VMware vCenter Log Insight User's Guide

vCenter Log Insight 1.5

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001300-00

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

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About VMware vCenter Log Insight User's Guide

The *VMware vCenter Log Insight User's Guide* provides information about using the Web user interface of VMware® vCenter™ Log Insight™, including procedures about filtering and searching log messages, performing analysis on the search results, and dynamically extracting fields from log messages based on customized queries.

Intended Audience

This information is intended for anyone who wants to use Log Insight.

Using Log Insight 1

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.

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

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

Near Real-Time Search

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

Log Insight supports complete keyword queries. Keywords are defined as any alpha-numeric, hyphen, or underscore characters. In addition to the complete keyword queries, 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 constraints (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 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.

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 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. 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 Log Insight must read the VMware vCenter Log Insight Security Guide.

The Security Guide contains concise reference to the security features of 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:

Overview of the Log Insight Web User Interface

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

Content packs can be imported or created by Log Insight users. See "Working with Content Packs," on page 26.

The Administration User Interface

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 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 constraint, by using the drop-down menus and the text box above the list of log events.

Within a single-row constraint, you can use comma-separated values to list OR constraints. 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** constraint treats each comma separated value as a complete keyword.

You can combine multiple field constraints by creating a new constraint row for each field. You can toggle the operator that is applied on multiple-row constraints .

- 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 constraint 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.

Information in Log Events

You can ingest logs in Log Insight by using syslog.

Each event contains the following information.

Type	Description
Timestamp	The time when the event occurred
Source	Where the event came from. This could be the originator of the syslog messages such as an ESXi host, or a forwarder such as a syslog aggregator.
Text	The raw text of the event
Fields	A name-value pair extracted from the event

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 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 Log Insight virtual appliance.

Procedure

1 From the **Time Range** drop-down menu on the right, select one of the predefined periods.

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

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 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 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 **Search**.

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

Prerequisites

Verify that you are logged in to the 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 Log Insight virtual appliance.

Procedure

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

2 Click **Add Constraint**.

3 In the constraint row under the search text box, use the first drop-down menu to select any field defined within 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 constraint **response_time = `02`** will match an event that contains a **response_time** field with a value 2. The constraint **response_time contains `02`** will not have the same match.

4 In the constraint 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** constraint matches full tokens: searching for "err" will not find "error" as a match.

5 In the text box to the right of the constraint 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 constraints, click **Add Constraint**.

A toggle button appears above the constraint rows.

7 (Optional) For multiple constraint rows, select the operator between constraints.

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

By default, **all** is selected.

8 Click **Search**.

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 constraint.

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 **Search**.

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 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 Log Insight virtual appliance.

Procedure

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

2 At the right of the event row, click the **Set time range from this event** icon 🕒.

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 constraints that you have specified previously.

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 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 Log Insight virtual appliance.

Procedure

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

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

3 Click **Search**.

Examples of Search Queries

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

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

IMPORTANT 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 constraint.

   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 **Search**.

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 constraint.

   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 **Search**.

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 constraint.

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

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

3 Click **Search**.

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 constraint.

   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 constraint.

   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 **Search**.

Using the Interactive Analytics Chart to Analyze Logs

The chart at the top of the **Interactive Analytics** tab 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.

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.

Type	Field	Description
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 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 Log 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 **Time Range** drop-down menu 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 drop-down menu to the right of the **Search** button, select A**dd Current Query to Dashboard**. 2 Type a name, select the destination dashboard from the drop-down menu, add information about the widget, and click **Add**.
Save a query as a chart to your custom dashboard	1 Select the drop-down menu next to the **Search** button. 2 Select **Add Current Query to Dashboard**. 3 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**.
Delete a chart from your custom dashboard	1 On the **Dashboards** tab, select the custom dashboard that contains the graph that you want to delete. 2 In the upper right corner of the graph 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 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 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** check box.
- To view only event values, deselect the **Time series** check box 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 Log Insight charts.

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

Selection in the First Drop-Down Menu	Selection in the Second Drop-Down Menu	Selection in the Third Drop-Down Menu	Text Displayed on the Screen	Result
Count	**Time series**	N/A	**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.	N/A	**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**	N/A	**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.

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 19.

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 Normal view. You cannot use this option in Raw view. On the **Interactive Analytics** tab, use the **View** drop-down menu above the list of log events to switch between views.

Prerequisites

Verify that you are logged in to the 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 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 **Extract Field** button appears next to the set of field names present in that event.

3 Click **Extract Field**.

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

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

5 (Optional) Modify the Context regular expression in the Fields pane.

6 If you are an administrator user, select which users can access the field.

Option	Description
All users	All users will see the field in the search drop-down menu.
Me only	Other users will not see the field in the **Search** drop-down menu.

7 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.

Extract Fields from Log Events

You can extract fields from log events and use these fields to search, filter, and aggregate log events.

Prerequisites

Verify that you are logged in to the 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 Log Insight virtual appliance.

Procedure

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

2 In the Fields pane, click **Extract Field**.

3 In the new widget that displays modifiable parameters for the extracted field, select a value type from the drop-down menu.

You can enter a custom regular expression that matches the value of the field that you want to extract in the text box below the drop-down menu.

4 Provide context before or after the value to be extracted.

A context helps eliminate false matches, as it filters out values that do not match the provided prefix and suffix values. You can provide context values as plain text or as a regular expression.

5 (Optional) Type a name for the extracted field.

If you do not provide a name, Log Insight assigns **field1** as a name of the extracted field.

6 If you are an administrator user, select which users can access the field.

Option	Description
All users	All users will see the field in the search drop-down menu.
Me only	Other users will not see the field in the **Search** drop-down menu.

7 Click **Save**.

Example: Example Queries for Field Extraction

You can run these queries on log events that come from a vSphere environment.

Table 1-2. Field Extraction Queries

Field to Extract	Value Type	Value	Context Before Value	Context After Value
Time taken to perform an operation	Integer	-?\d+	took	ms
HTTP version	Decimal	-?\d*\.?\d+	HTTP/	

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.

Examples of Regular Expressions

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

Table 1-3. 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
[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

Modify an Extracted Field

You can modify the definitions of extracted fields.

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.

You can modify only fields that have the **Edit this field** icon ✏ next to their names. 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 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 Log Insight virtual appliance.

Procedure

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

2 In the list of fields to the right, select the field that you want to modify, and click the **Edit this field** icon ✏. If the field does not appear in the list, select the drop-down menu to the right of the search button and select **Manage Extracted Fields**. Click the name of the field you want to edit.

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

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

Delete an Extracted Field

You can delete extracted fields that are no longer needed.

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, 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 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 Log Insight virtual appliance.

Procedure

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

2. In the list of fields to the right, select the field that you want to delete, and click the **Edit this field** icon ✏.

   The field properties appear.

   If the field does not appear in the list, select the menu drop-down menu to the right of the **Search** button and select **Manage Extracted Fields**. Hover over the name of the field you want to delete and click the red **X**.

3. Click **Delete**.

   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, 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, 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.

Save a Query in Log Insight

You can save your current query and time range in 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 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 Log Insight virtual appliance.

Procedure

1. On the **Interactive Analytics** tab, perform the query that you want to save.
2. From the drop-down menu next to the **Search** button, select **Save Current Query**.
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 My Saved Queries list.

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

Rename a Query in Log Insight

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

Prerequisites

Verify that you are logged in to the 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 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. 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 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 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 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 In the Saved 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 Log Insight

You can delete saved queries from Log Insight.

Prerequisites

Verify that you are logged in to the 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 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 **Delete this saved query** icon ✖.

4 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 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 Log Insight virtual appliance.

Procedure

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

2 From the drop-down menu next to the **Search** button, select **Share Current Query**.

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 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 Log Insight virtual appliance.

Procedure

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

2 From the drop-down menu next to the **Search** button, select **Export Query Results**.

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

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

Working with Dashboards

Dashboards in Log Insight are collections of chart and query list widgets.

Custom Dashboards

Custom dashboards are created by users of the current instance of Log Insight. Custom dashboards are organized in two categories, My Dashboards and Shared Dashboards. Shared dashboards are visible to all users of the 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 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 Log Insight, click **Dashboards** in the upper left corner of the Log Insight user interface . You can switch between dashboard categories by using the drop-down menu at the upper left.

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 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 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 1-4. 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 **Edit Dashboard Name**. Enter a new name and select **Save.**
Delete a custom dashboard	On the **Dashboards** tab, hover over the dashboard name, click the menu icon ⚙ and select **Delete Dashboard**. In the confirmation dialog box select **Delete**.
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 Dashboard** 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 drop-down menu to the right of the **Search** button, select A**dd Current Query to Dashboard**. 2 Type a name, select the destination dashboard from the drop-down menu, 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 25.
Add a query to a query list widget on a dashboard	See "Add a Query to a Query List Widget in a Dashboard," on page 25.
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 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 Log Insight virtual appliance.

Procedure

1. On the **Interactive Analytics** tab, run the query that you want to add to the dashboard.
2. From the drop-down menu next to the **Search** button, select **Add Current Query to Dashboard**.
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 25.

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 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 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. From the drop-down menu next to the **Search** button, select **Add Current Query to Dashboard**.
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**.

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

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 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 VMware - vSphere content pack is 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 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 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.

Export a Content Pack

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

Content packs are saved as vCenter 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, Log Insight creates these fields within the content pack during the export.

Prerequisites

- If you use Internet Explorer 9, verify that you have Adobe Flash Player installed on your system.
- Verify that you are logged in to the 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 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 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. 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.

Import a Content Pack

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

You can import only vCenter 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, Log Insight creates temporary copies of the fields for each query, chart, or alert that uses a deleted field.

Prerequisites

- If you use Internet Explorer 9, verify that you have Adobe Flash Player installed on your system.
- Verify that you are logged in to the 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 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 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 in 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.

Non-administrator 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.

The imported content appears in the Content Packs or the Custom Content list to the left.

NOTE Imported Alerts are disabled by default. See "Enable an Alert Query," on page 34.

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 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 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 Because content pack elements are grouped by type, click the button that corresponds to the element type .

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.

Alert Queries in Log Insight

You can configure 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, Log Insight can send email notifications and trigger notification events in vCenter Operations Manager.

To view the list of available alerts, navigate to the Interactive Analytics page and select **Manage Alerts** from the drop-down menu next to the **Search** button. 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 Log Insight

You can control the intervals at which alert queries run, and the conditions when 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 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.

Alert Based on Chart Values

The alert query triggers a notification if 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 Log Insight by default contains several predefined alert queries. They can trigger alerts if an ESXi host stops sending syslog data, if 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 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 constraint to the alert query and save it as a new alert to detect only ESXi hosts that stop sending feeds to your instance of 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 in Log Insight to Send Email Notifications on page 30

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

- Add an Alert Query in Log Insight to Send Notification Events to vCenter Operations Manager on page 31

  You can configure alert queries in Log Insight to send notification events to vCenter Operations Manager when specific Log Insight queries return results above a given threshold.

- View Existing Alert Queries on page 33

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

- Modify an Alert Query on page 34

  You can change the trigger of a saved alert query, and enable or disable the notifications that the query sends .

- Enable an Alert Query on page 34

  When an alert query is disabled, Log Insight does not send notification emails and does not trigger vCenter Operations Manager notification events.

- Delete an Alert Query on page 36

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

Add an Alert Query in Log Insight to Send Email Notifications

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

Prerequisites

- Verify that you are logged in to the 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 Log Insight virtual appliance.
- Verify that an administrator has configured SMTP to enable email notifications. See topic in the Log Insight Administration Guide.

Procedure

1. On the **Interactive Analytics** tab, run the query for which you want notifications to be sent .
2. From the drop-down menu on the right of the **Search** button, select **Add Alert for Current 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 Log Insight sends.
4. Select the **Email** check-box and type the email address to which you want 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 number of events within a period of time	Select the second option and use the drop-down menus to set the parameters. Queries run based on your selection in the second drop-down menu.
Based on chart values	Select the third radio button 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.

Add an Alert Query in Log Insight to Send Notification Events to vCenter Operations Manager

You can configure alert queries in Log Insight to send notification events to vCenter Operations Manager when specific Log Insight queries return results above a given threshold.

Notification events that Log Insight generates are associated with resources in vCenter Operations Manager. You can read more about resources in the *vCenter Operations Manager Getting Started Guide (Custom UI)*

NOTE Several minutes are required for notification events to appear in the vCenter Operations Manager user interface.

Prerequisites

- Verify that you are logged in to the 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 Log Insight virtual appliance.
- Verify that an administrator has configured the connection between Log Insight and vCenter Operations Manager to enable alert integration. See topic in the Log Insight Administration Guide.

Procedure

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

2 From the drop-down menu on the right of the **Search** button, select **Add Alert for Current Query…**.

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

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

4 Deselect the **Email** check box or provide at least one email address to receive the notification events.

Use commas to separate multiple addresses.

5 Select **Send to vCenter Operations Manager**.

6 Click **Select** to choose a vCenter Operations Manager resource to be associated with the notification events that Log Insight sends.

7 In the Select vCenter Operations Manager Resource to Receive Alert dialog box, type a resource name or browse for an object in the list.

You can use the drop-down menu to filter resources by power state.

Option	Description
Active VMs	Select to view only resources that are powered on.
All Resources	Select to view all resources, regardless of their power state.

8 From the **Criticality** drop-down menu, select the criticality level for the notification events that appear in vCenter Operations Manager Custom user interface.

9 Set the alert threshold.

Alert Type	Selection
Any Match	Select the **on any match** option. Queries run every 5 minutes.
Based on number of events within a period of time	Select the second option and use the drop-down menus to set the parameters. Queries run based on your selection in the second drop-down menu.
Based on chart values	Select the third radio button 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.

10 Click **Save**.

When the alert query returns results that match the alert criteria, a notification event is sent to vCenter Operations Manager. Alert queries run on a predefined schedule and are triggered only once for a given threshold time range.

The locations where notification events appear depend on the vCenter Operations Manager user interface that you use.

Example: Configure a Notification Alert to vCenter Operations Manager

Assume that in vCenter Operations Manager you have a virtual machine resource named vm-abc.

You have configured Log Insight to pull events from the vCenter Server system where the virtual machine vm-abc runs.

You want to receive a notification in vCenter Operations Manager each time the vm-abc virtual machine is powered off.

Here is how to configure Log Insight to send these notification events to vCenter Operations Manager.

1 In the search text box, type `Power Off virtual machine`.

2 Click **Add a Constraint**, select **vc_vm_name** and type `vm-abc`.

3 Click **Search**.

   If the vm-abc virtual machine has been powered off during the selected time range, the search returns all instances that occurred.

4 From the drop-down menu on the right of the **Search** button, select **Add Alert**.

5 In the Add Alert dialog box, type a name and description for the alert, unselect the **Email** checkbox, and select **Send to vCenter Operations Manager**.

6 Click **Select**, type `vm-abc`, and click **Search** to find the vm-abc resource in the list.

7 Click the vm-abc resource in the list to add it.

8 (Optional) Modify the criticality level that is displayed in the vCenter Operations Manager Custom user interface.

9 Under Raise an alert, select **on any match**.

10 Click **Save**.

Log Insight polls the vCenter Server system at five-minute intervals. If the query returns a new Power Off virtual machine task from VM vm-abc , Log Insight sends a notification event that is associated with the vm-abc resource in vCenter Operations Manager.

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.

View Existing 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 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 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 **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 an Alert Query

You can change the trigger of a saved alert query, and enable or disable the notifications that the query sends .

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.

Prerequisites

- Verify that you are logged in to the 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 Log Insight virtual appliance.
- Verify that an administrator has configured SMTP to enable email notifications. See topic in the Log Insight Administration Guide.
- Verify that an administrator has configured the connection between Log Insight and vCenter Operations Manager to enable alert integration. See topic in the Log Insight Administration Guide.

Procedure

1. Navigate to the **Interactive Analytics** tab.
2. From the drop-down menu on the right of the **Search** button, select **Manage Alerts**.
3. In the Alerts list, click the alert query that you want to modify, and change the query parameters as needed.

   NOTE If you deselect both 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 an Alert Query

When an alert query is disabled, Log Insight does not send notification emails and does not trigger vCenter 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 both 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 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 Log Insight virtual appliance.
- Verify that an administrator has configured SMTP to enable email notifications. See topic in the Log Insight Administration Guide.
- Verify that an administrator has configured the connection between Log Insight and vCenter Operations Manager to enable alert integration. See topic in the Log Insight Administration Guide.

Procedure

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

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

3 In the Alerts list, click the alert query that you want to enable.

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

Option	Description
Email	Type at least one email address in the text box. Use commas to separate multiple addresses.
Send to vCenter Operations Manager	Select a vCenter 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, 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 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 or vCenter Operations Manager notification events.

4 Click **Save to My Alerts**.

To detect only ESXi hosts that stop sending feeds to your instance of Log Insight, you can add the following constraint 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 VMware ESXi 5.0 host stops sending syslogs to remote server (2003127).

Delete an Alert Query

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 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 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 **Manage Alerts**.

3 Select the name of the alert that you want to delete and click the **Delete** icon ❌.

4 In the **Delete Alert** dialog box select **Delete**.

Index