Using vRealize Log Insight

05-SEP-2017

vRealize Log Insight 4.3

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

Copyright © 2014–2017 VMware, Inc. All rights reserved. Copyright and trademark information.

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

Contents

About Using vRealize Log Insight

Using vRealize Log Insight topics provide information about using the Web user interface, including procedures about filtering and searching log messages, performing analysis and visualizing the search results, working with alert queries, and dynamically extracting fields from log messages based on customized queries.

Working With vRealize Log Insight Features 1

vRealize Log Insight provides scalable log aggregation and indexing for the vCloud Suite, including all editions of vSphere, with near real-time search and analytics capabilities.

vRealize Log Insight collects, imports, and analyzes logs to provide real-time answers to problems related to systems, services, and applications, and derive important insights.

High Performance Ingestion

vRealize Log Insight can process any type of log-generated or machine-generated data. It supports very high throughput rates and low latency and accepts data through syslog and the Ingestion API.

Scalability

vRealize Log Insight can scale out by using multiple virtual appliance instances. This enables linear scaling of the ingestion throughput, increases query performance and allows for ingestion high availability. In cluster mode, vRealize Log Insight provides master and worker nodes. Both master and worker nodes are responsible for a subset of data. Master nodes can query all subsets of data and aggregate the results.

Near Real-Time Search

Data ingested by vRealize Log Insight is available for search within seconds. Also, historical data can be searched from the same interface with the same low latency.

vRealize Log Insight supports complete keyword queries. Keywords are defined as any alphanumeric, hyphen, or underscore characters. In addition to the complete keyword queries, vRealize Log Insight supports glob queries (for example, erro?, vm*) and field-based filtering (for example, hostname does NOT match test*, IP contains "10.64"). Furthermore, log message fields that contain numeric values can be used to define selection filters (for example, CPU>80, 10<threads<100, and so on).

Search results are presented as individual events. Each event comes from a single source, but search results may come from multiple sources. You can use vRealize Log Insight to correlate the data on one or multiple dimensions (for example, time and request identifiers) providing a coherent view across the stack. This way, root cause analysis becomes much easier.

Windows and Linux Agents

vRealize Log Insight includes agents that collect events and files on Linux and Windows machines.

Intelligent Grouping

vRealize Log Insight uses a new machine learning technology. Intelligent Grouping scans incoming unstructured data and quickly groups messages together by problem type in order to give you the ability to rapidly understand issues that may span your physical, virtual, and hybrid cloud environments.

Aggregation

Fields that are extracted from log data can be used for aggregation. This is similar to the functionality that GROUP-BY queries provide in a relational database or pivot-tables in Microsoft Excel. The difference is that there is no need for extract, transform, and load (ETL) processes and vRealize Log Insight scales to any size of data.

You can generate aggregate views of the data and identify specific events or errors without having to to access multiple systems an applications between systems and applications. For example, while viewing an important system metric, for example the number of errors per minute, you can drill down to a specific time-range of events and examine the errors that occurred in the environment.

Runtime Field Extraction

Raw log data is not always easy to understand, and you might need to process some data to identify the fields that are important for searching and aggregation. vRealize Log Insight provides runtime field extraction to address this problem. You can dynamically extract any field from the data by providing a regular expression. The extracted fields can be used for selection, projection, and aggregation, similar to how the fields that are extracted at parse time are used.

Dashboards

You can create dashboards of useful metrics that you want to monitor closely. Any query can be turned into a dashboard widget and summarized for any range in time. You can check the performance of your system for the last five minutes, hour, or day. You can view a breakdown of errors by hour and observe the trends in log events.

Security Considerations

IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of vRealize Log Insight must read the security topics in *Administering vRealize Log Insight*.

These topics provide concise references to the security features of vRealize Log Insight. Topics include the product external interfaces, ports, authentication mechanisms, and options for configuration and management of security features.

This chapter includes the following topics:

- "Alert Queries in vRealize Log Insight," on page 49

Overview of the vRealize Log Insight Web User Interface

The functionality that you can access depends on the user account that you use to log in to the vRealize Log Insight Web user interface.

The Dashboards Tab

The **Dashboards** tab contains custom dashboards and content pack dashboards. On the **Dashboards** tab, you can view graphs of log events in your environment, or create your custom sets of widgets to access the information that matters most to you.

The Interactive Analytics Tab

On the **Interactive Analytics** tab, you can search and filter log events, and create queries to extract events based on timestamp, text, source, and fields in log events. vRealize Log Insight presents charts of the query results. You can save these charts to look them up later on the **Dashboards** tab.

Content Packs

Content packs contain dashboards, extracted fields, saved queries, and alerts that are related to a specific product or set of logs. You access the content packs from the drop-down menu at the upper right of the vRealize Log Insight Web user interface.

Content packs can be imported or created by vRealize Log Insight users. See "Working with Content Packs," on page 34.

The Administration User Interface

vRealize Log Insight administrators can manage user accounts, configure storage location and archiving, configure an outgoing SMTP server for email notifications, and change several other parameters. The URL format of the Administration UI is https://*log_insight-host*/admin/, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Searching and Filtering Log Events

You can search and filter log events on the **Interactive Analytics** tab.

You can type any complete keywords, globs, or phrases in the search text box and click **Search** to find only events that contain the specified keywords.

You can specify the time range on either the **Dashboards** or **Interactive Analytics** pages in the Web user interface. Time ranges are inclusive when filtering.

You can search for log events that match certain values of specific fields. Using quoted text in the main search field will match exact phrases. Entering space in the main search field is a logical AND operator. Search uses only full tokens: searching for "err" will not find "error" as a match.

You can specify the field search criteria, or filters, by using the drop-down menus and the text box above the list of log events.

Within a single-row filter, you can use comma-separated values to list OR filters. For example, select **hostname contains** and type **`127.0.0.1, 127.0.0.2`**. The search returns events with the host name 127.0.0.1 or 127.0.0.2.

Note The **text contains** filter treats each comma separated value as a complete keyword.

Queries with fields using the internal query language syntax names, for example, `from` or `in`, are not able to be processed and should not be used.

You can combine multiple field filters by creating a new filter row for each field. You can toggle the operator that is applied to multiple-row filters .

- Select **all** to apply the AND operator.
- Select **any** to apply the OR operator.

Note Regardless of the toggle value, the operator for comma-separated values within a single filter row is always OR.

You can use globs in search terms. For example, vm* or vmw?re.

- Use * for 0 or more characters
- Use ? for one character.

Note Globs cannot be used as the first character of a search term. For example, you can use 192.168.0.*, but you cannot use *.168.0.0 in your filtering queries.

Event Types Grouping

Log Insight uses machine learning to group together similar events. Event Types grouping makes troubleshooting and root cause analysis easier.

When you run queries in Log Insight, the number of results depends the query and the time range. Often queries return a large number of results. Machine learning dynamically learns and adjusts patterns from events coming to Log Insight.

The **Event Types** tab is located on the Interactive Analytics page, under the search bar. When you click the **Event Types** tab you see a list of similar events that are grouped together.

Machine learning analyzes events and discovers the types of fields that similar log messages contain. For example, the types may be timestamp, string, int, hex and others. The discovered types appear as hyperlinks within the **Event Types** list.

Each type that machine learning discovers represents a new type of field called smart field. The default name of a smart field follows the format smart field - *type number* [*event_type*]. You can change the default name of a smart field. After you name a smart field, it appears under the Fields section just like other fields. You can rename or delete a smart field but you cannot modify its definition.

Machine learning introduces a new static field called event_type. You can use the event_type as a filter to include or exclude certain event types from queries.

Information in Log Events

vRealize Log Insight collects and analyzes all types of machine-generated log data, including application logs, network traces, configuration files, messages, performance data and system state dumps.

You can connect vRealize Log Insight to everything in your environment—operating systems, applications, storage, firewalls, network devices or something else—for enterprise-wide visibility using log analytics.

When vRealize Log Insight is configured and ready to collect logs, there are several ways you can ingest log data including:

- vSphere Integration — vRealize Log Insight can integrate with vSphere to automatically ingest events from a vCenter server and logs from ESXi hosts.
- vRealize Operations Manager Integration — vRealize Log Insight can integrate with vRealize Operations Manager to enable various alerts to send notification events in vRealize Operations Manager and e-mails to administrators.
- Agents — vRealize Log Insight has collection agents available to send files and event logs from Linux or Windows to vRealize Log Insight
- Syslog — vRealize Log Insight can ingest data from any source via syslog. Just set the vRealize Log Insight server as your syslog destination.
- CFAPI — Events are sent in their original format to vRealize Log Insight using cfapi. Events sent over cfapi do not have to follow the guidelines of a syslog event and are not modified to comply with the syslog RFC.

Each event contains the following information.

Type	Description
Timestamp	The time when the event occurred
Source	Where the event originated. This could be the originator of the syslog messages such as an ESXi host or a forwarder such as a syslog aggregation.
Text	The raw text of the event.
Fields	A name-value pair extracted from the event. Fields are delivered to the server as static fields only when an agent uses the CFAPI protocol.

Note vRealize Log Insight is not responsible for the content of the log messages from other VMware products. If you have a question about the log contents, contact the product team that generated the log message.

Filter Log Events by Time Range

You can filter log events to view only the events for a certain period.

You can specify the time range on either the **Dashboards** or **Interactive Analytics** pages in the Web user interface. Time ranges are inclusive when filtering.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 From the drop-down menu on the left of the **Search** button, select one of the predefined periods.

2 (Optional) To set the initial and final point of the time range, select **Custom time range**.

Search for Log Events that Contain a Complete Keyword

You can search for log events that contain a complete keyword. Keywords contain alpha-numeric, hyphen, and underscore characters.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 In the search text box, type the complete keyword that you want to search for in the log events, and click the **Search** button.

Log events that contain the specified complete keyword appear in the list.

The string that you searched for is highlighted in yellow.

What to do next

You can save the current query to load it at a later stage.

Search Log Events by Field Operations

You can use the list of existing fields to search log events with specific values for a field.

Important vRealize Log Insight indexes complete, alphanumeric, hyphen, and underscore characters.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 Click **Add Filter**.

3 In the filter row under the search text box, use the first drop-down menu to select any field defined within vRealize Log Insight.

For example, **hostname**.

The list contains all defined fields that are available statically, in content packs, and in custom content. Fields are sorted by name, except for the **text** field. Because **text** is a special field that refers to the message text, **text** appears at the top of the list, and is selected by default.

Note Numeric fields contain additional operators that string fields do not: **=**, **>**, **<**, **>=**, **<=**. These operators perform numeric comparisons and using them yields different results than using string operators. For example, the filter **response_time = `02`** will match an event that contains a **response_time** field with a value 2. The filter **response_time contains `02`** will not have the same match.

4 In the filter row under the search text box, use the second drop-down menu to select the operation to apply to the field selected in the first drop-down menu.

For example, select **contains**. The **contains** filter matches full tokens: searching for "err" will not find "error" as a match.

5 In the text box to the right of the filter drop-down menu, type the value that you want to use as a filter.

You can list multiple values separated by comma. The operator between these values is OR.

Note The text box is not available if you select the **exists** operator in the second drop-down menu.

6 (Optional) To add more filters, click **Add Filter**.

A toggle button appears above the filter rows.

7 (Optional) For multiple filter rows, select the operator between filters.

Option	Description
all	Select to apply the AND operation between filter rows
any	Select to apply the OR operation between filter rows

By default, **all** is selected.

8 Click the **Search** button.

Example: Search for a Group of Hosts that Have a Common String in Their Names

Assume that you have several hosts that have a host with the following name: w1-stvc-205-prod3, and another host that is called w1-stvc-206-prod5.

To find all logs for both hosts, create the following query.

1 1. Leave the search text box empty.

2 Define the filter.

a Select **hostname** from the field drop-down menu.

b Select **starts with** from the operator drop-down menu.

c Type `w1-stvc` in the value text box.

Alternatively, you can use the **contains** operator, but then you must use a glob in the search value. In this example, you must type `w1-stvc-*` in the value text box.

3 Click the **Search** button.

What to do next

You can save the current query to load it at a later stage.

Search for Events that Occurred Before, After, or Around an Event

You can search the list of log events for events that occurred before, after, and around an event in the list.

If you want to know more about the status of your environment before and after an event, you can check the surrounding events.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, locate the event in the list.

2 At the left of the event row, click  and select **Set Time Range From This Event**.

3 In the Set Time Range From Event dialog box, use the drop-down menus to select the period and direction of the time range.

You can select from a list of predefined periods from 1 second to 10 minutes.

4 Click **Set Range**.

The events that surround the selected event appear in the list.

Note This operation clears all search parameters and filters that you have specified previously.

View Event in Context

You can view the context of a log event and browse the log events that arrived before and after it.

If you want to know more about the status of your environment before and after an event, you can check the surrounding events.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, locate the event in the list.

2 At the left of the event row, click  and select **View Event In Context**.

3 (Optional) Scroll up or down to the edge of the window to load more events.

4 (Optional) Click the purple timestamp to scroll back to the highlighted message.

5 (Optional) To add filters, click **Add filter** at the top, or click a field inside the highlighted event.

6 (Optional) Add or remove specific event types by pointing to an event and clicking  .

Analyze Event Trends

You can analyze log events for trends and anomalies.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 Construct and run your query by using the search text box and applying filters.

3 In the Set Time Range From Event dialog box, use the drop-down menus to select the period and direction of the time range.

4 Click the **Event Trends** tab.

vRealize Log Insight compares your query to the same time period immediately before and displays the results.

Clear All Filtering Rules

You can clear filtering and search results to view the list of all log events.

After you perform a search on the events list, the search results remain on the screen until you clear all queries.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, remove all filters.

2 If text appears in the search text box, delete it.

3 Click the **Search** button.

Examples of Search Queries

You can use these examples when building your queries on the **Interactive Analytics** tab of vRealize Log Insight.

Example: Query for all heartbeat events reported by the ESX/ESXi hostd process yesterday between 9-10am

Important vRealize Log Insight indexes complete, alphanumeric, hyphen, and underscore characters.

To query for all heartbeat events reported by the ESX/ESXi hostd process:

1 In the search text box, type **`heartbeat*`**.

2 Define a filter.

a Select **appname** from the first drop-down menu.

b Select **contains** from the second drop-down menu.

c Type **`hostd`** in the value text box.

3 Define the time range.

a In the **Time Range** drop-down menu select **Custom**.

b In the first text box, enter yesterday's date and 9am.

c In the second text box, enter yesterday's date and 10am.

4 Click the **Search** button.

Example: Search for a Group of Hosts that Have a Common String in Their Names

Assume that you have several hosts that have a host with the following name: w1-stvc-205-prod3, and another host that is called w1-stvc-206-prod5.

To find all logs for both hosts, create the following query.

1 1. Leave the search text box empty.

2 Define the filter.

   a Select **hostname** from the field drop-down menu.

   b Select **starts with** from the operator drop-down menu.

   c Type `w1-stvc` in the value text box.

   Alternatively, you can use the **contains** operator, but then you must use a glob in the search value. In this example, you must type `w1-stvc-*` in the value text box.

3 Click the **Search** button.

Example: Query for all errors reported by vCenter Server tasks, events, and alarms

To query for all errors reported by vCenter Server tasks, events, and alarms:

1 In the search text box, type `error`.

2 Define a filter.

   a Select **vc_event_type** from the first drop-down menu.

   b Select the **exists** operator from the second drop-down menu.

3 Click the **Search** button.

Example: Query for SCSI latency over one second as reported by ESX/ESXi

To query for SCSI latency over one second as reported by ESX/ESXi:

1 In the search text box, type `scsi latency "performance has"`.

2 Define a filter.

   a Select **vmw_vob_component** from the first drop-down menu.

   b Select the **contains** operator from the second drop-down menu.

   c Type `scsiCorrelator` in the text box.

3 Define a second filter.

   a Select **vmw_latency_in_micros** from the first drop-down menu.

   b Select the **>** operator from the second drop-down menu.

   c Type `1000000` in the text box.

4 Click the **Search** button.

Examples of Regular Expressions

You can type regular expressions in text boxes for field values to extract fields from log events.

The expressions you type must use the Java regular expressions syntax.

Table 1-1. Characters operators

Regular Expression	Description
\	Escapes a special character
\b	Word boundary

Table 1-1. Characters operators (Continued)

Regular Expression	Description
\B	Not a word boundary
\d	One digit
\D	One non-digit
\n	New line
\r	Return character
\s	One space
\S	Any character except white space
\t	Tab
\w	One alphanumeric or underscore character
\W	One non alphanumeric or underscore character

For example, if you have the string `1234–5678` and apply the following regular expressions

Regular Expression	Result
\d	1
\d+	1234
\w+	1234
\S	1234-5678

Table 1-2. Quantifiers operators

Regular Expression	Description
.	Any character except new line
*	Zero or more characters as long as possible
?	Zero or one character OR as short as possible
+	One or more
{<n>}	Exactly <n> times
{<n>,<m>}	<n> to <m> times

For example, if you have the string *aaaaa* and apply the following regular expressions

Regular Expression	Result
.	a
*	aaaaa
.*?	aaaaa
.{1}	a
.{1,2}	aa

Table 1-3. Combinations operators

Regular Expression	Description
.*	Anything
.*?	Anything as short as possible before

For example, if you have the string `a b 3 hi d hi` and apply the following regular expressions

Regular Expression	Result
a.* hi	b 3 hi d
a .*? hi	b 3

Table 1-4. Logic operators

Regular Expression	Description
^	Beginning of a line OR not if in brackets
$	End of a line
()	Encapsulation
[]	One character in brackets
|	OR
-	Range
\A	Beginning of a string
\Z	End of a string

For example, if you apply the following regular expressions

Regular Expression	Result
(hello)?	Either contains hello OR does not contain hello
(a|b|c)	a OR b OR c
[a-cp]	a OR b OR c OR p
world$	Ends with world followed by nothing else

Table 1-5. Lookahead operators

Regular Expression	Description
?=	Positive lookahead (contains)
?!=	Negative lookahead (does not contain)

For example, if you apply the following regular expressions

Regular Expression	Result
is (?=\w+)\w{2} primary	is FT primary? false
opid=(?!WFU-1fecf8f9)\S+	WFU-3c9bb994

Table 1-6. Additional Examples of Regular Expressions

Regular Expression	Description
[xyz]	x, y, or z
(info|warn|error)	info, warn, or error
[a-z]	A lowercase letter
[^a-z]	Not a lowercase letter
[a-z]+	One or more lowercase letters
[a-z]*	Zero or more lowercase letters
[a-z]?	Zero or one lowercase letter

Table 1-6. Additional Examples of Regular Expressions (Continued)

Regular Expression	Description
[a-z] {3}	Exactly three lowercase letters
[\d]	A digit
\d+$	One or more digits followed by end of message
[0-5]	A number from 0 to 5
\w	A word character (letter, digit, or underscore)
\s	White space
\S	Any character except white space
[a-zA-Z0-9]+	One or more alphanumeric characters
([a-z] {2,} [0-9] {3,5})	Two or more letters followed by three to five numbers

Using the Interactive Analytics Chart to Analyze Logs

The chart at the top of the **Interactive Analytics** page lets you perform visual analysis on the results of your query.

Charts represent graphical snapshots of log search queries. You can use the drop-down menus under the chart to change the chart type.

You can use the first drop-down menu to the left to control the aggregation level of the chart. The **Count** function is selected by default.

Chart Types

You can select different chart types to change the way data is visualized on the Interactive Analytics page.

Different chart types require different aggregation functions, the use of time series, and group-by fields.

Chart Type	Aggregation Function	Time Series Requirement	Group-by Field Requirement
Column	Any	Time series	N/A
Line	Any	Time series	N/A
Area	Any	Time series	N/A
Bar	Any	Non-time series	At least one field
Pie	Count or Unique Count	Non-time series	At least one field
Bubble	Any	Non-time series	Two fields
Gauge	Count	Non-time series	N/A
Scalar	Count	Non-time series	N/A
Table	Any	Any	N/A

Multi-function Charts

You can use multi-function charts to compare variables that are not the same scale.

With multi-function charts, you can assign a y-axis for each series or an x-axis if you want to compare data sets of different categories. Each axis can be placed to the right or left of the chart. You can swap the functions to swap the y-axis on which they are plotted from right to left.

For example, you can chart the count of events grouped by channel and level in addition to the average of tasks grouped by channel and level.

Aggregation Function

vRealize Log Insight provides several aggregation functions.

Type	Field	Description
Count	Events only	Creates a chart of the number of events for a specific query.
Unique count	Any field	Creates a chart of the number of unique values for a field.
Minimum	Numeric fields only	Creates a chart of the minimum value for a field.
Maximum	Numeric fields only	Creates a chart of the maximum value for a field.
Average	Numeric fields only	Creates a chart of the average value for a field.
Std dev	Numeric fields only	Creates a chart of the standard deviation for a field's values.
Sum	Numeric fields only	Creates a chart of the sum of values for a field.
Variance	Numeric fields only	Creates a chart of the variance for the values of a field.

You can modify the way you view the query results.

View	Description
To group query results by specific field values	Use the second drop-down menu under the chart to group query results by specific field values rather than or in addition to time series.
To view the number of events for a field	For example, the number of events per host, deselect the **Time series** check box and select the check box for that field.
To view a stacked bar chart for a field with groupings over time	Select both the **Time series** check box and the field check box.

Working with Charts

You can change how charts look on the **Interactive Analytics** tab, add charts to your custom dashboards, and manage dashboard charts.

Task	Procedure
Change the time range of a chart	On the **Interactive Analytics** tab, use the drop-down menu to the left of the **Search** button to switch the period displayed in the chart.
Change the granularity of a chart	On the **Interactive Analytics** tab, use the buttons at the upper right to switch between different time ranges for each point represented on the chart. The available ranges depend on the time range specified for the query.
Load a dashboard chart on the **Interactive Analytics** tab	On the **Dashboards** tab, locate the chart and click the **Open in Interactive Analytics** icon . The time range is set to the current time range of the dashboard. You can modify the time range if needed.
Save a chart to your custom dashboard	1 At the upper left of the **Interactive Analytics** tab, click **Add to Dashboard**. Alternatively, from the menu to the right of the **Search** button, select **Add Current Query to Dashboard**. 2 Type a name, select the destination dashboard from the drop-down menu, select the widget type, add information about the widget, and click **Add**.
Save a query as a chart to your custom dashboard	1 Click **Add Current Query to Dashboard** next to the **Search** button. 2 Type a name, select the destination dashboard from the drop-down menu, make sure the widget type is set to **Chart**, add information about the widget, and click **Add**.

Task	Procedure
Save a query as a field table to your custom dashboard	1 Click **Add Current Query to Dashboard** next to the **Search** button. 2 Type a name, select the destination dashboard from the drop-down menu, make sure the widget type is set to **Field Table**, add information about the widget, and click **Add**.
Delete a widget from your custom dashboard	1 On the **Dashboards** tab, select the custom dashboard that contains the widget that you want to delete. 2 In the upper right corner of the widget, click the **Other Actions** icon, and select **Delete**. 3 In the Delete Widget dialog box, click **Delete** to confirm.

Change the Type of the Interactive Analytics Chart

You can change the aggregation and grouping of query results displayed in the chart to graphically analyse log events.

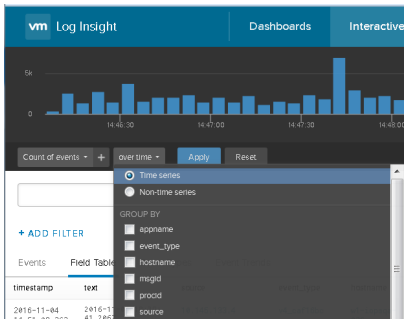
The number of drop-down menus that you see under the chart depends on the selected aggregation function.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Use the drop-down menus under the Interactive Analytics chart to change the aggregation function and grouping type.



- To view the number of events over time, select the **Time series** button.
- To view only event values, select the **Non-time series** button and select at least one field.

2 Click **Update**.

Example: Aggregation and Grouping in the Interactive Analytics Chart

The following table contains examples to illustrate aggregation and grouping in vRealize Log Insight charts.

Table 1-7. Example Aggregation and Grouping in the Interactive Analytics Chart

Selection in the First Drop-Down Menu	Selection in the Second Drop-Down Menu	Time series selection	Text Displayed on the Screen	Result
Count	**Time series**	**Time series**	**Count** of events **over time**	The chart displays a bar chart with the number of events for the current query over time.
Average	**vmw_op_latency (VMware - vSphere)**	**Time series**	**Average** of **vmw_op_latency (VMware - vSphere) over time**	The chart displays a line chart with average value of operations latency over time.
Count	**vmw_esx_problem** **Note** Thevmw_esx_problem field does not appear by default. You must extract the vmw_esx_problem field and save the query so that vmw_esx_problem appears in the drop-down menu.	**Non-time series**	**Count** of events **grouped by vmw_esx_problem**	The chart displays a bar chart of the number of events for containing the vmw_esx_problem field.
Count	**Time series**, **vmw_esx_problem**	**Time series**	**Count** of events **over time grouped by vmw_esx_problem**	The chart displays a stacked bar chart grouped by vmw_esx_problem over time.

Dynamic Field Extraction

In a large environment with numerous log events, you cannot always locate the data fields that are important to you.

vRealize Log Insight provides runtime field extraction to address this problem. You can extract any field dynamically from the data by providing a regular expression. See "Examples of Regular Expressions," on page 16.

Note Generic queries might be very slow. For example, if you attempt to extract a field by using the `\(\d+\)` expression, the query returns all log events that contain numbers in parenthesis. Verify that your queries contain as much textual context as possible. For example, a better field extraction query would be `Event for vm\(\d+\)`.

You can use the extracted fields to search and filter the list of log events, or to aggregate events in the Interactive Analytics chart.

Extract Fields by Using One-Click Extract

Instead of typing context values for extracting fields dynamically, you can use the one-click extract function.

The one-click extract populates all context values that correspond to the field that you select in a log event.

Note The one-click extract option is available only in Events tab.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 In the list of log events, highlight the text that represents the field that you want to extract.

An action menu appears above the set of field names present in that event.

3 Click **Extract Field**.

The pre and post context values in the Fields pane are populated automatically with the context needed to extract the highlighted field.

4 (Optional) Modify the Extracted value regular expression in the Fields pane.

5 (Optional) Modify the Pre and post context regular expressions in the Fields pane.

6 (Optional) Click **Add additional context** to add more keywords and filters.

You can add one or more keywords and use a single static field as a filter.

7 If you are an administrator user, select which users can access the field from the drop down menu.

Option	Description
All users	All users will see the field in their events and in the filter drop-down menu.
Me only	Only the creator of the field will see the field in their events and filter drop down menu.

8 (Optional) At the top of the Fields pane, click and then **Edit** to add notes to this field. Add notes in the **Edit Notes** window and click **OK**.

9 Click **Save**.

What to do next

You can use the extracted field to search and filter the list of log events, or to aggregate events in the Interactive Analytics chart.

You can modify saved field definitions or delete them if you no longer need them.

Modify an Extracted Field

You can modify the definitions of extracted fields.

vRealize Log Insight creates copies of the fields that you use when you create charts, queries, or alerts. If you modify a field definition, all charts, queries, and alerts that use the modified field are updated to reflect the new definition.

Normal users can modify only their own content. Administrator users can modify their own content and their shared content.

Content pack fields are read-only.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 At the top of the Fields pane, click **Manage extracted fields** and select an extracted field from the list.

3 Modify the values and click **Update**.

A dialog box displays a list of content that will be affected by the updated field. If the field is shared between multiple users, the dialog box also displays a list of affected users.

4 (Optional) At the top of the Fields pane, click and then **Edit** to add notes to this field. Add notes in the **Edit Notes** window and click **OK**.

5 Click **Update** to confirm your changes.

vRealize Log Insight updates all queries, alerts, and charts that use the field that you modified.

Duplicate an Extracted Filed

You can duplicate an extracted field.

You use the Duplicate option when you want to extract more than one field from an event and both fields appear in a similar context. After you extract a field and save it, open the extracted field definition and use the Duplicate option. The duplicated field has the exact same definition as the original extracted field. You can modify the definition of the duplicated field to match another value in the event that interests you.

Normal users can duplicate only their own content. Administrator users can modify their own content and their shared content.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 At the top of the Fields pane, click **Manage extracted fields** and select an extracted field from the list.

3 Click **Duplicate** to create a copy of the field.

4 (Optional) Modify the Extracted value regular expression in the Fields pane.

5 (Optional) Modify the Pre and post context regular expressions in the Fields pane.

6 (Optional) Click **Add additional context** to add more keywords and filters.

You can add one or more keywords and use a single static field as a filter.

7 If you are an administrator user, select which users can access the field from the drop down menu.

Option	Description
All users	All users will see the field in their events and in the filter drop-down menu.
Me only	Only the creator of the field will see the field in their events and filter drop down menu.

8 Click **Save**.

What to do next

You can use the extracted field to search and filter the list of log events, or to aggregate events in the Interactive Analytics chart.

You can modify saved field definitions or delete them if you no longer need them.

Delete an Extracted Field

You can delete extracted fields that are no longer needed.

vRealize Log Insight creates copies of the fields that you use when you create widgets, queries, or alerts. If you delete a field that is used in widgets, queries, or alerts, vRealize Log Insight creates a temporary copy of the deleted field for each widget, query, or alert that uses that field.

You can delete only fields that have the **Edit this field** icon next to their names. Normal users can delete only their own content. Administrator users can delete their own content and their shared content.

Content pack fields are read-only.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 At the top of the Fields pane, click **Manage extracted fields** and hover over an extracted field from the list.

3 Click .

A dialog box displays a list of content that uses the field that you want to delete. If you are an administrator user, and the field is shared by multiple users, the dialog box also displays a list of affected users.

4 Click **Delete** to confirm.

If a deleted field is used in existing queries, vRealize Log Insight creates a temporary copy of the field and displays it when you load a query that uses the deleted field.

If you export content that contains temporary fields, vRealize Log Insight creates the fields in the exported content pack to avoid temporary fields.

Managing Search Queries

You can export query results, share your queries with other users, and can save, delete, rename, and load existing queries. You can take snapshots of queries and save them to dashboards.

Save a Query in vRealize Log Insight

You can save your current query and time range in vRealize Log Insight to view it later. Saved queries can only be loaded from the **Interactive Analytics** page.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, perform the query that you want to save.

2 Click , select **Add current query to favorites** icon .

3 Type a name and click **Save**.

Note Saved queries include a fixed time range and are not updated. By saving a query, you take a snapshot of log messages available within the time range at the moment when you save.

The query is added to the Favorite queries list.

All users, including administrators, have an individual list of saved queries.

Rename a Query in vRealize Log Insight

You can change the name of a query that you saved in vRealize Log Insight.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 Click the Favorite queries icon

3 Point to the query that you want to rename, and click the **Edit this saved query** icon .

4 Type a new name and click **Save**.

Load a Query in vRealize Log Insight

You can load queries from content packs or queries that you saved to view them on the **Interactive Analytics** tab.

Saved queries are separate from dashboard items. They do not appear on any custom dashboard. If you want to view a saved query, you have to load it.

All users, including administrators, have an individual list of saved queries.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 Click the Favorite queries icon 

3 In the Favorite Queries list, click the query that you want to view on the **Interactive Analytics** tab.

The query is loaded on the **Interactive Analytics** tab. The time range of the query is displayed above the list of events.

What to do next

You can add the query to a dashboard, change the granularity of the chart, or apply additional filtering to the query results.

Delete a Query from vRealize Log Insight

You can delete saved queries from vRealize Log Insight.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 From the drop-down menu on the right of the **Search** button, select **Load Query**.

3 Click the Favorite queries icon 

4 In the Favorite Queries list, click  next to the query you want to delete.

5 Click **Delete** to confirm.

Share the Current Query

You can send your peers a link to the current query.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, perform the query that you want to share.

2 Click  and select **Share Query**.

vRealize Log Insight displays the URL to the query.

3 Copy the URL and send it to the person that you want to share with.

Export the Current Query

You can export the results of a log query to share them with other systems, or forward them to your support contact.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, perform the query that you want to export.

2 Click  and select **Export Event Results**.

3 Select the format to save the query to, and click **Export**.

Option	Description
Raw Events	Select to save the results in TXT format
JSON	Select to save the results in JSON format
XML	Select to save the results in XML format

Take a Snapshot of a Query

You can take a snapshot of your current query and time range in vRealize Log Insight for quick viewing or to save to a dashboard. Snapshots can be taken from the Interactive Analytics page.

A snapshot saves the log messages available within the time range at the moment when you take the snapshot. After you take a snapshot, click it to return to the query when you took the snapshot. If you want to save one or more snapshots, add them to an existing dashboard or create a new dashboard.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, perform the query that you want to save as a snapshot.

2 Click the Snapshot icon.

The snapshot appears at the bottom of the screen.

3 (Optional) Change the query and take additional snapshots.

The snapshots appear at the bottom of the screen.

4 (Optional) At the bottom of the screen, click  and select **Save All to Dashboard**.

a Select an existing dashboard or create a new dashboard.

b Click **Add.**

The snapshot is added to the selected or new dashboard.

5 (Optional) Click the "X" on a snapshot to delete the snapshot.

6 (Optional) Click  and select **Delete All** to delete snapshots.

Working with Dashboards

Dashboards in vRealize Log Insight are collections of chart, field table and query list widgets.

Custom Dashboards

Custom dashboards are created by users of the current instance of vRealize Log Insight. Custom dashboards are organized in two categories, My Dashboards and Shared Dashboards. Shared dashboards are visible to all users of the vRealize Log Insight instance.

My Dashboards are user-specific.

Normal users can modify only the dashboards in the My Dashboard section.

Admin users can modify the dashboards in the My Dashboards section, and the dashboards that they created in the Shared Dashboards section.

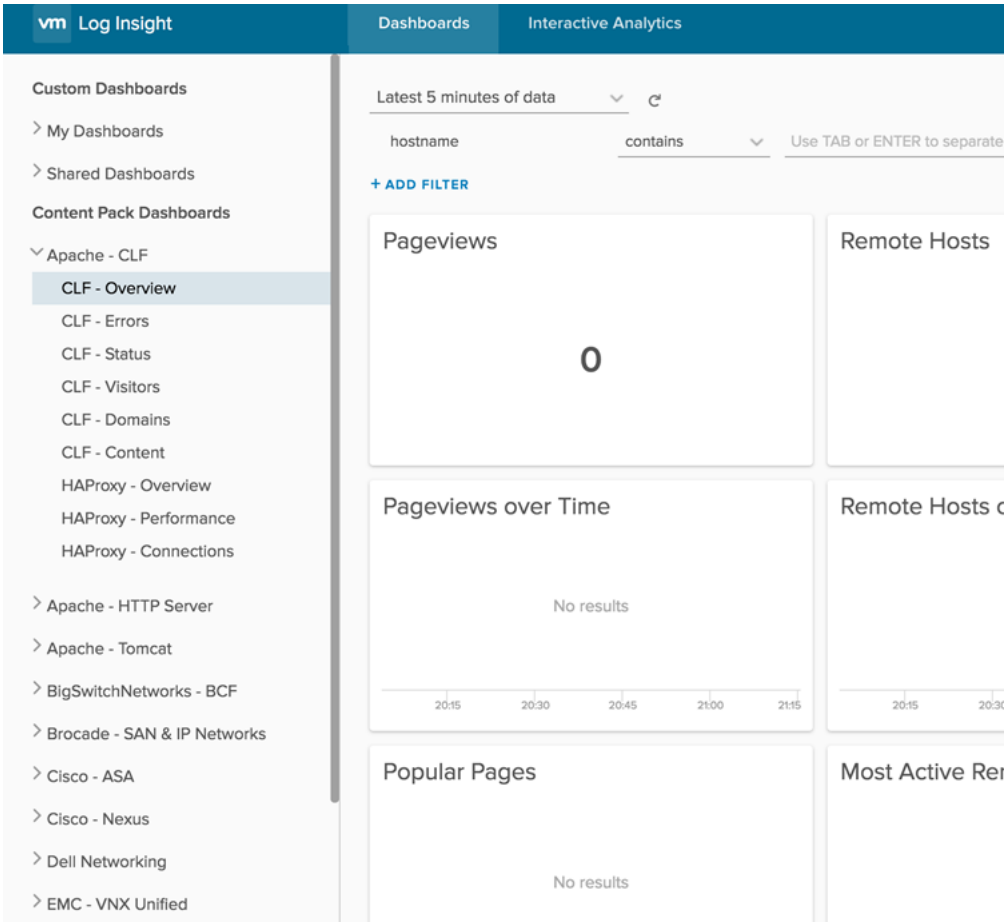
Content Pack Dashboards

Content pack dashboards are imported with content packs and are visible to all users of the vRealize Log Insight instance.

Note Content pack dashboards are read-only. You cannot delete or rename them. However, you can clone content pack dashboards to your custom dashboard. You can clone whole dashboards or individual widgets.

To view the dashboards that are available in your instance of vRealize Log Insight, click **Dashboards** in the upper left corner of the vRealize Log Insight user interface. The left pane that appears lists all dashboards you have access to, grouped by Custom Dashboards and Content Pack Dashboards. Click **>** next to each subgroup to display associated dashboards. You can open one dashboard group at a time by clicking **>** next to the group name. Click **>** next to another group name to open a new group and close the previous one. Only one group at a time can be open.

To view the contents of a dashboard, click the dashboard name in the list on the left.



Managing Dashboards

You can add, modify, and delete dashboards in your Custom Dashboards space.

Content Pack dashboards cannot be modified, but you can clone these dashboards to your Custom Dashboards space and modify the clones.

Important vRealize Log Insight does not perform checks for duplicate names of the dashboards, queries, and alerts that you save or clone. The display name is not a unique identifier when vRealize Log Insight saves queries. Therefore, you can save multiple charts, alerts, and dashboards with the same name. To ease data retrievability, do not duplicate names when you save charts, alerts, or dashboards.

Table 1-8. Working with Custom Dashboards

Task	Procedure
Create a new custom dashboard	On the **Dashboards** tab, select **My Dashboards**, and click **New Dashboard** in the lower left.
Edit the name of a custom dashboard	On the **Dashboards** tab, hover over the dashboard name, click the menu icon and select **Reame**. Enter a new name and click **Save.**
Delete a custom dashboard	On the **Dashboards** tab, hover over the dashboard name, click the menu icon and select **Delete**. In the confirmation dialog box select **Delete**.

Table 1-8. Working with Custom Dashboards (Continued)

Task	Procedure
Clone a dashboard from a content pack to your custom dashboard	1 On the **Dashboards** tab, select a content pack and hover over the dashboard that you want to clone. 2 Click the menu icon and select **Clone** from the drop-down menu. 3 Type a name and click **Save**. If you are an administrator user, you can select whether to share your dashboard with other users.
Add a chart widget to a dashboard	1 At the upper left of the **Interactive Analytics** tab, click **Add to Dashboard**. Alternatively, from the menu to the right of the **Search** button, select **Add Current Query to Dashboard**. 2 Type a name, select the destination dashboard from the drop-down menu, select the widget type, add information about the widget, and click **Add**.
Add a query list widget to the dashboard	See "Add a Query List Widget to the Dashboard," on page 31.
Add a query to a query list widget in a dashboard	See "Add a Query to a Query List Widget in a Dashboard," on page 32.
Add a query to a field table widget in a dashboard	See "Add a Field Table Widget to a Dashboard," on page 32
Add an event types widget to a dashboard	"Add an Event Types Widget to a Dashboard," on page 33
Add an event trends widget to a dashboard	"Add an Event Trends Widget to a Dashboard," on page 33
Delete a widget from a dashboard	1 On the **Dashboards** tab, select the custom dashboard that contains the widget that you want to delete. 2 In the upper right corner of the widget, click the **Other Actions** icon, and select **Delete**. 3 In the Delete Widget dialog box, click **Delete** to confirm.

Add a Query List Widget to the Dashboard

You can save lists of search queries to your custom dashboards by creating query list widgets.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, run the query that you want to add to the dashboard.

2 Click the **Add current query to dashbord** icon .

3 From the **Dashboard** drop-down menu, select the dashboard to which you want to add the query.

4 From the **Widget Type** drop-down menu, select **Query List**.

5 From the **Query List** drop-down menu, select **New Query List**, type a name for the list, and click **Save**.

6 Click **Add**.

The query list widget appears on the dashboard that you specified.

What to do next

You can add queries to the query list widget that you created. See "Add a Query to a Query List Widget in a Dashboard," on page 32.

Add a Query to a Query List Widget in a Dashboard

Query list widgets provide quick access to one or more saved queries from the dashboard.

You can modify your custom query list widgets to add new queries.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, run the query that you want to add to the query list widget.

2 Click the **Add current query to dashbord** icon  .

3 From the **Dashboard** drop-down menu, select the dashboard that contains the query list widget.

4 From the **Widget Type** drop-down menu, select **Query List**.

5 From the **Query List** drop-down menu, select the name of the widget to which you want to add the query, and click **Save**.

6 Click **Add**.

vRealize Log Insight adds the query to the widget that you selected.

Note Query list widgets use message queries. If you use the same message query in a Chart widget and choose a group-by field that does not exist in any of the messages, the chart will display no results.

Add a Field Table Widget to a Dashboard

Field table widgets provide quick access to one or more saved fields from the dashboard.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, run the query that you want to add to the field table widget.

2 Click the **Add current query to dashbord** icon  .

3 From the **Dashboard** drop-down menu, select the dashboard to which you want to add the field table.

4 From the **Widget Type** drop-down menu, select **Field Table**.

5 Select the fields you want to include in the field table.

6 Click **Add**.

The filed table widget appears on the dashboard that you specified.

Add an Event Types Widget to a Dashboard

Event Types widgets provide access to event type groups, which are created through machine learning to group similar events together.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, run the query that you want to add to the widget.

2 Click the **Add current query to dashbord** icon  .

3 From the **Dashboard** drop-down menu, select the dashboard to which you want to add the widget.

4 From the **Widget Type** drop-down menu, select Event Types.

5 Click **Add**.

The widget appears on the dashboard that you specified.

Add an Event Trends Widget to a Dashboard

Event Trends widgets provide access to information about event trends, which analyze trends in a specified time period.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, run the query that you want to add to the widget.

2 Click the **Add current query to dashbord** icon  .

3 From the **Dashboard** drop-down menu, select the dashboard to which you want to add the widget.

4 From the **Widget Type** drop-down menu, select Event Trends.

5 Click **Add**.

The widget appears on the dashboard that you specified.

Filter Using Field Values from Charts

You can use a field value in a chart as filter on the dashboard that contains the chart, on a different dashboard that uses the field, and in Interactive Analytics.

If you see a problem with a field value in a chart, you can quickly use the field value as an input and jump to another dashboard that uses that field. If no other dashboard uses this field, you can use the field value as a filter on the same dashboard or run it in Interactive Analytics.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 From the **Dashboard** drop-down menu, select the dashboard that contains a chart widget.

2 In the chart widget, hover over the chart data and view field values that appear as tooltips.

3 Click the field value that you want to use as a filter.

The **Add Value as Filter** menu appears.

4 Select where you want to use the field value as a filter.

Option	Action
Interactive Analytics	The Interactive Analytics page opens and displays the results of the chart query. The field value you selected in Step 3 is used as a filter.
This Dashboard	The field value you selected in Step 3 is used as a filter on the same dashboard.
Other Dashboard	The field value you selected in Step 3 is used as a filter on another dashboard that contains the field.

Working with Content Packs

Content packs contain dashboards, extracted fields, saved queries, and alerts that are related to a specific product or set of logs.

To view the content packs that are loaded on your system, select **Content Packs** from the drop-down menu in the upper right corner of the vRealize Log Insight user interface.

To view the contents of a content pack, click the content pack in the list on the left.

Content Packs

The Content Packs category contains imported sets of dashboards, extracted fields, queries, and alerts. The General and VMware - vSphere content packs are imported by default.

Note Content pack dashboards are read-only. You cannot delete or rename them. However, you can clone content pack dashboards to your custom dashboard. You can clone whole dashboards or individual widgets.

Custom Content

The Custom Content category contains dashboards, extracted fields, and queries created in the current instance of vRealize Log Insight. The My Content section contains the custom content of the user that is currently logged in. The Shared Content section contains content that is shared among all users of vRealize Log Insight.

Only Admin users can share content with other users. Only Admin users can manage shared content.

Note You cannot uninstall content from the Custom Content section. If you want to remove saved information from the Custom Content section, you have to delete individual elements, such as dashboards, queries, alerts, and fields.

Install a Content Pack from the Content Pack Marketplace

You can install content packs from the Content Pack Marketplace without leaving the vRealize Log Insight UI.

Prerequisites

- Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.
- Verify that you are logged in as a user with the **Edit Shared** permission.
- Verify that the Web browser that is running vRealize Log Insight can make an outbound connection to https://api.github.com/.

Procedure

1 From the drop-down menu on the upper right, select **Content Packs**.

2 From the menu on the left, select **Marketplace**.

3 Accept the EULA agreement.

4 Select the content pack you want to install and click **Install**.

The installed content pack appears in the Installed Content Packs list on the left.

Update an Installed Content Pack from the Content Pack Marketplace

You can update the content packs that are already installed from the Content Pack Marketplace without leaving vRealize Log Insight.

Note When alerts from content packs are enabled, the alerts are copied to a user's profile. Users can modify the copy's description or conditions. Beginning with alert definitions instantiated in 4.0, updating a content pack, and by extension its alert definitions, updates or removes the copies to match the improved content pack. If you want to preserve any user modifications, export them as a content pack first and import back into the user profile after the update.

Prerequisites

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

Procedure

1 From the drop-down menu on the upper right, select **Content Packs**.

2 From the menu on the left, select **Updates** to see a list of content packs for which updates are available.

- To update a single content pack, click its icon to open an informational window. Click **Update** to begin the import. Depending on the content pack, after the import is complete you might see further instructions. If these appear, follow the configuration steps to successfully complete the upgrade.
- To silently update all content packs with pending updates, click **Update All**. Read the instructions in the informational pop-up and click **Update** to proceed. After the upgrade, click each content pack to check for further configuration steps to successfully complete the upgrade following import. If you have exported a content pack to preserver user modifications, import it back into the user profile.

The updated content pack appears in the Installed Content Packs list on the left.

Import a Content Pack

You can import content packs to exchange user-defined information with other instances of vRealize Log Insight, or to upgrade your old content packs with later versions.

You can import only vRealize vRealize Log Insight Content Pack (VLCP) files.

Note If you import a new version of an already existing content pack, and the new version contains modified field definitions, all queries, alerts, and charts that use the modified field are updated to reflect the new definition. If fields that exist in the current content pack version are missing in the new version that you import, vRealize Log Insight creates temporary copies of the fields for each query, chart, or alert that uses a deleted field.

Prerequisites

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

Procedure

1 From the drop-down menu on the upper right, select **Content Packs**.

2 In the lower left corner, click **Import Content Pack**.

3 If you are an administrator user, select the import method.

Option	Description
Install as content pack	The content is imported as a read-only content pack that is visible to all users of the vRealize Log Insight instance. **Note** Content pack dashboards are read-only. You cannot delete or rename them. However, you can clone content pack dashboards to your custom dashboard. You can clone whole dashboards or individual widgets.
Import into My Content	The content is imported as custom content to your user space, and is visible only to you. You can edit the imported content without having to clone it. **Note** Content pack metadata, such as name, author, icon, and so on, are not displayed in this mode. Once imported in My Content, the content pack cannot be uninstalled as a pack. If you want to remove a content pack from My Content, you have to individually remove each of its elements, such as dashboards, queries, alerts, and fields.

Normal users can import content packs only in their own user spaces.

4 Browse for the content pack that you want to import, and click **Open**.

5 Click **Import**.

If you selected the option to import as custom content, a dialog box appears for you to select what content to import.

6 (Optional) If you selected to import as custom content, use the check-boxes to select which items to import, and click **Import** again.

Note Fields that are used in imported queries, charts, and alerts are also imported.

7 (Optional) For some content packs, if you are importing the content pack for the first time, you will see setup instructions pop up after the import is complete. Follow these instructions to complete the set up of the content pack.

8 (Optional) For some content packs, if you are importing the content pack as an upgrade, you will see upgrade instructions pop up after the import is complete. Follow these instructions to complete the set up of the content pack.

The imported content pack is ready to use and appears in the Content Packs or the Custom Content list to the left.

Note Imported Alerts are disabled by default. See "Enable Alert Queries," on page 59.

Export a Content Pack

You can export your custom dashboards, saved queries, alerts, and extracted fields as a content pack, to share content between vRealize Log Insight instances or with vRealize Log Insight users on the community.

Content packs are saved as vCenter vRealize Log Insight Content Pack (VLCP) files.

All fields that are used in queries, charts, and alerts that you export are included in the exported content pack.

If you export content that contains temporary fields, vRealize Log Insight creates these fields within the content pack during the export.

Prerequisites

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

Procedure

1 From the drop-down menu on the upper right, select **Content Packs**.

2 Click the content pack that you want to export and select **Export** from the drop-down menu  next to the name of the content pack.

3 (Optional) Select the content that you want to include in the content pack.

Note You cannot deselect fields that are used in dashboards, queries, or alerts selected for export.

4 In the text fields to the right, fill in the metadata for your content pack.

Option	Description
Name	The name is displayed when you import the pack into a vRealize Log Insight instance. The content pack file name is derived from the **Name** text box. The recommended format is *Vendor - Product* For example, VMware - vSphere.
Version	If you plan to upgrade this content pack, type a version. vRealize Log Insight displays the version when you try to install a content pack that already exists in the Content Packs list.
Namespace	The namespace is a unique identifier for the content pack. Use reverse DNS naming, for example **`com.companyname.contentpackname`**.
Author	Optionally, you can type your name or the name of your company.
Website	Optionally, you can provide a link to the Web site that is associated with the content pack. All users that can view the content pack can see the Web site link as well.
Description	Optionally, you can provide information about the contents and purpose of the pack.
Icon	Optionally, you can browse for an icon to be displayed next to the content pack name. **Note** The icon file format must be PNG or JPG, and will be scaled to 144 by 144 pixels in size.

Note This data is visible only if you import the content pack by using the **Install as content pack** option. You cannot view this information if you choose to import the content pack as custom content.

5 Click **Export**, browse to the location where you want to save the file, and click **Save**.

The exported VLCP file is downloaded to the selected location.

View Details About Content Pack Elements

You can open the queries that build up dashboards, or open the definitions of fields, queries, and alerts, directly from the Content Packs view.

You might want to use the definitions of content pack elements as templates for your custom definitions.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 From the drop-down menu on the upper right, select **Content Packs**.

2 Select the content pack that contains the element that you want to review.

3 Click the button that corresponds to the element type you want to review.

For example, click **Alerts** to view all alerts that the content pack contains.

4 In the list of elements, click the name of the element that you want to review.

The Interactive Analytics page opens and displays the query that corresponds to the selected element.

What to do next

You can modify the query or definition of the content pack element and save it to your custom content.

Uninstall a Content Pack

You can uninstall content packs. Uninstalling contact packs remove custom dashboards, saved queries, alerts, and extracted fields.

Content packs are saved as vCenter vRealize Log Insight Content Pack (VLCP) files.

Uninstalling a content pack makes it permanently unavailable for all users. Make a backup by exporting the content pack as a VLCP file first. See "Export a Content Pack," on page 37.

Prerequisites

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

Procedure

1 From the drop-down menu on the upper right, select **Content Packs**.

2 Click the content pack that you want to uninstall and select **Uninstall** from the drop-down menu  next to the name of the content pack.

3 Click **Uninstall**.

The content pack is removed from the Installed Content Packs list.

Creating Content Packs

Any Log Insight user can create a content pack for private or public usage.

Content packs are immutable or read-only plug-ins to vRealize Log Insight, that provide predefined knowledge about specific types of events, such as log messages. The goal of a content pack is to provide knowledge about a specific set of events in a format that is easily understandable by administrators, engineers, monitoring teams, and executives.

Content packs give information about the health status of a product or application. In addition, a content pack helps you understand how a product or an application works.

You can save the information from a content pack by using either the Dashboards or Interactive Analytics pages in vRealize Log Insight. The information in a content pack includes:

- Queries - usually a content pack contains at least three queries and three chart widgets for each dashboard, which means more than nine queries in total
- Fields - a content pack should have at least twenty extracted fields
- Aggregations
- Alerts - each content pack contains at least five alerts
- Dashboards - there are at least three dashboards in each content pack
- Dashboard filters - see "Searching and Filtering Log Events," on page 9
- Visualizations - see "Using the Interactive Analytics Chart to Analyze Logs," on page 19

By default, vRealize Log Insight ships with the VMware - vSphere content pack. You can import additional content packs if needed.

Content Packs Terms

The content pack creation workflow is based on several concepts and terms. You should get familiar with them in order to create and maintain content packs effectively.

Instance

Only vRealize Log Insight administrators can import a content pack file as a content pack. If a content pack is imported as a content pack it cannot be edited.

All users can import a content pack file into a user space. If you import a content pack file into a user space, the operation selectively imports the objects under My Content. When you import a content pack into a user space, you can edit the content packs in a vRealize Log Insight instance. If you want to publish or modify a content pack you need an exported content pack.

User

Content packs are created in part from the content saved under Custom Dashboards, also known as user space, or more specifically either My Dashboards or Shared Dashboards on the Dashboards page. While objects from a custom dashboard can be selectively exported, it is recommended that every individual content pack be authored by a separate user entity in vRealize Log Insight to ensure a clean user space per content pack.

For information on creating users in vRealize Log Insight, see the *VMware vCenter Log Insight Administration Guide*.

Use a separate content pack author user in vRealize Log Insight for every content pack you create.

Events

It is essential to collect relevant events before attempting to create a content pack to ensure that a content pack covers all relevant events for a product or an application. One common way to collect relevant events is to ask quality assurance and support teams as these teams usually have access to, and knowledge about common events.

Attempts to generate events while you create a content pack are time consuming and results in missing important events. If QA and support teams are unable to supply events, you may simulate events and use them instead if product or application events are known and documented.

Once you collect the appropriate logs, they must be ingested into vRealize Log Insight.

Authors

The authors of a content pack need to have the following qualifications:

- Experience using VMware vRealize Log Insight.
- Real world operating knowledge of the product or application.
- Understanding and ability to generate optimized regular expressions.
- Experience debugging multiple problems with product or application using logs.
- Support background, with exposure to a myriad of problems.
- System administrator background with previous syslog experience.

Workflow

The recommended approach for content pack creation is to start on the Interactive Analytics page and begin querying for specific types of events such as error or warning. Look at the results of the queries and analyze and extract potential field candidates as appropriate. With some understanding of the types of events and useful pieces of information available in the events, construct and save relevant queries as appropriate. For queries that highlight an issue that needs a quick action, create and save alerts. As you save queries, remove them from the results list using a filter to show other events that may be potential candidates for new saved queries. Once you save all relevant queries, organize and display them in a logical manner on the Dashboards page.

Queries

Queries in vRealize Log Insight can retrieve and summarize events.

You can create and save queries from the Interactive Analysis page. A query consists of one or more of the following:

Keywords	Complete, or full-text, alphanumeric, hyphen, and/or underscore matches.
Globs	Complete, or full-text, alphanumeric, hyphen, and/or underscore matches.
Regular expressions	Sophisticated string pattern matching based on Java regular expressions.
Field operations	Keyword, regular expression, and pattern matches applied to extracted fields.
Aggregations	Functions that are applied to one or more subgroups of the results.

vRealize Log Insight supports the following types of queries:

- Message. A query made up of keywords, regular expressions and/or field operations.
- Regular expression or field. A query made up of keywords and/or regular expressions.
- Aggregation. A query made up of a function, one or more groupings, and any number of fields.

You can define custom alerts in vRealize Log Insight and trigger them from scheduled queries of any type.

Best Practices for Creating Message Queries

Basic concepts for creating message queries.

You can enter message queries by using the Search bar, or by entering filters.

Use the search bar to refine the results for events in a vRealize Log Insight instance. While you can use a filter instead of the search bar, it is often easier to understand a query that leverages the search bar over an equivalent filter. The best practice is to use the search bar instead of an equivalent filter when possible.

A filter allows you to create queries by using a regular expression, a field, logical OR operation, or a combination of search bar and filter queries.

When you create queries by using the search bar and filters, the following best practices apply:

- Ensure queries are not environment specific. Public content packs need to be generic to any environment and as such need not to rely on environment specific information. Examples of environment specific information include source, hostname, and potentially facility if the facility uses *local**.
- When constructing a query, use keywords when possible, when keywords are not sufficient use globs, and when globs are not sufficient use regular expressions. Keyword queries are the least resource intensive type of query. Globs are a simplified version of regular expression and are the next least resource intensive type of query. Regular expressions are the most expensive type of query.

- Provide as many keywords as possible when using regular expressions or fields. If a regular expression includes a logical OR, for example *this*|*that*, do not include keywords. vRealize Log Insight is optimized to perform keyword queries prior to regular expressions to minimize regular expression overhead.

Field Queries

Fields are a powerful way to add structure to unstructured events and allow the manipulation of both the textual and visual representation of data.

Fields are one of the most important items in a content pack as they can be used in different ways including aggregations and filters. Aggregations allow you to apply functions and groupings to fields. Filters allow you to perform operations over fields.

You must extract any part of a log message that might be applicable to a query or aggregation. Fields are a type of regular expression query and are useful for complex pattern matching so you do not need to know, remember, or learn complicated regular expressions.

Field Context Value	Definition
Regex before value	Include as many keywords as possible. If this field is empty or only contains special characters, then the Regex after value must include keywords.
Regex after value	Include as many keywords as possible. If this field is empty or only contains special characters, then the Regex before value must include keywords.
Name	Only use alphanumeric characters. Ensure all characters are lower case and use underscores instead of spaces as this makes fields easier to view. Keep in mind that names for content pack fields and user fields can be the same, though content pack fields will have a namespace in parenthesis to the right of the field name. Prefix content pack fields with an abbreviation, for example vmw_, to avoid confusion.
Keyword Search Terms	One or more keywords, separated by space, that appear within events containing the field.
Filter	A static field, operator, and a potential value that appears within events containing the field. It is common to use this in conjunction with the vRealize Log Insight agent and tags for events that do not contain keywords.
Information ("i" button)	Used to provide information about the field including what it means, what potential values could be returned, and possibly a user-friendly mapping of values to human-understandable information.

Best Practices

In addition to the various components that make up a field, several best practices apply.

- Only create fields for regular expression patterns. If a field can be queried using keyword queries, or will only ever return a single value, then use keyword queries instead of a pre-defined field. If a field will only return two values then consider constructing individual queries instead of extracting a field. Fields are meant to add structure to unstructured data as well as provide a way to query over specific parts of an event.
- Only create fields for regular expression patterns that return a fraction of the total events. Fields that will match most events and/or return a very large number of results are not a good candidate for field extraction. The regular expression will need to be applied to a large quantity of events resulting in a resource intensive operation. If possible add additional keywords to reduce the number of results returned and optimize the query.
- If a field contains keywords within regular expression syntax, then add such keywords as a filter without regular expression syntax. For example, if the value or the context of a field contains keywords within regular expression syntax such as *this*|*that*, then add the keywords as a text filter to optimize the query like **`text contains this, that`**.

- Use of the additional context with one or more keywords is recommended over complex regular expressions in the before or after context.
- Add additional context to all extracted fields in order to optimize query performance.

Temporary Fields

A temporary field is a field that exists as part of a query, but is not saved globally within a vRealize Log Insight instance or as part of an installed content pack.

vRealize Log Insight reduces the chances of creating a temporary field by automatically updating the query that relies on a field being modified.

Note If you delete a field that a saved query relies on, the saved query contains a temporary field.

You can see temporary fields when you run a saved query in the Interactive Analysis page and a field used in the saved query contains the namespace Temporary to the right of the field name.

Queries to contain one or more fields. For saved queries in vRealize Log Insight the field definition used when a query is saved will be modified if the field is modified. Field modifications include

- Changing the field value
- Changing the regex before value and the regex after field value
- Changing the name of the field
- Deleting the field

When you export a content pack vRealize Log Insight converts all temporary fields to content pack fields. If you see a temporary field in a content pack, you might be looking at a content pack from a previous product version that is exported with temporary fields, or the content pack is manually edited.

If a temporary field exists with the same name as an existing extracted field, the temporary field displays ending in {n}. For example, if you have a field called `product_test_field`, product_test_field {2} might also be visible during export. If you see this behavior, a temporary field exists. To address the issue, choose the **Select None** option at the bottom of the export dialog box and select each dashboard and/or alert until the extract field(s) with the {n} ending are checked. Go to those dashboards and/or alerts and edit each query. When you find a query using the extracted field, change the filter or aggregation to use the field without the {n} ending, run the query, and save the query. After you complete these steps for all queries using a field ending in {n}, the field no longer displays during export.

Aggregation Queries

vRealize Log Insight lets you manipulate the visual representation of events by using aggregation queries.

Aggregation queries consist of two district attributes

- Functions
- Groupings

An aggregation query requires one function and at least one grouping. Groupings are an important part of the content packs. Functions and groupings impact the way charts are displayed.

Bar Charts

By default, the overview chart in the Interactive Analysis page of vRealize Log Insight displays a count of events over time. If you use the count function in conjunction with the time series grouping, vRealize Log Insight creates a bar chart.

If you use the count function in conjunction with a single field grouping instead of time series, vRealize Log Insight creates bar charts with quantities listed from greatest to least.

Line Charts

All functions, except the count function, are mathematical. They require a field, against which you apply the equation. When performing a mathematical function on a field and grouping by time series, vRealize Log Insight creates a line chart.

Stacked Charts

By default, the overview chart on the Interactive Analytics page of vRealize Log Insight is a count of events over time. If you add one field to the time series grouping, then vRealize Log Insight creates a stacked chart.

If you use grouping by time series, plus a field, and you use any function except count, vRealize Log Insight creates stacked line chart. Stacked charts are powerful when attempting to find anomalies for an object.

You must decide which type of stacked chart to use, based on the number of object that the aggregation query might return. Displaying more objects require more resources, that are needed to parse and display information. In addition, the number of colors is fixed, and distinguishing between objects might become challenging, depending on the number of returned objects. In general the following best practices apply

- If the number of returned objects in each bar is less than ten, then you might want to use stacked charts.
- If the number of returned objects in each bar is or could be between ten and twenty, then stacked charts could be good. You must consider the way to visually represent the chart in a content pack.
- If the number of returned objects in each bar is or could be greater than twenty, then stacked charts are discouraged.

Multi-Colored Charts

If you create a grouping by using more than one field and time series, then vRealize Log Insight creates a multi-colored chart. The chart consists of two colors that interchange. Each interchange represents a new time range. Multi-colored charts can be hard to interpret so consider the value of such a chart before including it in a content pack.

When you make a grouping by multiple fields, consider using non-time series. Removing time series makes the bar chart easier to understand.

If multiple fields are important in a given time range, then you can create multiple charts for each field individually over the time range. You can then display the charts in the same column of a dashboard group in a content pack.

Other Charts

Several other chart types are available, including pie, bubble, and table charts. To use these charts, a specific query type is required. If the option for these charts are available, then you already have the correct query. If the option for these charts is not available, hover over the chart name you want to use. A pop-up message describes the type of query required for the chart type.

Message Queries

When constructing an aggregation query, the message query should only return results relevant to the aggregation query. This makes analyzing easier and ensures that only results only show relevant fields. To ensure the message query returns the same results as the aggregation query, you must add filters using the *exists* operator for each field that is used in the aggregation query.

Changing Chart Type

If you want to change the chart type of a widget on a dashboard, click the gear icon on the widget and select **Edit Chart Type**. If you want to change a widget type, save a new widget and delete the old widget.

Alerts

Alerts provide a way to trigger a reaction when a certain type of event occurs.

vRealize Log Insight supports two types of alerts

- Email
- vRealize Operations Manager

You can save alerts only in a user space. By default all content pack alerts are disabled. If you create an enabled alert and export it as a part of a content pack, the alert will be disabled in the content pack.

Content packs do not contain email and vRealize Operations Manager settings. And you cannot add these settings to a content pack.

Thresholds

Thresholds set a limit to the number of triggered alerts.

It is important to understand how thresholds work to ensure that, if enabled, a content pack alert does not unintentionally spam a user. When considering the usage of a threshold, there are two questions you must keep in mind

- How frequently to trigger the alert? Log Insight comes with pre-defined frequencies. Alerts will only trigger once for a given threshold window.
- How often to check if an alert state has occurred? An alert is triggered by a query. Alerts, like queries, are not real-time in the current version. For each threshold window, a pre-determined query frequency is allocated. Changing the threshold changes the query time.

Groupings

When you create an email alert it is important to group by a field that identifies the source of the alert.

The email that the alert sends contains a table of results for a particular aggregation query. You can see the visual representation of the query on the Interactive Analytics page.

Without a unique identifier to group by you will not know if the result is relevant for one or multiple systems in your environment. You should group by hostname field and not by source field. You can also add any field that uniquely identifies where the event comes from.

Dashboards Best Practices

Dashboards are part of the content packs. There are some best practices that apply when creating dashboards.

When creating dashboards, the following best practices apply

- Content packs usually contain a minimum of three dashboards. The best practice is to start with an overview dashboards to provide high-level information about the events for a particular product or application. In addition to the overview dashboards, dashboards should be created based on logical groupings of events. The logical groupings are product-specific or application-specific, but some common approaches are performance, faults, and auditing. It is also common to create dashboards for a component, like disk and controller. With the component approach, it is important to note that it is only effective if queries can be constructed to return results from specific components. If this is not possible, then the logical approach is recommended.
- When you name dashboards, make the title generic and avoid adding product-specific or application-specific names unless being used in a component specific fashion. For example, in the VMware - vSphere content pack, there is a dashboard groups called ESX/ESXi instead of VMware ESX/ESXi.

- Dashboards must contain a minimum of three dashboard widgets and a maximum of six dashboard widgets. With any less than three dashboard widgets the amount of knowledge that can be attained by dashboards is minimal. In addition, having a lot of dashboards with only a limited amount of dashboard widgets requires a user to switch between different pages and does not provide information in a coherent way.

  Conversely, any more than six dashboard widgets for dashboards can have negative impact. You might get too much information that might be confusing. Too many widgets require intense usage of your system resources, as each widget is a query that must be run against the system.

  When you include more than six dashboard widgets in dashboards, you must separate the information and create multiple dashboards. If a dashboard widget is applicable to one or more dashboards, create the widget in each applicable dashboards.

Dashboard Filters

Dashboard filters can be used to drill down to specific events. The filters function similar to the filters on the Interactive Analytics page and leverage fields to drill down. Every dashboard should have at least one dashboard filter, typically with the hostname field, but up to five fields can be added to each dashboard.

The field added should be used by the majority of widgets on a given dashboard so that if the dashboard filter is used, most of the widgets return results. Examples of dashboard filters could include a severity field, a user field, or even a component field.

Note The field and the operator used by the dashboard filter will be saved in an exported content pack. Any value used by a dashboard filter will not be saved during export as the value is likely to be specific to an environment and not generic to all environments.

Dashboard Widgets

Dashboard widgets help you visualize information.

There are several types of widgets in vRealize Log Insight that you can add to a dashboard. These include:

- A Chart widget that contains a visual representation of events with a link to a saved query.
- A Query List widget that contains title links to saved queries.
- A Field table widget that contains events where each field represents a column.
- A simplified Event Types table widget that contains similar events combined in single groups.
- A simplified Event Trends table widget that shows a list of event types found in the query, sorted by number of occurrences. This is a quick way to see what sorts of events are happening very frequently in a query.

Chart

A dashboard chart widget contains a visual representation of events. You can represent a chart as a bar or line chart and either can be displayed as a stack.

There are several ways to represent charts:

- Charts can contain a lot of information. Avoid having more than two chart widgets in a single row. In some rare cases, three chart widgets can be used effectively, but more than three is strongly discouraged. When determining whether chart widgets are readable or not, be sure to use the minimum resolution supported by vRealize Log Insight, which is 1024 x 768 pixels.
- If any row except the last row has a single chart widget, then make that widget full-width
- When naming a chart widget, use a descriptive title and avoid cryptic field names. For example, an extracted field is called `vmw_error_message`. Instead of calling a chart Count of `vmw_error_message`, call it Count of error messages

- You can save similar charts and stack them in the same column of a dashboard group for visual comparison. For example:
  - Average X of events over time + Maximum X of events over time. Given the different functions used, the Y-axis of the charts might have a different scale.
  - Count of events over time grouped by X + Count of events over time grouped by Y.

Query List

A dashboard query list widget contains one or more links to pre-defined queries.

You can use Query list widgets for the following reasons

- When a chart widget does not provide significant value, but the underlying query does.
- To save complex queries such as those using regular expressions.
- To use different aggregations on the same underlying query within a dashboard group.

Field Table

A Field Table that contains events where each field represents a column.

A dashboard field table widget contains the latest events for the given query in a table format where each field represents a column.

You can use a field table widget for the following reasons.

- To see the latest events for the given query. This can be useful for change management or for security reasons.
- To see only the fields you care about for a given query. This can be useful to limit event output.

Content Pack Import Errors

When you import a content pack, you might get some warnings or error messages.

Upgrade

You might get an upgrade message. It means that another content pack is installed in the system that has the same namespace. In this case you can either upgrade, and replace the existing content pack, or cancel the upgrade process and keep the existing content pack.

Invalid Format

You might get a message stating the format is invalid. This means that the VLCP file is manually edited and contains syntax errors. The syntax errors must be fixed before you import the content pack.

Newer Version

This type of message implies that the content pack is created and is supported only oin a newer version of Log Insight. On product versions, later than Log Insight 1.5 seeing this type of message means that the VLCP file is manually edited.

Unrecognized Version

When the VLCP file is manually edited and contains syntax errors you might see this type of message. You must fix the syntax errors before you attempt to import the content pack.

Note You should not edit VLCP files manually. As a result, it is hard to locate and fix syntax errors.

Requirements for Publishing Content Packs

When you create and want to publish a content pack, make sure the content packs meet the basic publishing requirements.

You must check both the content pack requirements and the publishing requirements.

Content Pack Requirements

Content packs must meet some requirements for the content, quality and standards.

The content requirements include

- Minimum of three dashboards
- Minimum of one, ideally three, and up to five dashboard filters per dashboard
- Minimum of three dashboard widgets per dashboards
- Maximum of six dashboard widgets per dashboards
- Maximum of three dashboard widgets per row
- Minimum of five alerts
- Minimum of twenty extracted fields

The quality requirements for a content pack are the following

- Every query has at least one full-text keyword and ideally three or more keywords
- Queries are not based on environment specific attributes like source, hostname, or *facility**
- Every field has at least one full-text keyword and ideally three or more keywords
- Fields are specific to product/application and will not return results for other product/application logs
- Every dashboard widget must contain information/links on what the chart shows and why it is important

The standards for creating content packs follow these rules

Content pack part	Format
Content pack name format	*Company - Product*
Content pack namespace format (content pack must be exported with namespace)	*Ext.Domain.Product*
Extracted field format	*Prefix_Field_Name* Where Prefix is the company name or company abbreviation.

Publishing Requirements

Before you publish a content pack, check if it meets the publishing requirements. Use the content pack publisher on the Developer Center for content pack recommendations and to upload a version for review to VMware. https://developercenter.vmware.com/web/loginsight

Publishing Requirement	Description
Content Pack file format	A VLCP file.
Events	The appropriate events necessary to validate content pack.
Overview	A one to two paragraph overview of the content pack.
Highlights	Three highlights, demonstrating the value of the content pack.

Publishing Requirement	Description
Description	A two to three paragraph description of the content pack and its value.
Tech Specs	Describe the minimum system requirements including Product versions and configuration and Log Insight version and configuration. In addition, provide all directions require to configure the product to log to Log Insight and populate the content pack.
Screenshots	Three or more screenshots showing the content pack with real data.
Video (Optional)	Example of how the content pack brings value.
White Paper (Optional)	How to configure the product or application to forwards logs to vRealize Log Insight.

Submit Content Pack

Submit the content pack you created on VMware Solutions Exchange.

Prerequisites

- Verify that your content pack meets the "Requirements for Publishing Content Packs," on page 48.
- If you do not have an account on http://solutionexchange.vmware.com, click the **Register** and select **Partner**. Fill out the Partner Registration Request form and submit. You will receive a notification email if your login request is approved.

Procedure

1. Go to http://solutionexchange.vmware.com and click **Log In Now** in the top right corner of the page.
2. Enter your username and password and click **Log In Now**.
3. Click the **Administration** and choose **Manage Solutions** to add or edit a solution.
4. Click **Add Solution** and fill out the required information.

   Use the **Save Draft** button frequently to make sure that you do not lose any of your work.
5. Click **Submit for Approval**.

   Your solution is sent to the VMware Solution Exchange Alliance Team for review and approval.

You will receive an email regarding the approval status of your solution.

What to do next

For more information about completing a solution listing click the **Partner Corner** link at the top of the page. If you do not find the information you need, contact VSXAlliance@vmware.com with any questions.

Alert Queries in vRealize Log Insight

You can configure vRealize Log Insight to run specific queries at scheduled intervals.

If the number of events that match the query exceeds the thresholds that you have set, vRealize Log Insight can send email or webhook notifications and trigger notification events in vRealize Operations Manager.

To view the list of available alerts, navigate to the Interactive Analytics page and select **Manage Alerts...** from the **Create and manage alerts...** drop-down menu next to the **Search** field. The status of each alert appears under the alert name.

Note Alert queries are user specific. You can manage only your own alerts.

Types of Alerts that You Can Create in vRealize Log Insight

You can control the intervals at which alert queries run, and the conditions when vRealize Log Insight sends alert notifications by selecting one of the alert types.

Alert for Any Match	The alert query runs automatically every five minutes. A notification is triggered when at least one event within the last 5 minutes matches the query.
Alert Base on Event Type	The alert query runs automatically every five minutes. A notification is triggered when a specified event type is seen.
Alert Based on Number of Events Within a Custom Period of Time	Alert query intervals depend on your settings. A notification is triggered according to your settings, when more or less than *X* matching events occur in the last *Y* minutes. If this type of alert is triggered, it is snoozed for the duration of its time period to prevent duplicate alerts from being raised for the same set of events. If you want to enable an alert while it is snoozing, you can disable and then re-enable it.
Alerts Based on Aggregation Queries	The aggregation query alert triggers a notification if value in a function in a grouping exceeds a value you define. You can see this on a chart, where at least one bar in the chart is above or below the threshold that you have set, within the period that you specified. This alert type can be set for charts that do not visualize **Count** of events **over time**.

Content Pack Alerts

Content packs can contain alert queries. The vSphere content pack that is included in vRealize Log Insight by default contains several predefined alert queries. They can trigger alerts if an ESXi host stops sending syslog data, if vRealize Log Insight can no longer collect events, tasks, and alarms data from a vCenter Server, or when an alarm status changes to red. You can use these alert queries as templates to create alerts that are specific to your environment.

All content pack alerts are disabled by default.

Enabling the **vCenter Server: ESX/ESXi stopped logging** alert is a good practice, because certain versions of ESXi hosts might stop sending syslog data when you restart vRealize Log Insight. This alert monitors for the vCenter Server event `esx.problem.vmsyslogd.remote.failure` to detect whether there is an ESXi host that has stopped sending syslog feeds. For details about syslog problems and solutions, see VMware ESXi 5.x host stops sending syslogs to remote server (2003127).

You can add the following filter to the alert query and save it as a new alert to detect only ESXi hosts that stop sending feeds to your instance of vRealize Log Insight: **vc_remote_host (VMware - vSphere) contains** *log-insight-hostname*.

Content pack alert queries are read-only. To save changes to a content pack alert, you have to save the alert to your custom content.

- Add an Alert Query to Send Email Notifications on page 51

  You can configure alert queries in vRealize Log Insight to send email notifications when specific data appears in the logs.

- About Using Webhooks to Send Alerts to Third-Party Products on page 52

  You can send vRealize Log Insight user alerts to third-party products by using webhooks.

- View Alert Queries on page 57

  You can view the alert queries that you have created and check whether the notifications for these queries are enabled.

- Modify Alert Queries on page 57

  You can change the trigger of alert queries, enable or disable the notifications that a query sends, or change the notification method (email, webhook, or send to vRealize Operations Manager.

- Enable Alert Queries on page 59

  When an alert query is disabled, vRealize Log Insight does not send email or webhook notifications and does not trigger vRealize Operations Manager notification events.

- Delete Alert Queries on page 60

  You can delete alert queries when you no longer need them.

Add an Alert Query to Send Email Notifications

You can configure alert queries in vRealize Log Insight to send email notifications when specific data appears in the logs.

Prerequisites

- Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.
- Verify that an administrator has configured SMTP to enable email notifications. See Configure the SMTP Server for Log Insight.

Procedure

1 On the **Interactive Analytics** tab, run the query for which you want notifications to be sent .

2 From the **Create or manage alerts** menu on the right of the **Search** button, click  and select **Create Alert from Query**.

3 In the Add Alert dialog box, type a name for the alert, and provide a short meaningful description of the event that triggers the alert.

The alert name and description are included in the email that vRealize Log Insight sends.

4 Select the **Email** check-box and type the email address to which you want vRealize Log Insight to send the notifications.

Use commas to separate multiple addresses.

5 Set the alert threshold.

Alert Type	Selection
Any Match	Select the **on any match** option. Queries run every 5 minutes.
Based on the event type	Select the **When a new event type is seen** option. Queries run every 5 minutes.

Alert Type	Selection
Based on number of events within a period of time	Select the third option and use the drop-down menus to set the parameters. Queries run based on your selection in the drop-down menu.
Based on chart values	Select the fourth option and use the drop-down menus to configure the parameters. **Note** This alert type is available only if you select to group events according to at least one field. You cannot create this alert type for charts that visualize only time series. Queries run based on your selection in the second drop-down menu.

The orange line in the preview chart shows the current threshold.

6 Click **Save**.

What to do next

You can enable, disable, or delete your saved alerts.

Note Alert queries are user specific. You can manage only your own alerts.

About Using Webhooks to Send Alerts to Third-Party Products

You can send vRealize Log Insight user alerts to third-party products by using webhooks.

vRealize Log Insight uses webhooks to send alerts over HTTP POST to other applications. vRealize Log Insight sends a webhook in its own proprietary format, but third-party solutions expect incoming webhooks to be in their pwn proprietary format. To use information sent with vRealize Log Insight webhooks, the third-party application must have either native support for the vRealize Log Insight format or you must create a mapping between vRealize Log Insight formats and the format used by the third-party with a shim. The shim translates, or maps, the vRealize Log Insightformat to a different format.

System notifications, alerts created with message queries, and alerts created with aggregate queries each have their own webhook format.

You must be a vRealize Log Insight administrator to create system notifications.

Authenticated webhooks are not supported.

Add an Alert Query to Send Webhook Notifications

You can configure alert queries in vRealize Log Insight to send webhook notifications to a remote web server when specific data appears in the logs. Webhooks provides event notifications over HTTP POST.

Prerequisites

- Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.
- Verify that a webserver has been configured to receive webhook notifications.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 From the **Create or manage alerts** menu on the right of the **Search** button, click  and select **Create Alert from Query**.

3 In the Add Alert dialog box, type a name for the alert, and provide a short meaningful description of the event that triggers the alert.

The alert name and description are included in the notification that vRealize Log Insight sends.

4 Select the **Webhooks** check-box and enter the URL to which you want vRealize Log Insight to send the notifications.

5 Set the alert threshold.

Alert Type	Selection
Any Match	Select the **on any match** option. Queries run every 5 minutes.
Based on the event type	Select the **When a new event type is seen** option. Queries run every 5 minutes.
Based on number of events within a period of time	Select the third option and use the drop-down menus to set the parameters. Queries run based on your selection in the drop-down menu.
Based on chart values	Select the fourth option and use the drop-down menus to configure the parameters. **Note** This alert type is available only if you select to group events according to at least one field. You cannot create this alert type for charts that visualize only time series. Queries run based on your selection in the second drop-down menu.

The orange line in the preview chart shows the current threshold.

6 Click **Save**.

What to do next

You can enable, disable, or delete your saved alerts.

Note Alert queries are user specific. You can manage only your own alerts.

About Writing Translation Shims for vRealize Log Insight Alerts

Shims are used to map varying webhook formats.

vRealize Log Insight sends a webhook in its own proprietary format and third-party solutions expect incoming webhooks to be in their proprietary format. This means either the third-party solution needs to have native support for the vRealize Log Insight format or a shim between vRealize Log Insight and the third-party solution is needed which translates vRealize Log Insight format to third-party format.

The following figures show a user alert query and the webhook that is generated for it. You can use this information to better understand the mapping required for supporting shims.

Figure 1-1. User-defined Alert Query

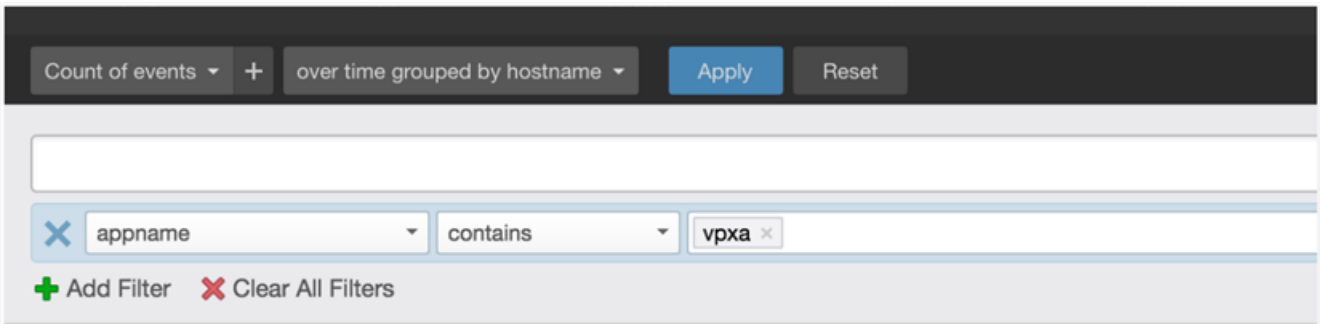


Figure 1-2. Webhook Output for the User Alert Aggregation Query


```
{
   "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
}
```


Webhook Format for User Alert Message Queries

The format used by a vRealize Log Insight webhook depends on the type of query from which it is created. System notifications, user alert message queries, and alerts generated from aggregate user queries each have a different webhook format.

When you send an alert generated by a user alert message query to a third-party program, you must write a shim to make vRealize Log Insight information understandable by the third-party program's formats.

User Alert Message Query Webhook Format

The following example shows the format of a vRealize Log Insight webhook for a user alert message query.

```
{
   "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
}
```

Webhook Format for a User Alert Aggregation Query

The format used by a vRealize Log Insight webhook depends on the type of query from which it is created. System notifications, user alert message queries, and alerts generated from aggregate user queries each have a different webhook format.

When you send a system notification to a third-party program, you must write a shim to make vRealize Log Insight information understandable by the third-party program's formats.

Webhook Format for User Alert Aggregation Queries

```
{
   "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
}
```

Webhook Format for a User Alert Aggregation Query

The format used by a vRealize Log Insight webhook depends on the type of query from which it is created. System notifications, user alert message queries, and alerts generated from aggregate user queries each have a different webhook format.

When you send a system notification to a third-party program, you must write a shim to make vRealize Log Insight information understandable by the third-party program's formats.

Webhook Format for User Alert Aggregation Queries

```
{
   "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
}
```

View Alert Queries

You can view the alert queries that you have created and check whether the notifications for these queries are enabled.

Note Alert queries are user specific. You can manage only your own alerts.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 From the menu on the right of the **Search** button, click and select **Manage Alerts**.

You see a list of all your alert queries. The status of alert notifications is displayed under the name of the alert.

What to do next

You can click alert queries in the list to modify their parameters, or delete the queries that you no longer need.

Content pack alert queries are read-only. To save changes to a content pack alert, you have to save the alert to your custom content.

Modify Alert Queries

You can change the trigger of alert queries, enable or disable the notifications that a query sends, or change the notification method (email, webhook, or send to vRealize Operations Manager.

Note Alert queries are user specific. You can manage only your own alerts.

Content pack alert queries are read-only. To save changes to a content pack alert, you have to save the alert to your custom content.

You can apply your changes to one or more alerts at the same time.

Prerequisites

- Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.
- Verify that an administrator has configured SMTP to enable email notifications. See Configure the SMTP Server for Log Insight.
- Verify that an administrator has configured the connection between vRealize Log Insight and vRealize Operations Manager to enable alert integration. See Configure Log Insight to Send Notification Events to vRealize Operations Manager.
- If you are using webhooks, verify that a webserver has been configured to receive webhook notifications.

Procedure

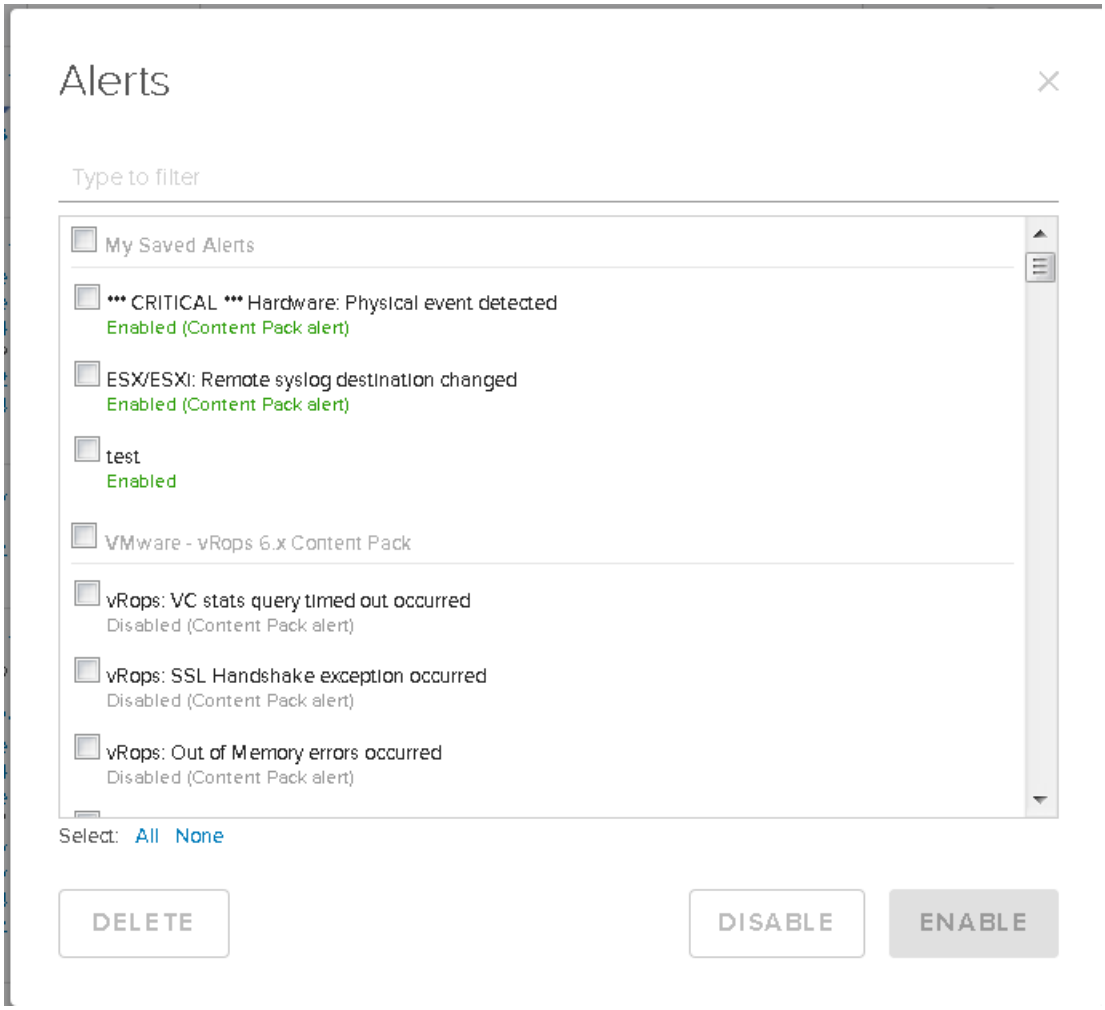
1 Navigate to the **Interactive Analytics** tab.

2 From the **Create or manage alerts** menu on the right of the **Search** button, click and select **Manage Alerts**.

3 In the Alerts list, select one or more alert query that you want to modify, and change the query parameters as needed.

You can find queries by entering a string as a filter. Queries are labeled as enabled or disabled and whether they are a Content Pack query.

Note If you deselect all notification options, the alert query is disabled.



4 Save your changes.

Option	Description
Save	This button appears when you modify your own alerts.
Save to My Alerts	This button appears when you modify a shared alert or a content pack alert. The original alert remains unchanged, but you save a copy of the alert to your custom content.

Enable Alert Queries

When an alert query is disabled, vRealize Log Insight does not send email or webhook notifications and does not trigger vRealize Operations Manager notification events.

Note Alert queries are user specific. You can manage only your own alerts.

An alert query is disabled under the following conditions.

- If you disable all notification options in the Edit Alert dialog box.
- If the alert is part of a content pack.

Content pack alert queries are read-only. To save changes to a content pack alert, you have to save the alert to your custom content.

Prerequisites

- Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.
- Verify that an administrator has configured SMTP to enable email notifications. See Configure the SMTP Server for Log Insight.
- Verify that an administrator has configured the connection between vRealize Log Insight and vRealize Operations Manager to enable alert integration. See Configure Log Insight to Send Notification Events to vRealize Operations Manager.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 From the **Create or manage alerts** menu on the right of the **Search** button, click  and select **Manage Alerts**.

3 In the Alerts list, click one or more alert queries that you want to enable.

4 Select the notification options that you want to enable, and provide the required parameters.

Option	Description
Email	Enter at least one email address in the text box. Use commas to separate multiple addresses.
Webhook	Enter the URL to which you want vRealize Log Insight to send the notifications.
Send to vRealize Operations Manager	Select a vRealize Operations Manager resource to associate with the notifications events, and select the criticality level of the events.

5 Save your changes.

Option	Description
Save	This button appears when you modify your own alerts.
Save to My Alerts	This button appears when you modify a shared alert or a content pack alert. The original alert remains unchanged, but you save a copy of the alert to your custom content.

When the alert query returns results that match the alerting criteria, vRealize Log Insight sends notifications according to your configuration.

Example: Enable an Alert from the VMware - vSphere Content Pack

The VMware - vSphere content pack contains several predefined alert queries, including the **vCenter Server: ESX/ESXi stopped logging** alert.

Enabling the **vCenter Server: ESX/ESXi stopped logging** alert is a good practice, because certain versions of ESXi hosts might stop sending syslog data when you restart vRealize Log Insight. This alert monitors for the vCenter Server event `esx.problem.vmsyslogd.remote.failure` to detect if there is an ESXi host that has stopped sending syslog feeds.

1 On the **Interactive Analytics** tab, expand the drop-down menu on the right of the **Search** button, and select **Manage Alerts**.

2 Under VMware - vSphere Content Pack, click **vCenter Server: ESX/ESXi stopped logging**.

3 Enable Email notifications, Webhook notifications, or vRealize Operations Manager notification events.

4 Click **Save to My Alerts**.

To detect only ESXi hosts that stop sending feeds to your instance of vRealize Log Insight, you can add the following filter to the alert query: **vc_remote_host (VMware - vSphere) contains** <*log-insight-hostname*>, and save the new query to your alerts.

For details about syslog problems and solutions, see the Knowledge Base article VMware ESXi 5.x host stops sending syslogs to remote server (2003127) at https://kb.vmware.com/kb/2003127.

Delete Alert Queries

You can delete alert queries when you no longer need them.

Note Alert queries are user specific. You can manage only your own alerts.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 From the menu on the right of the **Search** button, click  and select **Manage Alerts**.

3 Select one or more alerts that you want to delete and click **Delete** or the delete icon  .

4 In the **Delete Alert** dialog box, select **Delete** to confirm the action.

Index