Esta alerta supervisa que el evento vCenter Server `esx.problem.vmsyslogd.remote.failure` detecte si hay un host ESXi que dejó de enviar feeds de syslog. Para conocer detalles acerca de problemas y soluciones de syslog, consulte [Host VMware ESXi 5.x deja de enviar syslogs al servidor remoto \(2003127\)](#).

Puede añadir el siguiente filtro a la consulta de alerta y guardarlo como una alerta nueva para detectar únicamente los hosts ESXi que dejen de enviar feeds a su instancia de vRealize Log Insight: **vc_remote_host (VMware - vSphere)contains***nombre-de-host-log-insight*.

Las consultas de alerta del paquete de contenido son de solo lectura. Para guardar los cambios efectuados en una alerta del paquete de contenido, debe guardar la alerta en su contenido personalizado.

- [Definir una consulta de alerta](#)

Puede definir una consulta de alerta en vRealize Log Insight y enviar notificaciones por correo electrónico o enlace web si el número de eventos que coinciden con la consulta supera los umbrales establecidos.

- [Agregar una consulta de alerta para enviar notificaciones por correo electrónico](#)

Puede configurar las consultas de alerta en vRealize Log Insight para que envíen notificaciones por correo electrónico cuando aparecen datos específicos en los registros.

- [Acerca de usar webhooks para enviar alertas a productos de terceros](#)
Puede enviar alertas de usuario de vRealize Log Insight a productos de terceros usando webhooks.
- [Agregar una consulta de alerta para enviar notificaciones a vRealize Operations Manager](#)
Puede configurar consultas de alerta en vRealize Log Insight para enviar eventos de notificación a vRealize Operations Manager cuando las consultas de vRealize Log Insight específicas devuelven resultados que superan un umbral determinado.
- [Ver consultas de alerta](#)
Puede visualizar las consultas de alerta que ha creado y revisar si están habilitadas las notificaciones para estas consultas.
- [Modificar consultas de alerta](#)
Puede cambiar la activación de consultas de alerta, habilitar o deshabilitar las notificaciones que envía una consulta, o cambiar el método de notificación (correo electrónico, webhook o envío a vRealize Operations Manager).
- [Habilitar consultas de alerta](#)
Cuando se deshabilita una consulta de alerta, vRealize Log Insight no envía notificaciones por correo electrónico ni de webhooks, y no activa eventos de notificaciones de vRealize Operations Manager.
- [Eliminar consultas de alerta](#)
Puede eliminar consultas de alerta cuando ya no las necesite.


Definir una consulta de alerta

Puede definir una consulta de alerta en vRealize Log Insight y enviar notificaciones por correo electrónico o enlace web si el número de eventos que coinciden con la consulta supera los umbrales establecidos.

Requisitos previos

- Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.
- Verifique que un administrador haya configurado el SMTP para habilitar las notificaciones por correo electrónico. Vea [Configurar el servidor SMTP para Log Insight](#).

Procedimiento

- 1 En la pestaña **Análisis interactivo**, ejecute la consulta para la que desea enviar notificaciones.
- 2 A la derecha del botón **Buscar**, haga clic en  y seleccione **Crear alerta a partir de la consulta**.
- 3 En el cuadro de diálogo Nueva alerta, introduzca un nombre para la alerta.

- 4 Opcionalmente, introduzca una breve descripción significativa del evento que activa la alerta. Esta descripción se incluye en el mensaje de notificación enviado para la alerta.
- 5 Opcionalmente, introduzca una recomendación para la alerta. Esta recomendación se incluye en el mensaje de notificación enviado para la alerta.
- 6 Seleccione el tipo de notificación que desea enviar para la alerta y configúrela. Para obtener más información, consulte los temas siguientes:
 - [Agregar una consulta de alerta para enviar notificaciones por correo electrónico](#)
 - [Agregar una consulta de alerta para enviar notificaciones de webhook](#)
- 7 Configure el umbral de alerta.

Alert Type (Tipo de alerta)	Selección
En cualquier coincidencia	<p>Seleccione la primera opción.</p> <p>Las consultas se ejecutan cada cinco minutos.</p> <p>Esta opción está disponible para todos los tipos de consultas. El contenido de la alerta contiene una lista de los primeros 10 eventos que coinciden con la consulta de alerta.</p>
Según el tipo de evento	<p>Seleccione la segunda opción y seleccione una hora en el menú desplegable.</p> <p>Las consultas se ejecutan cada cinco minutos.</p> <p>Esta opción está disponible para todos los tipos de consultas. El contenido de la alerta contiene una lista de los primeros 10 eventos que coinciden con la consulta de alerta.</p>
Según la cantidad de eventos dentro de un período	<p>Seleccione la tercera opción y utilice los menús desplegables para establecer los parámetros.</p> <p>Las consultas se ejecutan según la selección efectuada en el menú desplegable.</p> <p>Esta opción está disponible para todos los tipos de consultas. El contenido de la alerta contiene una lista de los primeros 10 eventos que coinciden con la consulta de alerta.</p>
A partir de los valores del gráfico	<p>Seleccione la cuarta opción y utilice los menús desplegables para configurar los parámetros.</p> <p>Las consultas se ejecutan en función a la selección efectuada en el segundo menú desplegable.</p> <p>Nota Este tipo de alerta solo está disponible cuando se utiliza una Función de agregación.</p> <p>El contenido de la alerta tiene una tabla con los 10 grupos principales que coinciden con la consulta de alerta.</p>

La línea naranja del gráfico de vista previa muestra el umbral actual.

- 8 Haga clic en **Guardar**.

Pasos siguientes

Puede habilitar, deshabilitar o eliminar sus alertas almacenadas.

Nota Las consultas de alerta son específicas para el usuario. El usuario solo puede administrar sus propias alertas. Debe tener asignada un rol de superadministrador para poder administrar las alertas de otros usuarios.


Agregar una consulta de alerta para enviar notificaciones por correo electrónico

Puede configurar las consultas de alerta en vRealize Log Insight para que envíen notificaciones por correo electrónico cuando aparecen datos específicos en los registros.

Requisitos previos

- Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.
- Verifique que un administrador haya configurado el SMTP para habilitar las notificaciones por correo electrónico. Vea [Configurar el servidor SMTP para Log Insight](#).

Procedimiento

- 1 En la pestaña **Análisis interactivo**, ejecute la consulta para la que desea enviar notificaciones.
- 2 A la derecha del botón **Buscar**, haga clic en  y seleccione **Crear alerta a partir de la consulta**.
- 3 En el cuadro de diálogo **Añadir**, escriba un nombre para la alerta y proporcione una descripción breve y significativa del evento que activa la alerta.

El nombre y la descripción de la alerta se incluyen en el correo electrónico que envía vRealize Log Insight.
- 4 Marque la casilla de verificación **Correo electrónico** y escriba la dirección de correo electrónico a donde desea enviar las notificaciones de vRealize Log Insight.

Use comas para separar varias direcciones.
- 5 Establezca el umbral de alerta como se describe en [Definir una consulta de alerta](#).
- 6 Haga clic en **Guardar**.

Pasos siguientes

Puede habilitar, deshabilitar o eliminar sus alertas almacenadas.

Nota Las consultas de alerta son específicas para el usuario. El usuario solo puede administrar sus propias alertas. Debe tener asignada un rol de superadministrador para poder administrar las alertas de otros usuarios.

Acerca de usar webhooks para enviar alertas a productos de terceros

Puede enviar alertas de usuario de vRealize Log Insight a productos de terceros usando webhooks.

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

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

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

La implementación de webhooks de vRealize Log Insight hace solicitudes HTTP salientes a un servidor remoto. El servidor puede notificar que se ha realizado correctamente o que se produjo un error. vRealize Log Insight vuelve a intentar las solicitudes fallidas. Todas las respuestas de código de estado HTTP/2xx se consideran correctas, mientras que las demás respuestas (incluido si se agota el tiempo de espera o si la conexión se rechaza) se consideran errores que se volverán a intentar más tarde.

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

Agregar una consulta de alerta para enviar notificaciones de webhook

Puede configurar las consultas de alerta en vRealize Log Insight para que envíen notificaciones de webhook a un servidor web remoto cuando aparezcan datos específicos en los registros. Los webhooks proporcionan notificaciones de eventos por medio de HTTP POST.


El contenido de la notificación de webhook contiene un máximo de 10 eventos que cumplen los criterios de alerta. En las consultas agregadas, el contenido contiene un máximo de 10 grupos que cumplen los criterios de alerta. El contenido contiene el número total de eventos y grupos, así como un vínculo a la página Análisis interactivo. En esta página se muestran todos los eventos o grupos de eventos.

Nota El servidor puede notificar un resultado correcto o un error. vRealize Log Insight lo volverá a intentar en caso de error. vRealize Log Insight trata a todas las respuestas del código de estado HTTP/2xx como correctas. El resto de respuestas (incluido si se agota el tiempo de espera o si la conexión se rechaza) se tratan como errores que se volverán a intentar más tarde.

Requisitos previos

- Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.
- Verifique que el servidor web se configuró para recibir notificaciones de webhook.

Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.
- 2 A la derecha del botón **Buscar**, haga clic en  y seleccione **Crear alerta a partir de la consulta**.
- 3 En el cuadro de diálogo **Añadir**, escriba un nombre para la alerta y proporcione una descripción breve y significativa del evento que activa la alerta.

El nombre y la descripción de la alerta se incluyen en la notificación que envía vRealize Log Insight.
- 4 Marque la casilla de verificación **Webhooks** y escriba la URL a la cual desea enviar las notificaciones de vRealize Log Insight.
- 5 Establezca el umbral de alerta como se describe en [Definir una consulta de alerta](#).
- 6 Haga clic en **Guardar**.

Pasos siguientes

Puede habilitar, deshabilitar o eliminar sus alertas almacenadas.

Nota Las consultas de alerta son específicas para el usuario. El usuario solo puede administrar sus propias alertas. Debe tener asignada un rol de superadministrador para poder administrar las alertas de otros usuarios.

Acerca de Escribir shims de traducción para alertas de vRealize Log Insight

Se usan shims para asignar formatos de webhook que varían.

vRealize Log Insight envía un webhook en su propio formato de propiedad exclusiva y las soluciones de terceros esperan que los webhooks entrantes usen sus propios formatos de propiedad exclusiva. Esto supone que cada solución de terceros debe tener soporte nativo para el formato vRealize Log Insight o que es necesario un shim entre vRealize Log Insight y la solución para convertir el formato vRealize Log Insight al formato de terceros.

Las siguientes imágenes muestran una consulta de alerta de usuario y el webhook que se genera para ella. Puede usar esta información para entender la asignación que es necesaria para los shims de compatibilidad.

Figura 9-1. Consulta de alerta definida por el usuario

The screenshot shows the search bar with the following configuration:

- Count of events + over time grouped by hostname
- Buttons: Apply, Reset
- Search filters: appname contains vpxa
- Buttons: + Add Filter, X Clear All Filters

Figura 9-2. Salida de webhook para la consulta de agregación de alerta de usuario

```
{
  "AlertType":1,
  "AlertName":"ESXi Vpxa Alert",
  "SearchPeriod":300000,
  "HitCount":0.0,
  "HitOperator":2,
  "messages":[
    {
      "text":"2016-06-24T15:42:42.055Z esx01 Vpxa: [4845FB90 verbose 'VpxaHalCnxHostagent'
opID=WFU-dcfc2d3a] [WaitForUpdatesDone] Starting next WaitForUpdates() call to hostd",
      "timestamp":1451940578545,
      "fields":[
        {
          "name":"hostname",
          "content":"esx01"
        },
        {
          "name":"appname",
          "content":"vpxa"
        }
      ]
    },
    {
      "text":"2016-06-24T15:42:42.055Z esx02 Vpxa: [4845FB90 verbose 'vpxavpxaInvtVm'
opID=WFU-dcfc2d3a] [VpxaInvtVmChangeListener] Guest DiskInfo Changed",
      "timestamp":1451940561008,
      "fields":[
        {
          "name":"hostname",
          "content":"esx02"
        },
        {
          "name":"appname",
          "content":"vpxa"
        }
      ]
    }
  ],
  "HasMoreResults":false,
}
```

```

    "Url":"https://10.11.12.13/s/8pgzq6",
    "EditUrl":"https://10.11.12.13/s/56monr",
    "Info":"This is an alert for all the 'ESXi Vpxa' messages",
    "NumHits":2
  }

```

Formato de webhook para consultas de mensaje de alerta de usuario

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

Si envía una alerta generada por una consulta de mensaje de alerta de usuario a un programa de terceros, debe escribir un shim para que los formatos de dicho programa puedan comprender la información de vRealize Log Insight.

Formato de webhook para las consultas de mensaje de alerta de usuario

El siguiente ejemplo muestra el formato de un webhook de vRealize Log Insight para una consulta de mensaje de alerta de usuario.

```

{
  "AlertType":1,
  "AlertName":"Hello World Alert",
  "SearchPeriod":300000,
  "HitCount":0.0,
  "HitOperator":2,
  "messages":[
    {
      "text":"hello world 1",
      "timestamp":1451940578545,
      "fields":[
        {
          "name":"Field_1",
          "content":"Content 1"
        },
        {
          "name":"Field_2",
          "content":"Content 2"
        }
      ]
    },
    {
      "text":"hello world 2",
      "timestamp":1451940561008,
      "fields":[
        {
          "name":"Field_1",
          "content":"Content 1_2"
        },
        {
          "name":"Field_2",
          "content":"Content 2_2"
        }
      ]
    }
  ]
}

```

```

    ]
  }
],
"HasMoreResults":false,
"Url":"https://10.11.12.13/s/8pgzq6",
"EditUrl":"https://10.11.12.13/s/56monr",
"Info":"This is an alert for all the 'Hello World' messages",
"NumHits":2
}

```

Formato de webhook para una consulta de agregación de alerta de usuario

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

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

Formato de webhook para consultas de agregación de alerta de usuario

```

{
  "AlertType":2,
  "AlertName":"field_1 aggregated alert",
  "SearchPeriod":300000,
  "HitCount":2.0,
  "HitOperator":2,
  "messages":[
    {
      "fields":[
        {
          "name":"Field_1",
          "content":"Content 1"
        }
      ]
    }
  ],
  "HasMoreResults":false,
  "Url":"https://10.11.12.13/s/r25g3s",
  "EditUrl":"https://10.11.12.13/s/n3gsed",
  "Info":null,
  "NumHits":1
}

```

Agregar una consulta de alerta para enviar notificaciones a vRealize Operations Manager

Puede configurar consultas de alerta en vRealize Log Insight para enviar eventos de notificación a vRealize Operations Manager cuando las consultas de vRealize Log Insight específicas devuelven resultados que superan un umbral determinado.


Los eventos de notificación que vRealize Log Insight genera se asocian con recursos en vRealize Operations Manager. Puede consultar más información acerca de los recursos en la *Guía de inicio de vRealize Operations Manager (UI personalizada)*.

Nota Se requieren varios minutos para que los eventos de notificación aparezcan en la interfaz de usuario de vRealize Operations Manager.

Requisitos previos

- Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde *host-log_insight* es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.
- Verifique que un administrador haya configurado la conexión entre vRealize Log Insight y vRealize Operations Manager para habilitar la integración de alertas. Consulte [Configurar Log Insight para enviar eventos de notificación a vRealize Operations Manager](#).

Procedimiento

- 1 En la pestaña **Análisis interactivo**, ejecute la consulta para la que desea enviar notificaciones.
- 2 A la derecha del botón **Buscar**, haga clic en  y seleccione **Crear alerta a partir de la consulta**.
- 3 En el cuadro de diálogo Añadir, escriba un nombre para la alerta y proporcione una descripción breve y significativa del evento que activa la alerta.

El nombre y la descripción de la alerta se incluyen en el evento de notificación que envía vRealize Log Insight.
- 4 Anule la selección de la opción **Correo electrónico**. Para recibir las notificaciones por correo electrónico, proporcione al menos una dirección de correo electrónico.

Use comas para separar varias direcciones.
- 5 Seleccione **Enviar a vRealize Operations Manager**.

6 Proporcione un objeto de reserva.

Cuando se integran con vRealize Operations Manager 6.0 y superiores, las alertas se envían como notificaciones a las máquinas virtuales, los hosts ESX o los objetos de vCenter Server que causaron la alerta. Las alertas emitidas por otras entidades se envían al objeto de reserva seleccionado.

- a Haga clic en **Seleccionar**.
- b En el cuadro de diálogo Seleccionar objeto de conmutación, introduzca un nombre de recurso o desplácese por un objeto de la lista.

Opción	Descripción
Objetos activos	Seleccione para ver únicamente los recursos que están conectados.
Todos los objetos	Seleccione para ver todos los recursos, independientemente de su estado de energía.

- 7 (opcional) En el menú desplegable **Criticidad**, seleccione el nivel de criticidad para los eventos de notificación que aparecen en la interfaz de usuario personalizada de vRealize Operations Manager.
- 8 (opcional) Para cancelar la alerta en vRealize Operations Manager si no se ha activado dentro de un período determinado, active la casilla **Cancelación automática** e introduzca el período de cancelación.
- 9 Establezca el umbral de alerta como se describe en [Definir una consulta de alerta](#).
- 10 Haga clic en **Guardar**.

Resultados

Cuando la consulta de alerta devuelve resultados que coinciden con los criterios de alerta, se envía un evento de notificación a vRealize Operations Manager. Las consultas de alerta se ejecutan en un calendario predefinido y se activan solo una vez para un intervalo de umbral determinado.

Las ubicaciones de los eventos de notificación dependen de la versión de la interfaz de usuario de vRealize Operations Manager que use. Consulte [Eventos de notificación de Log Insight en vRealize Operations Manager](#).

Ejemplo: Configure una alerta de notificación para vRealize Operations Manager

Supongamos que en vRealize Operations Manager, tiene un recurso de máquina virtual llamado *vm-abc*.

Ha configurado vRealize Log Insight para extraer eventos del sistema vCenter Server donde se ejecuta la máquina virtual *vm-abc*.

Usted desea recibir una notificación en vRealize Operations Manager cada vez que la máquina virtual *vm-abc* se apaga.

Este es el modo de configurar vRealize Log Insight para que envíe estos eventos de notificación a vRealize Operations Manager.

- 1 En el cuadro de texto de búsqueda, escriba **Apagar máquina virtual**.
- 2 Haga clic en **Añadir un filtro**, seleccione **vc_vm_name** y escriba **vm-abc**.
- 3 Haga clic en **Buscar**.
Si la máquina virtual *vm-abc* se apagó durante el intervalo seleccionado, la búsqueda devolverá todas las instancias que ocurrieron.
- 4 En el menú desplegable a la derecha del botón **Buscar**, seleccione **Añadir alerta**.
- 5 En el cuadro de diálogo Añadir alerta, escriba un nombre y una descripción para la alerta, desmarque la opción **Correo electrónico** y seleccione **Enviar a vRealize Operations Manager**.
- 6 Haga clic en **Seleccionar**, escriba **vm-abc** y haga clic en **Buscar** para encontrar el recurso *vm-abc* en la lista.
- 7 Haga clic en el recurso *vm-abc* de la lista para añadirlo.
- 8 (opcional) Modifique el nivel de criticidad que aparece en la interfaz de usuario personalizada de vRealize Operations Manager.
- 9 (opcional) Seleccione una configuración de cancelación automática y el período de cancelación.
- 10 En **Emitir una alerta**, seleccione **en cualquier coincidencia**.
- 11 Haga clic en **Guardar**.

vRealize Log Insight sondea el sistema vCenter Server a intervalos de cinco minutos. Si la consulta devuelve una nueva tarea de apagar la máquina virtual desde la máquina virtual *vm-abc*, vRealize Log Insight envía un evento de notificación que está asociado con el recurso *vm-abc* en vRealize Operations Manager.

Pasos siguientes

Puede habilitar, deshabilitar o eliminar sus alertas almacenadas.

Nota Las consultas de alerta son específicas para el usuario. El usuario solo puede administrar sus propias alertas. Debe tener asignada un rol de superadministrador para poder administrar las alertas de otros usuarios.

Ver consultas de alerta

Puede visualizar las consultas de alerta que ha creado y revisar si están habilitadas las notificaciones para estas consultas.

Utilice la ventana **Alertas de usuario** como punto de partida para ver y administrar las alertas que creó como usuario. En esta ventana, puede supervisar la actividad de las alertas y ver el historial de alertas, así como administrarlas. Puede realizar las siguientes tareas:

- Activar o desactivar alertas individuales o todas las alertas
- Ordenar las alertas por nombre, nombre de propietario o paquete de contenido
- Cambiar los parámetro de una alerta
- Eliminar una alerta

Utilice la información sobre herramientas para saber más sobre cada icono que aparece en la pantalla.

Nota Las consultas de alerta son específicas para el usuario. El usuario solo puede administrar sus propias alertas. Debe tener asignada un rol de superadministrador para poder administrar las alertas de otros usuarios.

Figura 9-3. Alertas de usuario

Name	Enabled	Owner	Avg Run	Frequency	Dally Run	Last Hit	Last Run	Ne
test_		admin	84ms	288/day	24s	1mo 11d ago	9d 6h ago	

El valor de la columna Último acierto se mantiene como never hasta que se produzca el primer acierto.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 Haga clic en el icono del menú desplegable de la configuración y seleccione **Administración**.
- 2 En la sección Administración del menú de la izquierda, haga clic en **Alertas de usuario**.

Resultados

Se ve una lista de todas las consultas de alerta. Se muestra el estado de las notificaciones de alerta debajo del nombre de la alerta.

Pasos siguientes

Puede hacer clic en las consultas de alerta en la lista para modificar sus parámetros o puede eliminar las consultas que ya no necesite.

Las consultas de alerta del paquete de contenido son de solo lectura. Para guardar los cambios efectuados en una alerta del paquete de contenido, debe guardar la alerta en su contenido personalizado.

Modificar consultas de alerta

Puede cambiar la activación de consultas de alerta, habilitar o deshabilitar las notificaciones que envía una consulta, o cambiar el método de notificación (correo electrónico, webhook o envío a vRealize Operations Manager).

Nota Las consultas de alerta son específicas para el usuario. El usuario solo puede administrar sus propias alertas. Debe tener asignada un rol de superadministrador para poder administrar las alertas de otros usuarios.


Las consultas de alerta del paquete de contenido son de solo lectura. Para guardar los cambios efectuados en una alerta del paquete de contenido, debe guardar la alerta en su contenido personalizado.

Puede aplicar los cambios a una o más alertas al mismo tiempo.

Requisitos previos

- Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.
- Verifique que un administrador haya configurado el SMTP para habilitar las notificaciones por correo electrónico. Vea [Configurar el servidor SMTP para Log Insight](#).
- Verifique que un administrador haya configurado la conexión entre vRealize Log Insight y vRealize Operations Manager para habilitar la integración de alertas. Consulte [Configurar Log Insight para enviar eventos de notificación a vRealize Operations Manager](#).
- Si utiliza webhooks, verifique que el servidor web se haya configurado para recibir notificaciones de webhook.

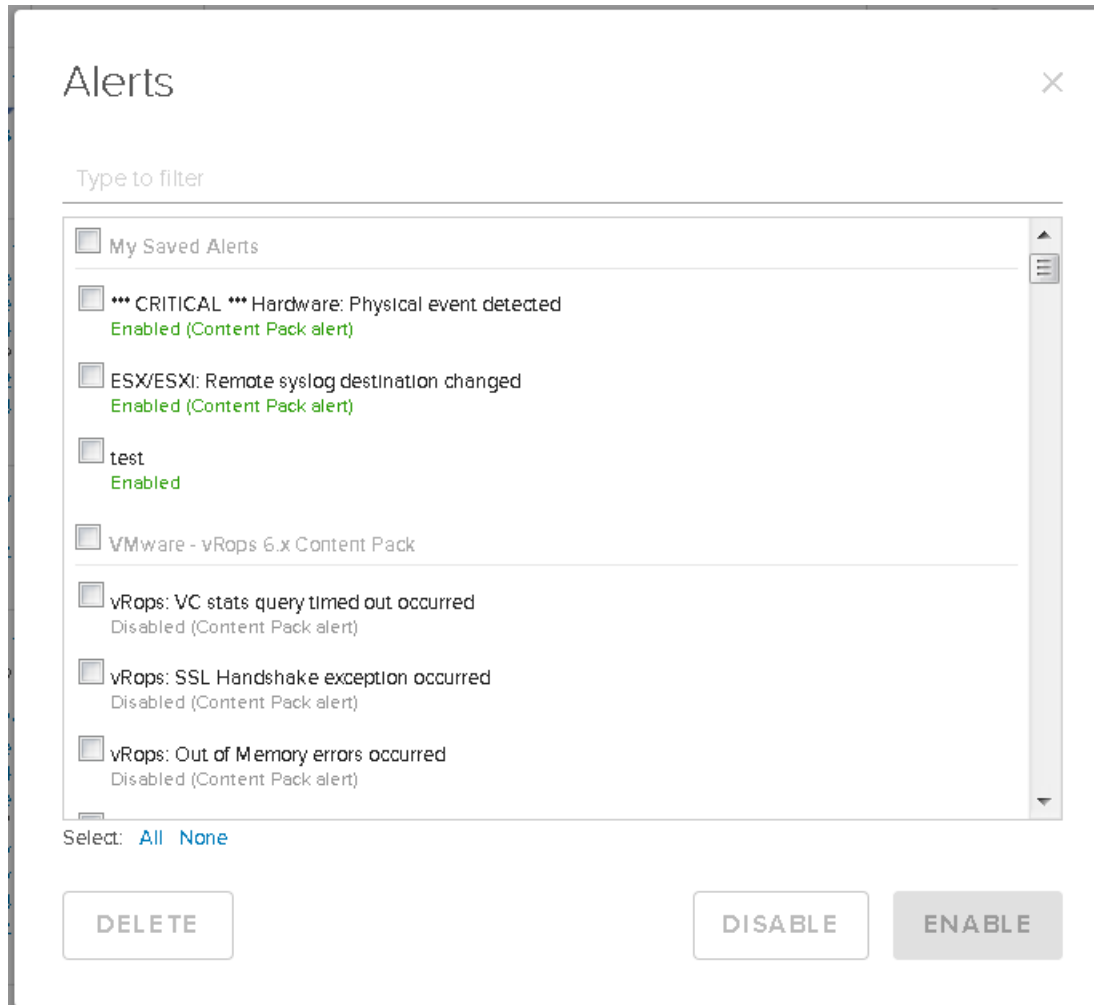
Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.
- 2 En el menú **Crear o administrar alertas**, situado a la derecha del botón **Buscar**, haga clic en  y seleccione **Administrar alertas**.

- En la lista de alertas, seleccione una o varias consultas de alerta que desee modificar y cambie los parámetros de consulta según sea necesario.

Puede encontrar consultas introduciendo una cadena como filtro. Las consultas están etiquetadas como habilitadas o deshabilitadas y se especifica si forman parte de una consulta de paquete de contenido.

Nota Si anula la selección de todas las opciones de notificación, se deshabilita la consulta de alerta.



- Guarde sus cambios.

Opción	Descripción
Guardar	Este botón se muestra cuando modifica sus propias alertas.
Guardar en Mis alertas	Este botón se muestra cuando modifica una alerta compartida o una alerta de paquete de contenido. La alerta original permanece sin cambios, pero guarda una copia de la alerta en su contenido personalizado.

Habilitar consultas de alerta

Cuando se deshabilita una consulta de alerta, vRealize Log Insight no envía notificaciones por correo electrónico ni de webhooks, y no activa eventos de notificaciones de vRealize Operations Manager.

Nota Las consultas de alerta son específicas para el usuario. El usuario solo puede administrar sus propias alertas. Debe tener asignada un rol de superadministrador para poder administrar las alertas de otros usuarios.

Una consulta de alerta está deshabilitada en las siguientes condiciones.


- Si deshabilita todas las opciones de notificación en el cuadro de diálogo Editar alerta.
- Si la alerta forma parte de un paquete de contenido.

Las consultas de alerta del paquete de contenido son de solo lectura. Para guardar los cambios efectuados en una alerta del paquete de contenido, debe guardar la alerta en su contenido personalizado.

Requisitos previos

- Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.
- Verifique que un administrador haya configurado el SMTP para habilitar las notificaciones por correo electrónico. Vea [Configurar el servidor SMTP para Log Insight](#).
- Verifique que un administrador haya configurado la conexión entre vRealize Log Insight y vRealize Operations Manager para habilitar la integración de alertas. Consulte [Configurar Log Insight para enviar eventos de notificación a vRealize Operations Manager](#).

Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.
- 2 En el menú **Crear o administrar alertas**, situado a la derecha del botón **Buscar**, haga clic en  y seleccione **Administrar alertas**.
- 3 En la lista de alertas, haga clic en una o más consultas de alerta que desee habilitar.

- 4 Seleccione las opciones de notificación que desee habilitar, y proporcione los parámetros necesarios.

Opción	Descripción
Correo electrónico	Escriba al menos una dirección de correo electrónico en el cuadro de texto. Use comas para separar varias direcciones.
Webhook	Escriba la URL a la que desea que vRealize Log Insight envíe las notificaciones.
Enviar a vRealize Operations Manager	Seleccione un recurso de vRealize Operations Manager para asociar a los eventos de notificación, y seleccione el nivel de gravedad de los eventos. Para cancelar la alerta en vRealize Operations Manager si no se ha activado dentro de un período determinado, active la casilla Cancelación automática e introduzca el período de cancelación.

- 5 Guarde sus cambios.

Opción	Descripción
Guardar	Este botón se muestra cuando modifica sus propias alertas.
Guardar en Mis alertas	Este botón se muestra cuando modifica una alerta compartida o una alerta de paquete de contenido. La alerta original permanece sin cambios, pero guarda una copia de la alerta en su contenido personalizado.

Resultados

Cuando la consulta de alerta devuelve resultados que coinciden con los criterios de alertas, vRealize Log Insight envía notificaciones de acuerdo a su configuración.

Ejemplo: Habilitar una alerta desde el paquete de contenido VMware - vSphere

El paquete de contenido VMware - vSphere incluye varias consultas de alerta predefinidas, incluida la alerta **vCenter Server: ESX/ESXi dejó de registrar**.

Habilitar la alerta **vCenter Server: ESX/ESXi dejó de registrar** constituye una buena práctica, porque determinadas versiones de hosts ESXi podrían dejar de enviar datos de syslog al reiniciar vRealize Log Insight. Esta alerta supervisa el evento de vCenter Server `esx.problem.vmsyslogd.remote.failure` para detectar si hay un host ESXi que ha dejado de enviar feeds de syslog.

- 1 En la pestaña **Análisis interactivo**, expanda el menú desplegable a la derecha del botón **Buscar**, y seleccione **Administrar alertas**.
- 2 En Paquete de contenido VMware - vSphere, haga clic en **vCenter Server: ESX/ESXi dejó de registrar**.
- 3 Habilite notificaciones por correo electrónico, notificaciones de webhook o eventos de notificación de vRealize Operations Manager.
- 4 Haga clic en **Guardar en Mis alertas**.

Para detectar solo hosts ESXi que dejaron de enviar feeds a su instancia de vRealize Log Insight, puede añadir el siguiente filtro a la consulta de alerta: **vc_remote_host (VMware - vSphere) contains <nombre-de-host-log-insight>** y guardar la nueva consulta en sus alertas.

Para obtener más información acerca de los problemas y las soluciones de syslog, consulte el artículo de la Base de conocimientos sobre los casos en que el host VMware ESXi 5.x deja de enviar syslogs al servidor remoto (2003127) en la página <https://kb.vmware.com/kb/2003127>.

Eliminar consultas de alerta



Puede eliminar consultas de alerta cuando ya no las necesite.

Nota Las consultas de alerta son específicas para el usuario. El usuario solo puede administrar sus propias alertas. Debe tener asignada un rol de superadministrador para poder administrar las alertas de otros usuarios.

Requisitos previos

Verifique que haya iniciado sesión en la interfaz de usuario web de vRealize Log Insight. El formato URL es `https://host-log_insight`, donde `host-log_insight` es la dirección IP o el nombre del host del dispositivo virtual de vRealize Log Insight.

Procedimiento

- 1 Desplácese hasta la pestaña **Análisis interactivo**.
- 2 En el menú de la derecha del botón **Buscar**, haga clic en  y seleccione **Administrar alertas**.
- 3 Seleccione una o más alertas que desee eliminar y haga clic en **Eliminar** o en el icono de eliminación .
- 4 En el cuadro de dialogo **Eliminar alerta**, seleccione **Eliminar** para confirmar la acción.