Using VMware vRealize Log Insight Cloud

VMware vRealize Log Insight Cloud

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

https://docs.vmware.com/

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

Contents

Using VMware vRealize Log Insight Cloud

1

vRealize Log Insight Cloud (formerly known as VMware Log Intelligence) provides visibility across public and private cloud environments including AWS. vRealize Log Insight Cloud features robust log aggregation and sophisticated analytics that enable you to determine root causes for an issue quickly and thoroughly.

This chapter includes the following topics:

Sending Data

Set up your log collection with vRealize Log Insight Cloud and learn about the steps for log flows from multiple sources, with recommendations for collections of specific log types.

Setting Up vRealize Log Insight Cloud

Before you begin using vRealize Log Insight Cloud, you must install a Cloud Proxy and configure connections for receiving data from log and event sources.

There are two initial setup tasks.

- Download and install a Cloud Proxy.

  A Cloud Proxy receives log and event information from monitored sources and sends this information to vRealize Log Insight Cloud where it can be queried and analyzed. vRealize Log Insight Cloud includes the Cloud Proxy as a .ova file for you to download and install, typically on a vCenter virtual machine.

  For more information, see Deploy a First Cloud Proxy for vRealize Log Insight Cloud.

- Configure event forwarding for the Cloud Proxy.

  After the Cloud Proxy is in place, you configure your data sources and protocol settings to forward events to the Cloud Proxy. Several protocols are supported, including syslog, rsyslog, syslog-ng and others. Use of the vRealize Log Insight ingestion API and agent are also supported. For more information about protocols, see Port Requirements of Remote Cloud Proxy.

Deploy a First Cloud Proxy for vRealize Log Insight Cloud

You must have an active VMware Cloud Proxy before you can use vRealize Log Insight Cloud. If none are present, you are informed of this when you open the landing page and prompted to begin download and deployment.

Prerequisites

Log in to vRealize Log Insight Cloud by specifying the URL `https://www.mgmt.cloud.vmware.com/li/` and entering your login credentials.

Procedure

1. Click **Add Collector** in the Event Observations widget on the vRealize Log Insight Cloud **Home** page.

   This displays the Set up a Cloud Proxy Virtual Appliance screen. (Leave this screen open, you will need it later.)

2. To deploy the Cloud Proxy, click **Download OVA**.
3. Navigate to your VMware vSphere Web Client data center and click on the name of your vCenter cluster. In the drop-down menu, select **Deploy OVF Template**.
4. In the Deploy OVF Template form, perform the following actions.
   a. Click **Select template**, then **Local File**. Paste in the path to the OVA Cloud Proxy file you downloaded. Click **Next**.
   b. Click **Select name and location**, then enter the name of your OVA file. Select the cluster where you want to install the Cloud Proxy, and click **Next**.
   c. Click **Select a resource** and the cluster where you want to run the Cloud Proxy, and then click **Next**.

d Review the details of your Cloud Proxy deployment. Notice the **Size on disk** text box. The location where you deploy the Cloud Proxy in the following steps must have enough space available. Click **Next**.

e **Accept** the License Agreement. Click **Next**.

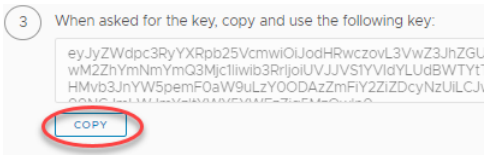
f Click **Select storage** and select a datastore from the list with enough free space for the OVA file. Click **Next**.

g Click **Select networks** and select a destination network, and then click **Next**.

h Click **Customize template** and enter the required information. Do not click **Next**.

- For **Root User Password**, choose a unique password. It does not need to match the vCenter password.

i Return to vRealize Log Insight Cloud and collect the token key provided on the Setup a Cloud Proxy Virtual Appliance form. Click **Copy** to copy the key. Use the **Copy** control to ensure you are copying the entire key.



Token keys are should be used within 24 hours and should be used for only one Cloud Proxy.

j Return to the template form and click **Networking Properties**. If you use DHCP in your vCenter network, do not enter any information. If you do not use DHCP, then you must provide information for each setting. Click **Next**.

k Click **Ready to complete** and review your configuration data. Click **Finish**.

The Cloud Proxy is installed.

5 Click the green arrow at the top of your page to run the Cloud Proxy.

6 To verify that your Cloud Proxy is running, look under the **VMs** tab at the list of your virtual machines to ensure its state is **Powered On**.

7 Return to the vRealize Log Insight Cloud **Set Up a Cloud Proxy Virtual Appliance** form. Wait for a success message saying a connection has been made. (This may take several minutes.)

What to do next

Consult Port Requirements of Remote Cloud Proxyand then enable log and event forwarding to the Cloud Proxy.

Deploy Additional Cloud Proxies for vRealize Log Insight Cloud

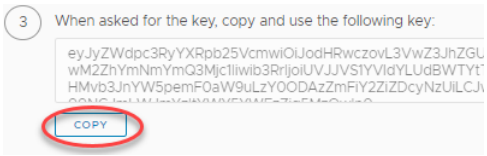
You can deploy additional Cloud Proxies for your installation.

Prerequisites

Log in to vRealize Log Insight Cloud by entering the URL `https://www.mgmt.cloud.vmware.com/li/` and entering your login credentials.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
2. Navigate to **Configuration > Cloud Proxies**.
3. Click **New**.
4. To deploy the Cloud Proxy, click **Download OVA**.
5. Navigate to your VMware vSphere Web Client data center and click the name of your vCenter cluster. In the drop-down menu, select **Deploy OVF Template**.
6. In the Deploy OVF Template form, perform the following actions.
   a. Click **Select template**, then **Local File**. Paste in the path to the OVA Cloud Proxy file you downloaded. Click **Next**.
   b. Click **Select name and location**, then enter the name of your OVA file. Select the cluster where you want to install the Cloud Proxy, and click **Next**.
   c. Click **Select a resource** and the cluster where you want to run the Cloud Proxy, and then click **Next**.
   d. Review the details of your Cloud Proxy deployment. Notice the **Size on disk** text box. The location where you deploy the Cloud Proxy in the following steps must have enough space available. Click **Next**.
   e. **Accept** the License Agreement. Click **Next**.
   f. Click **Select storage** and select a datastore from the list with enough free space for the OVA file. Click **Next**.
   g. Click **Select networks** and select a destination network, and then click **Next**.
   h. Click **Customize template** and enter the required information. Do not click **Next**.
      - For **Root User Password**, choose a unique password. It does not need to match the vCenter password.
   i. Return to vRealize Log Insight Cloud and collect the token key provided on the Setup a Cloud Proxy Virtual Appliance form. Click **Copy** to copy the key. Be sure to use the **Copy** control to ensure that you are copying the entire key.



   Token keys are good for 24 hours and should be used for only one Cloud Proxy.

j Click **Networking Properties**. If you use DHCP in your vCenter network, do not enter any information. If you do not use DHCP, then you must provide information for each setting. Click **Next**.

k Click **Ready to complete** and review your configuration data. Click **Finish**.

The Cloud Proxy is installed.

7 Go to the vSphere Web Client and click the green arrow at the top of your page to run the Cloud Proxy.

8 To verify that your Cloud Proxy is running, look under the VMs tab at the list of your virtual machines to ensure it is **Powered On**.

9 Return to the vRealize Log Insight Cloud **Set Up a Cloud Proxy Virtual Appliance** form. Wait for a success message saying a connection has been made. (This may take several minutes.)

What to do next

Consult Port Requirements of Remote Cloud Proxyand then enable log and event forwarding to the Cloud Proxy.

Port Requirements of Remote Cloud Proxy

You can forward events and logs from syslog and vRealize Log Insight sources.

Port Requirements

Before you configure event forwarding, become familiar with port requirements for the Cloud Proxy.

Source	Destination	Port	Protocol	Service Description
Standard system log	Remote Cloud Proxy	514	TCP,UDP	Syslog data over TCP or UDP
vRealize Log Insight Agents or Server	Remote Cloud Proxy	9000	TCP	vRealize Log Insight log data in JSON format (CFAPI)
Remote Cloud Proxy	vRealize Log Insight Cloud	443	TCP	vRealize Log Insight Cloud data over HTTPS

Syslog Agents for vRealize Log Insight Cloud

The remote Cloud Proxy supports any agent sending syslog RFC 3195 or RFC 5424 compliant messages.

For best results, use the following agents:

- Rsyslog
- Syslog-ng
- NXLOG

- Fluentd

Forwarding Events and Logs to vRealize Log Insight Cloud

You can forward events and logs from syslog and vRealize Log Insight sources to vRealize Log Insight Cloud.

You can find information about setting up event and log forwarding from your source by using the links in the following table.

Before you begin, see Syslog Agents for vRealize Log Insight Cloud.

If you are forwarding messages from...	For instructions, see...
vCenter Server 5.5 and later	■ 6.5 Redirect vCenter Server Appliance Log Files to Another Machine ■ 6.0 Redirect vCenter Server Appliance Log Files to Another Machine ■ 5.5 Configure a vCenter Server Appliance to Forward Log Events to Log Insight
ESXi Host 5.5 and later	■ ESXi 5.5 and later
NSX 6.0 and later	■ Manager ■ Controller ■ Edge
vRealize Log Insight You can forward events from vRealize Log Insight with the Log Insight API (CFAPI) or the vRealize Log Insight agent.	■ Agent Installation ■ Configuration ■ Server Event Forwarding
Third-party	■ Rsyslog Configuration ■ Syslog-ng Configuration ■ NXLOG ■ Fluentd

Explore and Modify the Home Page

You can search for log events in the **Home** page. You can also view widgets that contain information about log trends, event types, alerts, and so on. As an administrator, you can decide which widgets are displayed for the members of your organization.

Procedure

- To search for log events, do the following:
  a Enter keywords in the search text box.
  b Optionally, click the calendar icon to provide a date range for the log results.
  c Click the search icon.

  The search result is a list of log events that contain the keywords.

To modify the time interval of the results, click the date range in the upper-right corner of the **Home** page.

Clicking the last search result labeled **Log Query** opens the **Explore Logs** page to find logs that contain the keywords. You can modify this query if needed. For more information, see Searching for Logs.

- In the **System Overview** section, you can view widgets that provide information about log volume trends, event types, favorite dashboards, recent alerts, and so on.
  - To view the query for a widget, click the title of the widget.
  - To modify the time interval for the information displayed in the widgets, click the date range in the upper-right corner of the section.
- If you are an administrator, you can decide which widgets are displayed for the members of your organization in the **System Overview** section. You can also resize and reposition the widgets.

  To add, remove, or resize widgets, click the three dots icon in the upper-right corner of the section and click **Edit Home Page**.
  - To add a widget, expand a category in the **Widget Categories** pane and drag a widget under the category to the **Home** page.
  - To remove a widget, click the trash icon in the upper right corner of the widget.
  - To resize a widget, drag the double-headed arrow icons in the lower-left and lower-right corners of the widget.
  - To reposition a widget, drag it across the page.

  Click **Save** when done.

Searching for Logs

You can search for and filter log events in the **Explore Logs** page by using queries. You can use fields in your search criteria for efficient log monitoring. You can also save queries, clone queries and modify them, compare query results from multiple systems, share queries and their results with other users, and pin queries to the pinboard.

Search for and Filter Logs

You can search for and filter log events in the **Explore Logs** page by entering queries in the search text box.

Expand the main menu and click **Explore Logs** to perform the following tasks:

Procedure

- Enter keywords, globs, or phrases in the search text box and click the **Search** button to find only events that contain the keywords.

  Use the glob * in search terms for zero or more characters. For example, searching for vm* returns results that match VMware and VMtools.

  Note You cannot use globs 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.

- Select a time range next to the search text box to find events within the range. Time ranges are inclusive when filtering.
- Search for log events that match certain values of specific fields. Using text in quotes in the main search text box matches exact phrases. Entering space in the main search text box is a logical AND operator. The search uses only full tokens. For example, searching for "err" does not find "error" as a match.
- Enter 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, press **Enter** or **Tab** to separate multiple OR filters. For example, select **hostname contains** and type **`127.0.0.1`**, press **Enter**, and type **`127.0.0.2`**. The search returns events with the host name 127.0.0.1 or 127.0.0.2.

  You can combine multiple field filters by creating a 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 multiple values within a single filter row is always OR.

Group Logs During Search

While searching for log events, you can group log events by multiple fields and see a time-series or non time-series visualization.

Procedure

1 In the **Explore Logs** page, fetch your query search results for log events. For more information, see Search for and Filter Logs.

2 In the chart under the query, click **Over Time** and select **Time series** or **Non-time series**. You can also do a group-by for the results as time series or non-time series data:

Option	Description
Time series	The results from the search time-frame are split into multiple subresults and for each subresult, a group-by is performed.
Non-time series	A group-by is performed for all the results across the search time-frame.

Tip You can view the result count alone by selecting **Non-time series** without a group-by option.

3 Click the **Search** button.

Perform Numerical Functions on Log Results

You can perform numerical functions on your log results to view the count of events, unique count of field names, and so on.

Procedure

1 In the **Explore Logs** page, fetch your query search results for log events. For more information, see Search for and Filter Logs.

2 In the chart under the query, click **Count of Events** and select one of the following options:

Option	Description
Count of events	This is the default option, which shows the total count of log events.
Unique count of [field name]	This option shows the number of unique instances for the selected field name.
Numerical function for [field name]	This is applicable only for numerical fields. You can select multiple numerical options such as **Average**, **Maximum**, and so on. For example, if you select the field **process** in the drop-down menu with the **Average** and **Maximum** options, the results display the average and maximum counts for the field *process*.

Tip You can group the results of the numerical functions and see a time series or non-time series visualization as explained in Group Logs During Search.

3 Click the **Search** button.

View the Context of a Log

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.

Procedure

1 In the **Explore Logs** page, fetch your query search results for log events. For more information, see Search for and Filter Logs.

2 Locate an event in the chart under the query.

3 Click the three dots icon and select **View in Context**.

Chart Types for Logs

In the **Explore Logs** page, you can select different chart types to change the way the data is displayed in the chart under the query.

You can fetch your query search results as described in Search for and Filter Logs. After fetching the results, select the chart type in the drop-down menu in the upper-right corner of the chart.

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

Chart Type	Aggregation Function	Time Series Requirement	Group-By Requirement	Additional Tasks
Area	Any	Time series	Optional	■ Select **Gradient** to view the chart in gradient color. ■ Select **Line Plot** to view the chart as a series of data points connected by straight line segments. ■ Select **Logarithmic Axis** to view the chart on a logarithmic scale. ■ Select a color theme for the chart.
Column	Any	Any	Optional	■ Select **Gradient** to view the chart in gradient color. ■ Select **Logarithmic Axis** to view the chart on a logarithmic scale. ■ Select a color theme for the chart.

Chart Type	Aggregation Function	Time Series Requirement	Group-By Requirement	Additional Tasks
Line	Any	Time series	Optional	■ Select **Gradient** to view the chart in gradient color. ■ Select **Line Plot** to view the chart as a series of data points connected by straight line segments. ■ Select **Logarithmic Axis** to view the chart on a logarithmic scale. ■ Select a color theme for the chart.
Pie	Count or Unique Count	Non-time series	At least one field	■ Select **Donut** to view the pie chart with the center cut out. ■ Select a color theme for the chart.
Bubble	Any	Non-time series	Two fields	■ Select **Donut** to view the pie chart with the center cut out.
Table	Any	Any	Optional	None

Event Types

vRealize Log Insight Cloud summarizes a large number of individual events into a smaller number of broad event types. The system uses machine learning to group similar events together, with each group showing the approximate number of events in the group. Grouping events helps identify the most communicative events and the most quiet ones, both of which are critical for troubleshooting.

vRealize Log Insight Cloud tries to automatically detect groups of similar events based on the number of common parts that the events have. For example, consider the following events:

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

These events have eight common parts - time stamp, thread name, host IP, logging level, class name, message text, token number, and duration.

Now, consider the following events:

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

These events only have three common parts - time stamp, host IP, and logging level.

In the **Explore Logs** page, the **Types** tab under the chart provides an aggregated view of similar events. By default, the types are sorted with the highest number of event occurrences. You can select **Least** in the drop-down menu to sort by the least number of events. You can also click the three dots icon against an event to add a filter in the query with similar or dissimilar events.

Event Trends

vRealize Log Insight Cloud groups similar events into event types. You can use event trends to observe the current progression of each event type as compared to a previous time.

In the **Explore Logs** page, the **Event Trends** tab under the chart displays the trends that event types follow. In the first drop-down menu, you can select the time that is used as a basis to analyze the progression of event types. The default time is **Previous 50 minutes**, which means that, for each event type, the system compares the current number of events arriving per minute with the number of events that arrived per minute, 50 minutes ago. The trends are sorted by increasing event types, which you can modify in the second drop-down menu. You can click the three dots icon against an event type to add a filter in the query with events similar or dissimilar to the events in the event type.

Event trends show:

- Increasing and decreasing event types, and the increase and decrease rates.
- Event types with events newly added to the system, to help identify unexpected behavior.
- Event types with events arriving at a constant rate.
- Event types with events that are no longer in the system.

Event trends use the following icons for new, existing, and deleted events in each event type, by comparing the current event rate to the event rate at the time that you select in the first drop-down menu. You can point to these icons to view the increase and decrease rates.

Icon	Description
	The event type has newly added events.
	The event type has a high increase rate for events.

Icon	Description
	The event type has a moderate increase rate for events.
	The event type has a low increase rate for events.
	The event type has the same number of events.
	The event type has a low decrease rate for events.
	The event type has a moderate decrease rate for events.
	The event type has a high decrease rate for events.
	The event type no longer has any events.

Fields in vRealize Log Insight Cloud

In a large environment with numerous log events, you cannot always locate the data fields that are important to you.vRealize Log Insight Cloud supports the creation of fields to use in queries and filters to address this concern. 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 a type of regular expression query useful for complex pattern matching. With fields, you can construct queries or build filters without needing to know, remember, or learn complicated regular expressions.

vRealize Log Insight Cloud supports indexed, content, and extracted fields. Indexed fields are part of your vRealize Log Insight Cloud deployment. Content fields are installed as part of content packs. And extracted, or custom fields, are user created.

Fields are listed in the **Fields** pane on the **Stream** tab on the **Explore Logs** page. Click a field name to find out more about its use in queries, or click the gear icon to go to the **Fields** page for information about the field's definition.

The **Fields** page lists all vRealize Log Insight Cloud fields, organizing them into two groups: Query Results. and Other Fields. Field cards tell you the field type and include a menu of possible user actions for the field.

Table 1-1. Types of fields in vRealize Log Insight Cloud

		User Actions	
Field Type	**Definition**	**Admin permissions**	**User permissions**
Indexed	Created by vRealize Log Insight Cloud based on intelligent grouping algorithms applied to received logs and messages.	■ None	■ None
Content	Defined in a content pack and available for use with queries after the content pack is imported.	■ Clone	■ View
Extracted or custom	Created by vRealize Log Insight Cloud users with admin permissions based on log data. Used to filter and query log events.	■ Edit ■ Clone ■ Delete	■ View

Note Generic custom queries might be 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 parentheses. Verify that your queries contain as much textual context as possible. For example, `Event for vm\(\d+\)` is a better field extraction query.

Create an Extracted Field

You can manually create an extracted field.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
2. Go to the **Explore Logs** page.
3. On the **Stream** tab, click the three dots icon to the left of any log message.

   The **Add Filter** menu appears.
4. Click **Extract Field** on the **Add Filter** menu.

   The **Create Custom Field** form appears.
5. Fill in values for the field.
6. Click **Save**.

Results

The new field appears on the list of fields on the **Explore Logs** page and can be used in filters and queries.

What to do next

You can use the extracted field to search and filter your list of log events.

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

Clone a Field

You can create a duplicate of an imported or extracted field.

Cloning a field can be useful when you want to extract more than one field from an event and both fields appear in a similar context. Go to the **Fields** page and locate the extracted field you want to clone. When you clone a field, vRealize Log Insight Cloud creates a copy of the field with the word copy appended to the field name. Modify the values in the **Clone Field** window and save your work.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Cloud web user interface as an administrator.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
2. Go to the **Explore Logs** page.
3. To open the **Fields** page, click the gear icon in the upper-right corner of the **Fields** section. This page lists all vRealize Log Insight Cloud fields by organizing them into two groups - fields found in queries and fields found in other fields.
4. Locate the field you want to clone. You can use the **Filter** field to search.
5. Click the three dots icon next to the field and select **Clone**.

   Note You cannot clone indexed fields.

   The **Clone Field** window appears and displays the field's values and the name of the field you cloned with the word copy appended.
6. Optionally, provide or modify the following values:
   - Name of the field in the **Field Name** text box
   - The field type and regular expression value in the **Extracted Value** section
   - The pre and post context regular expressions in the **Location Context** section
   - Keywords in the **Additional Context** section
7. Click **Save**.

Modify an Extracted Field

You can modify the definitions of extracted fields.

When you modify a field, all charts, queries, and alerts that use the field you have modified are updated to use the new definition.

vRealize Log Insight Cloud user accounts can modify only the extracted fields that they have created. vRealize Log Insight Cloud administrator accounts can modify their own content and shared content.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
2. Go to the **Explore Logs** page.
3. Click the gear icon in the upper-right corner of the **Fields** section to open the **Fields** page.
4. Locate the field that you want to modify.
5. Click the three dots icon on the fields card and click **Edit** on the drop-down menu.
6. Modify the values as needed.
7. Click **Save**.

Delete a Field

When you no longer need it, you can delete an extracted field from vRealize Log Insight Cloud after ensuring it is not used in any queries.

Prerequisites

You must have administrator permissions to delete an extracted field.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
2. Go to the **Explore Logs** page.
3. Click the gear icon in the upper-right corner of the **Fields** section to open the **Fields** page.
4. Locate the field that you want to delete.
5. Click the three dots icon on the fields card and click **Delete**.

   If the field is being used in a query, you are informed of this. Fields cannot be deleted while they are being used.
6. Click **Delete** in the confirmation pop-up to finish the deletion.

Working with Queries

You can save a query to view it later, share a query with other users, and clone a saved query.

Save a Query

You can save a query in the **Explore Logs** page and view it later.

Procedure

1. Expand the main menu and click **Explore Logs**.

2 Enter a query and click the **Search** button to view the results.

   Select a time period and use filters for more specific query results. For more information, see Searching for Logs.

3 In the upper-right corner of the page, click the **Save** icon.

4 In the pop-up window, enter a name and description for the query and click **Save**.

What to do next

To view the saved query, click the three dots icon in the upper-right corner of the **Explore Logs** page and select **Open Saved Query**. You can use the query to create alerts and dashboards.

Modify or Clone a Saved Query

You can modify or clone a saved query in the **Explore Logs** page.

Procedure

1 Expand the main menu and click **Explore Logs**.

2 Click the three dots icon in the upper-right corner and select **Open Saved Query**.

3 In the pop-up window, click a query to open it.

4 In the **Explore Logs** page, modify the query according to your requirement. For more information, see Searching for Logs.

5 In the upper-right corner of the page, click the three dots icon and do either of the following:

   - If you are modifying the query, select **Save**.
   - If you are cloning the query, select **Save As**. In the pop-up window, enter a name and description for the cloned query and click **Save**.

Share a Query

When you create a query for troubleshooting, you might want to share the query with other users. Sharing saves time by ensuring that other users do not have to configure the same query criteria again. Sharing the query also helps you discuss your observations in the logs with other developers.

Procedure

1 Expand the main menu and click **Explore Logs**.

2 Enter a query and click the **Search** button to view the results.

   Select a time period and use filters for more specific query results. For more information, see Searching for Logs.

3 In the upper-right corner of the page, click the export or share icon and click **Share Query**.

4 Copy the link in the pop-up window and click **Close**.

Results

A link containing your query is copied to your clipboard, which you can share directly with other users.

Mark a Query as Favorite

You can mark a new or saved query as favorite in the **Explore Logs** page for quick viewing.

Procedure

1. Expand the main menu and click **Explore Logs**.
2. Do either of the following:
   - To save a new query as favorite, enter a query and click the **Search** button. For more information, see Searching for Logs.
   - To mark a saved query as favorite, click the three dots icon in the upper-right corner of the page and select **Open Saved Query**.
3. In the upper-right corner of the page, click the star icon and do either of the following:
   - To save a new query as favorite, click **Save and favorite query**.
   - To mark a saved query as favorite, click **Favorite this query**.
4. To save a new query as favorite, enter a name and description for the query and click **Save**.

Results

The star icon is yellow for queries marked as favorite. When you click the icon, you can view the list of favorite queries and open a query by clicking it. To remove a query from this list, open the query, click the star icon, and click **Unfavorite this Query**.

Examples of Search Queries

You can use these examples when building your queries in the **Explore Logs** page. The logs for the last five minutes are displayed by default. vRealize Log Insight Cloud indexes complete, alphanumeric, hyphen, and underscore characters.

Query for NSX-T Firewall Logs for a Firewall Rule ID in an SDDC

To query for NSX-T firewall logs for a rule ID in an SDDC:

1. Define a filter.
   a. In the **Explore Logs** page, click **Add Filter** and select **vmw_nsxtvmc_firewall_rule_id** from the first drop-down menu.
   b. Select **contains** from the second drop-down menu.
   c. Enter the rule ID in the value text box.
   d. Click **Add Filter** and select **sddc_id** from the first drop-down menu.
   e. Select **contains** from the second drop-down menu.

f Enter the SDDC id in the value text box.

2 Define the time range.

a Click the time range next to the **Search** button.

b Select a time range on the **Relative to now** or **Relative to time** tab or define a custom time range on the **Custom range** tab. You can also select a recently used time range on the **Recently used** tab.

3 Click the **Search** button.

Query for AWS Audit Trail Logs for an AWS Account ID

To query for AWS audit logs for an AWS account ID:

1 Define a filter.

a In the **Explore Logs** page, click **Add Filter** and select **log_type** from the first drop-down menu.

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

c Enter **`aws_cloud_trail`** in the value text box.

d Click **Add Filter** and select **useridentityaccountid** from the first drop-down menu.

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

f Enter the account ID in the value text box.

2 Define the time range as explained in the first example.

3 Click the **Search** button.

Query for Heartbeat Events Reported by the ESX/ESXi hostd Process

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

1 Define a filter.

a In the **Explore Logs** page, click **Add Filter** and select **appname** from the first drop-down menu.

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

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

2 Define the time range as explained in the first example.

3 Click the **Search** button.

Query for 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, enter **`error`**.

2 Define a filter.

   a In the **Explore Logs** page, click **Add Filter** and select **vc_event_type** from the first drop-down menu.

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

3 Click the **Search** button.

Export Logs

You might have to share entire or partial logs with users in your organization or another organization. To share logs, you can export the results of a query in RAW or JSON format. You can download these logs to a file and share the file with other users.

Procedure

1 Expand the main menu and click **Explore Logs**.

2 Enter a query and click the **Search** button to view the results.

   Select a time period and use filters for more specific query results. For more information, see Searching for Logs.

3 In the upper-right corner of the page, click the export or share icon and click **Export Logs**.

4 In the pop-up window, enter a name and format for the log export file.

5 Click **Export**.

Results

The export progress is displayed in the **Available Exports** pane. This pane lists all your log exports. You can access the pane at any time by clicking **Export** in the right side of the window. When the export is finished, you can download the file.

Compare Logs

While troubleshooting, you might have to analyze logs from multiple systems that interact with each other. For a specific time interval, you can run multiple queries with different query criteria to search for logs from various systems, and compare the logs.

Procedure

1 Expand the main menu and click **Explore Logs**.

2 Enter a query and click the **Search** button to view the results.

   Select a time period and use filters for more specific query results. For more information, see Searching for Logs.

3 Click the two arrows icon in the upper-right corner of the page.

4 In the **Compare Logs** page, click the **Add Query** icon to add queries for comparing logs. You can compare up to four sets of logs.

5 Click **Compare**.

Results

The log comparison is displayed as a stacked line chart and the query results appear in separate tabs under the chart.

Pin Queries to the Pinboard

You can pin queries and view them in the pinboard. Pinning helps you temporarily recall queries that have been executed and also lets you compare two or more queries

Note The pinboard holds queries per session and is cleared when the page refreshes or you log out. However, you can navigate to different pages in vRealize Log Insight Cloud without losing the queries in the pinboard.

Procedure

- To pin a query to the pinboard, after fetching your query search results in the **Explore Logs** page, click the pin icon in the upper-right corner of the page. You can pin multiple queries in a session.
- To view the pinboard, click **Pinboard** in the right side of the window. You can view the pinboard from any page in vRealize Log Insight Cloud. For each pinned query, you can see the time stamp at which it was created and a time series view of the query.
- To remove a pinned query from the pinboard, open the pinboard and click the **Close** icon in the upper-right corner of the query.
- If you navigate to different pages from the **Explore Logs** page or if you are viewing a query other than your pinned query in the **Explore Logs** page, you can recall the pinned query to view or modify it. To recall a pinned query, open the pinboard and click the time stamp of the query.
- To compare the queries in the pinboard, open the pinboard and click **Compare Logs** to open the **Compare Logs** page.

  Note Removing a query from the **Compare Logs** page does not remove the query from the pinboard.

Extracting Metrics from Logs

Application logs contain important information about processes and operations in metrics. You can use these metrics to observe or troubleshoot applications for failures and to monitor their performance based on parameters at various levels of granularity in a data center. In vRealize

Log Insight Cloud, you can extract the metrics from logs, tag them according your requirement, and post them to a metric store.

Note vRealize Log Insight Cloud supports only Wavefront as a metric store. For more information about Wavefront, see https://docs.wavefront.com/.

Configure Metric Extraction

You can use metrics to troubleshoot applications and monitor their performance. You can create a configuration to extract metrics from logs and post these metrics to a metric store. vRealize Log Insight Cloud supports only Wavefront as a metric store.

Prerequisites

Get the metric store URL and API key from Wavefront. For information about Wavefront, see https://docs.wavefront.com/.

1 Log in to your Wavefront instance.

2 Copy the Wavefront URL, for example, symphony.wavefront.com. You must use this URL in the **Send To** text box in the metric extraction configuration.

3 If you do not have an API token for your Wavefront account, generate the token by following the instructions in https://docs.wavefront.com/users_account_managing.html.

4 Copy the API token. You must use this token in the **API Key** text box in the metric extraction configuration.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
2. Click **Explore Logs**.
3. Enter a query and click the **Search** button to view the results.

   You can select a time period and use filters for more specific query results. For more information, see Searching for Logs.
4. On the **Stream** tab under the chart, locate a log.
5. Click the three dots icon for the log and select **Create Metric**.
6. Provide the following information to configure metric extraction:

Option	Description
Name	A name for the metric extraction configuration.
Enabled	A toggle that enables or disables the metric extraction configuration. The toggle is green when the configuration is enabled and gray when it is disabled. If disabled, the metrics for the configuration are not sent to the metric store.
Send To	The metric store URL.

Option	Description
API Key	The API token from the metric store.
Source Type	The log filtering criteria.
Pattern	When you select a log in the **Explore Logs** page to configure metric extraction, the system recommends matching grok patterns in this drop-down menu. A grok pattern is a named regular expression pattern for parsing logs. You can select one of the recommended grok patterns. If none of the recommended patterns match your log, you can write your own grok pattern in the text area under the drop-down menu. After defining the grok pattern, click **Parse** to see the metrics that can be extracted from your log based on the pattern. The system displays the list of numeric metrics that you can send to the metric store, for example, *avgbandwidth*, *avgiops*, and *avglatencyinms*. You can configure each of these metrics in the **Metric Values to Send** section.
Sample Message	This text area is auto-populated with the text from your selected log.

7 Provide the following information in the **Metric Values to Send** section to configure the metrics that you want to send to the metric store:

Option	Description
Value	Select a field from the drop-down menu whose value is sent to the metric store.
Name	The name for the metric in the metric store.

Source Tag	A single value that represents the source of the logs in a metric store.
	To add a source tag, click **Configure Source Tag**. In the pop-up window, configure an expression by selecting fields under **Available Fields (Parsed or Metadata)**. These fields are the parsed text fields from your selected log and log metadata. You can also use custom static string values with the fields to build the expression in the text box.
	Note Because the fields are enclosed in the characters "<" and ">", you cannot use these characters in the static string.
	For example, consider the following expression:
	`sddc-<env>.<sddc_id>.<component>.<sub_component>`
	Here, `sddc-` is a static string and `<env>`, `<sddc_id>`, `<component>`, and `<sub_component>` are the fields parsed from your selected log or metadata.
	This expression evaluates to:
	`sddc-prd.9d8ff46c-125c-4b72-b9b4-173d6bc71ab8.vm.mgmt`
	Click **Verify** to test the source tag configuration and then click **Save**.

Point Tag	A key-value pair sent to a metric store, which is used to filter the metrics in the chart. Select one or more point tags for the metric from the drop-down menu. The point tags in the drop-down menu are populated by using text fields parsed from your selected log based on your grok expression and the metadata of the log.

8 To configure more metrics, click **Add Metric Value** and repeat step 7.

9 Click **Save**.

Working with Dashboards

Dashboards present a visual overview of the state of events in vRealize Log Insight Cloud. A dashboard is a collection of widgets, in which each widget is associated with alerts or a query.

Dashboards are of three types - private, shared, and content pack dashboards. In the **Dashboards** page, for private and shared dashboards, the dashboard type is displayed under each dashboard name. For content pack dashboards, the content pack name is displayed instead.

The following permissions are applicable for the dashboard types:

Private Dashboards

- Any user can create a private dashboard.
- A user without administrator privileges can view only their private dashboards.

Shared Dashboards

- Users cannot create shared dashboards directly. Instead, they can create private dashboards and share them with other users.
- Any user can view the dashboards shared by them and with them by other users.
- Only the dashboard creator or a user provided with write access while sharing can modify or remove a shared dashboard.

  Note A user provided with write access can also modify the access control rights for a shared dashboard.

- Only the dashboard creator can change a shared dashboard back to a private dashboard.

Content Pack Dashboards

- Content pack dashboards are imported with content packs, so users cannot create or remove them.
- All users can view content pack dashboards, but cannot modify them. They can only add minor enhancements for their convenience, such as:
  - Mark a dashboard as favorite.
  - View queries associated with widgets in a dashboard.
  - Add tags to a dashboard.
  - Add a dashboard to a list.
  - Filter or refresh dashboard content.

- Select time ranges for dashboard content.
- Set a dashboard as the landing page for the logged in user.
- Export a dashboard in PDF format.
- Clone a dashboard. The cloned dashboard is a private dashboard, and all the permissions for private dashboards are applicable for the clone.
- Download the content pack associated with a dashboard from the **Content Packs** page and reimport the content pack as private for their shared content.

Create a Dashboard

To view the status of the events in vRealize Log Insight Cloud, you can create a private dashboard. When you create a dashboard for the first time, you add one or more widgets to the dashboard. Each widget is based on a query or one or more alerts.

Procedure

- To create a private dashboard with a widget based on a new query:
  a. Expand the main menu and click **Explore Logs**.
  b. Enter a query and click the **Search** button to view the results.

     Select a time period and use filters for more specific query results. For more information, see Searching for Logs.
  c. Optionally, select a chart type for the widget that is based on the query.

     For more information about chart types, see Chart Types for Logs.
  d. In the upper-right corner of the page, click the three dots icon and select **Add to Dashboard**.
  e. In the **Add Widget to Dashboard** pop-up window, enter the name, type, and description for the widget to add to the dashboard. This widget is based on the query that you entered in the **Explore Logs** page.
  f. Under the widget details, click **New Dashboard**.
  g. Enter a name for the dashboard and click **Add**.
- To create a private dashboard with widgets based on alerts or saved queries:
  a. Expand the main menu and click **Dashboards**.
  b. In the upper-right corner of the page, click **New Dashboard**.
  c. Enter a name for the dashboard.
  d. From the left pane, drag alerts or queries to the dashboard. Each alert or query that you drag corresponds to a widget, and the widget name and description are copied accordingly.
  e. Click **Save**.

- To create a private dashboard with a widget based on multiple alerts:
  a Expand the main menu and click **Alerts > Alert Definitions**.
  b Select multiple alerts and click **Actions > Add to Dashboard**.
  c In the **Add Widget to Dashboard** pop-up window, enter the name, type, and description for the widget to add to the dashboard. This widget is based on the alerts that you selected in the **Alert Definitions** page.
  d Under the widget details, click **New Dashboard**.
  e Enter a name for the dashboard and click **Add**.

Modify a Dashboard

After creating a private dashboard, you can modify the dashboard and its widgets. You can edit shared dashboards only if you have write access. You can also make minor modifications to content pack dashboards, such as export them in PDF format, add them to lists, mark them as favorite, and so on.

Prerequisites

Verify that you have the permission to modify the dashboard. For more information about dashboard types and permissions, see Working with Dashboards.

Procedure

1. Expand the main menu and click **Dashboards**.
2. Locate the dashboard that you want to modify. You can search for the dashboard by entering keywords in the search text box or by using the sort, list, or filter functionalities. You can filter dashboards by content packs, tags, and creators.
3. Do either of the following:
   - Mark the dashboard as favorite by clicking the star icon against the dashboard name.

     The dashboard appears when you:
     - Click the **List** drop-down menu in the **Dashboards** page to search for dashboards by list, and then click **Favorites**.
     - Add a widget to a dashboard. The dashboard appears under **Favorite Dashboards** in the **Choose Dashboard** drop-down menu.

     To remove the dashboard from favorites, click the star icon again.
   - Share a Dashboard.
   - Duplicate the dashboard. Click the three dots icon against the dashboard name and click **Clone**.

- Add the dashboard to a list. Click the three dots icon against the dashboard name and click **Add to List**. You can select an existing list or create a new list.

  Note Lists help users group dashboards according to their requirement. Lists are associated with individual users and are not visible to other users in the organization.

  In the **Dashboards** page, you can filter dashboards by lists. Click the **List** drop-down menu and click a list to view the dashboards in the list.

- Remove the dashboard. Click the three dots icon against the dashboard name and click **Delete**.
- Add tags to the dashboard. Click **Add tags** or the plus icon under the dashboard name. You can select existing tags or create a new tag.

  Note Similar to lists, tags help users group dashboards, but they are visible to all the users in the organization.

  In the **Dashboards** page, you can filter dashboards by tags. Click **Filters** and under **Tags**, select one or more tags to view the dashboards linked to the tags.

- Filter the dashboard content to view your preferred information. Click the dashboard name and click **Add Filters** under the dashboard name.
- Refresh the dashboard to view the latest data. Click the dashboard name and click **Refresh** in the upper-right corner.
- Modify the time range for the dashboard content. Click the dashboard name and click the time range in the upper-right corner.
- Make the dashboard your landing page. Click the dashboard name, click the three dots icon in the upper-right corner, and click **Set as Landing Page**. The next time you access vRealize Log Insight Cloud, the dashboard will be the first page you see.
- Export the dashboard in PDF format. Click the dashboard name, click the three dots icon in the upper-right corner, and click **Export as Report**.
- Modify the dashboard name. Click the dashboard name, click the three dots icon in the upper-right corner, click **Edit**, and in the upper-left corner, edit the name in the text box. Click **Save**.

4 Add a Widget to a Dashboard.

5 View the query associated with a widget in the dashboard. Click the dashboard name, click the three dots icon in the upper-right corner of a widget, and click **View Log Query**.

6 To modify a widget, click the dashboard name, click the three dots icon in the upper-right corner, click **Edit**, and do either of the following:

- Resize a widget by using the double-headed arrow icons in the lower-left and lower-right corners of the widget.
- Reposition a widget by dragging it across the dashboard.

- Modify the name and description of a widget. Click the pencil icon in the upper-right corner of the widget.
- Change the widget chart type. Click the presentation icon in the upper-right corner of the widget and select a chart type. For example, you can change a column chart to a line chart.

  For information about charts, see Chart Types for Logs.
- Remove a widget by clicking the trash icon in the upper-right corner of the widget.

Click **Save** after modifying the widget.

Add a Widget to a Dashboard

You can add a widget to an existing dashboard in vRealize Log Insight Cloud. Each widget is associated with a query or one or more alerts.

Prerequisites

Verify that you have the permission to modify the dashboard. For more information about dashboard types and permissions, see Working with Dashboards.

Procedure

- To add a widget based on a new query:
  a. Expand the main menu and click **Explore Logs**.
  b. Enter a query and click the **Search** button to view the results.

     Select a time period and use filters for more specific query results. For more information, see Searching for Logs.
  c. In the upper-right corner of the page, click the three dots icon and select **Add to Dashboard**.
  d. In the **Add Widget to Dashboard** pop-up window, enter the name, type, and description for the widget to add to the dashboard. This widget is based on the query that you entered in the **Explore Logs** page.
  e. Under the widget details, click **Private Dashboard** or **Shared Dashboard**, based on the type of dashboard you are adding the widget to.
  f. Select a dashboard from the **Choose Dashboard** drop-down menu and click **Add**.
- To add a widget based on a saved query or an alert:
  a. Expand the main menu and click **Dashboards**.
  b. Click the name of a dashboard. You can search for a dashboard by entering keywords in the search text box or by using the sort, list, or filter functionalities.
  c. In the upper-right corner, click the three dots icon and click **Edit**.

d Drag a query or alert from the left pane to the dashboard. Each alert or query that you drag corresponds to a widget, and the widget name and description are copied accordingly.

Tip Alternatively, you can add a widget based on multiple alerts in **Alerts > Alert Definitions**. Select one or more alerts and click **Actions > Add to Dashboard**. Enter the details in the pop-up window, similar to the details for adding a widget based on a new query. Click **Add**.

e Click **Save**.

Results

The widget appears when you open the associated dashboard from the **Dashboards** page.

Share a Dashboard

You can share a dashboard to make it visible to other users. You can assign read and write permissions to the users in your organization, based on their roles. You can also provide read access to external users.

Prerequisites

Verify that you have the permission to modify the dashboard. For more information about dashboard types and permissions, see Working with Dashboards.

Procedure

1. Expand the main menu and click **Dashboards**.
2. Locate the dashboard that you want to share. You can search for the dashboard by entering keywords in the search text box or by using the sort, list, or filter functionalities.
3. Click the three dots icon against the dashboard name and then click **Access Control**.

   Alternatively, you can click the dashboard name and then click the **Share** icon in the upper-right corner.
4. Do either of the following:

   - To provide access to users in your organization, in the **Choose Roles** drop-down menu, select roles and whether you want to provide read or write access to each of these roles. The access rights apply to all the users associated with the selected roles, when they are logged in.

     After providing access, click **Done**.

     As a result, the dashboard no longer appears as a private dashboard in the **Dashboards** page but instead appears as a shared dashboard.

     Note The users provided with write access can further modify the access control rights for the dashboard.

- To provide read access to users outside your organization, click **Copy Link**, and then click **Copy Link** again in the pop-up window. You can share this link with external users. When these users access the link, they see a read-only view of the dashboard without logging in.

  After copying the link, click **Close**.

Alerts and Notifications

vRealize Log Insight Cloud provides built-in system alerts for critical issues. You can also configure alerts based on queries that run at scheduled intervals or on every log ingested. You can view the recent alerts in the system and send email and webhook notifications for alerts.

Note You must be an administrator to edit alerts.

Types of Alerts that You Can Create

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

Alerts Based on Number of Events Within a Custom Period of Time

The alert query intervals for these alerts, also known as windowed alerts, depend on your settings. A notification is triggered according to your settings, when more or less than *X* matching logs occur in the last *Y* minutes.

If this type of alert is triggered, it is snoozed during its time period to prevent duplicate alerts from being raised for the same set of events.

Alerts on Every Match

You can create real-time alerts that match the alert query for every log that is ingested into vRealize Log Insight Cloud.

Content Pack Alerts

Content packs can contain alerts. The vSphere content pack that is included in vRealize Log Insight Cloud by default contains several predefined alerts. You can enable these alerts in your environment.

All content pack alerts are disabled by default.

Define an Alert

You can define an alert to notify users when specific data appears in the logs. An alert is based on a query.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Cloud web user interface as an administrator.

Procedure

1 Click the two arrows icon in the upper-left corner of the screen to expand the main menu.

2 Click **Explore Logs**.

3 Enter a query and click the **Search** button to view the results.

You can select a time period and use filters for more specific query results. For more information, see Searching for Logs.

Tip You can also create an alert from a saved query. To access a saved query, click the three dots icon in the upper-right corner, click **Open Saved Query**, and then click a saved query.

4 To create an alert from the query, click the exclamation mark icon.

5 In the **Save as an alert** dialog box, enter the following information:

- A name for the alert.
- A short meaningful description of the event that triggers the alert.
- A recommendation for the alert, which is included in the notification message when the alert is sent.

6 Click **Save**.

The alert definition opens.

7 To configure alert notifications, click the pencil icon next to **Notification**.

- To send email notifications, select the **Email** check box and enter a comma-separated list of recipient email addresses.
- To send webhook notifications, select the check boxes for the webhooks that you want to notify.

Tip You can send additional details for an alert to the webhook payload. In the **Notification Metadata** section, add key-value pairs to include custom fields in addition to the default values. These key-value pairs are appended to the webhook payload when the notification is sent.

8 In the **Trigger** section, set the alert threshold.

Option	Description
On every match	This alert query is matched with every log that is ingested. The time period is not relevant.
When total count of events is applied with operation *X* for threshold *Y*	This alert query is run within the window of the time period. The results are matched with the operation *X* for the threshold of *Y*. The time period is used to query logs.

Option	Description
When unique count of field *F* is applied with operation *X* for threshold *Y*	This alert query is run within the window of the time period. The query returns the unique count of field *F*. The results are matched with the operation *X* for the threshold of *Y*. The time period is used to query logs.
When aggregation operation *A* on field *F* is applied with operation *X* for threshold *Y*	This alert query is run within the window of the time period. The query returns the result of the aggregation operation *A* applied on the field *F*. The results are matched with the operation *X* for the threshold of *Y*. The time period is used to query logs.

9 The alert is disabled indefinitely by default. To enable the alert, click the three dots icon in the upper-right corner and click **Enable**.

10 Click the **Save** icon.

Results

The alert definition appears in **Alerts > Alert Definitions**.

Enable or Disable User-Defined Alerts

You can enable one or more alerts defined by you or any other administrator in your organization. You can also disable alerts indefinitely or for a specific period.

For information about defining alerts, see Define an Alert.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Cloud web user interface as an administrator.

Procedure

1 Click the two arrows icon in the upper-left corner of the screen to expand the main menu.

2 Navigate to **Alerts > Alert Definitions**. Each alert displays information about whether it is enabled or disabled.

3 You can disable one alert or multiple alerts.

- To enable or disable one alert, locate the alert and click the three dots icon against it.
- To enable or disable multiple alerts, select the check boxes against the alerts.

4 Do either of the following:

Task	Steps
Enable one or more alerts.	■ To enable one alert, click **Enable**. ■ To enable multiple alerts, click **Actions** and then click **Enable**.
Disable one or more alerts.	■ To disable one alert, click **Disable** and then select the period for which you want to disable the alert. ■ To disable multiple alerts, click **Actions** and then click **Disable**. Select the period for which you want to disable the alert. To disable one or more alerts indefinitely, select **Forever**. To disable one or more alerts for a custom period, select **Custom Range** and define the period. The alerts are disabled during the period and enabled before and after the period.

Viewing Recent Alerts

You can view the alerts that have been triggered in the last hour, day, or week. You can also view details for the last 100 alerts triggered.

To view the recent alerts triggered for your organization, expand the main menu and select **Alerts > Recent Alerts**. Alerts appear in a time-line view and a detailed view.

Time-Line View

The first panel displays a time-line view of the recent alerts. You can click a period in the upper-right corner of the panel to view the alerts triggered in the last hour, day, or week. You can also hover over each alert in the time-line to view the time at which the alert was triggered.

Detailed View

The second panel displays the following details for the last 100 alerts triggered for your organization:

- Name and description of the alert
- Tagging of the alert type

  Note Periodic alerts are tagged as "Total Count" and real-time alerts are tagged as "On Every Match".

- Time at which the alert was triggered
- How long ago the alert was triggered

When you click the three dots icon for an alert, you can select the following menu items:

Details

You can view the data and threshold with which the alert was triggered.

Definition

You can view and edit the alert definition.

Query

You can view the query and the data corresponding to the query for the alert.

Viewing System Alerts

vRealize Log Insight Cloud provides built-in system alerts for critical issues that need your immediate attention or activities that you must be aware of. A system alert is triggered when the system wants to notify you about a problem and also when the problem is resolved.

You can view the system alerts when you expand the main menu and select **Configuration > System Alerts**. If you are an administrator, you can use a toggle to enable or disable a system alert in the **System Alerts** page. You can also configure email and webhook notifications for the enabled alerts in this page:

- To send email notifications to specific users, under **Email Recipients**, add recipient email addresses and click **Save**. For information about configuring an email server, see Configure an Email Server to Send Alert Notifications.
- To send webhook notifications to a remote web server, under **Webhooks**, select webhooks and click **Save**. For information about configuring a webhook, see Configure a Webhook to Send Alert Notifications.

vRealize Log Insight Cloud provides the following system alerts:

Alert	Description	Action Required
Cloud Proxy Dropping Logs	The Cloud Proxy configured to send logs to the vRealize Log Insight Cloud service is dropping logs because there is a latency between the Cloud Proxy and the service, or the Cloud Proxy is under a heavy load.	Ensure that: ■ The Cloud Proxy is resourced correctly. ■ There is no high latency between the Cloud Proxy and the vRealize Log Insight Cloud service.
Failure to Forward Logs	vRealize Log Insight Cloud cannot forward logs to the endpoint because the endpoint is not accessible or under a heavy load.	If you are an administrator, ensure that: ■ The log forwarding endpoint configuration is correct. ■ The log forwarding endpoint is accessible across the Internet, if the log forwarding configuration has a cloud destination type. ■ The log forwarding endpoint is accessible to the Cloud Proxy configured to forward logs, if the log forwarding configuration has an on-premise destination type.

Alert	Description	Action Required
Inactive Cloud Proxy	The connection between the Cloud Proxy and the vRealize Log Insight Cloud service is broken.	Ensure that: ■ The Cloud Proxy is resourced correctly. ■ The Cloud Proxy can connect to the vRealize Log Insight Cloud service.
Ingestion Delay	There is a delay in viewing and querying the data collected by vRealize Log Insight Cloud. The delay might be because of indexing taking more time or a planned maintenance window.	None.
Ingestion Failures At Cloud Proxy	The Cloud Proxy fails to forward all incoming messages to vRealize Log Insight Cloud because there is a latency between the Cloud Proxy and the service, or the Cloud Proxy is under a heavy load.	Ensure that: ■ The Cloud Proxy is resourced correctly. ■ There is no high latency between the Cloud Proxy and the vRealize Log Insight Cloud service.
Ingestion Quota Exceeded	You have exceeded your ingestion limit for the day and no more logs are ingested for the day. Ingestion will begin again at the start of the next day (PST time zone).	None.

Configure an Email Server to Send Alert Notifications

You can configure an SMTP server to send email notifications for alerts.

Procedure

1 Click the two arrows icon in the upper-left corner of the screen to expand the main menu.

2 Navigate to **Configuration > Email Configuration**.

3 To use the VMware-hosted SMTP server, under **SMTP server**, select **Default - VMware Hosted** and skip to step 5.

4 To use a custom SMTP server:

   a Under **SMTP server**, select **Custom**.

   b Provide the following information:

Option	Description
Custom	Enter the server address and port number of the SMTP server that you want to use to send email notifications.
Security	If the selected SMTP server uses an encrypted connection, select the encryption protocol.
Username	Enter a user name to authenticate with the SMTP server when sending system notifications.
Password	Enter a password to authenticate with the SMTP server when sending system notifications.
Sender email	Enter an email address to use when sending system notifications.
Sender name	Enter a name to use when sending system notifications.

5 Click **Save**.

6 To verify the connection, click **Send Test Email**. Enter recipient email addresses for the test email and click **Send**.

Configure a Webhook to Send Alert Notifications

You can configure a webhook to send alert notifications to a remote web server. Webhooks provide notifications over HTTP POST/PUT.

Prerequisites

Ensure that the remote web server is a public endpoint.

Procedure

1 Click the two arrows icon in the upper-left corner of the screen to expand the main menu.

2 Navigate to **Configuration > Webhook Configuration**.

3 Click **New Webhook**.

4 Enter a name for the webhook configuration in the text box.

5 Provide the following information:

Option	Description
Notification Type	Select whether the webhook configuration is for an alert notification or a system alert notification.
Endpoint	Select the endpoint to which you want to send the notification, for example, PagerDuty, Slack, or Datadog. Based on the selected endpoint type: ■ The user interface provides additional input options. For example, a PagerDuty endpoint requires you to enter an integration key for webhook requests. ■ The user interface populates the webhook payload with a predefined template, which you can customize according to your requirement. If you select **Custom** as the endpoint type, you can select the **Use vRealize Log Insight Template** check box for the webhook payload, to use the default template.
Destination URL	Enter the URL for the remote web server where you want to post the webhook notification.
Advanced Settings	The default value for **Action** (HTTP request method) is **POST** and **Content Type** is **JSON**. You can customize these options and add additional headers to the request under **Custom headers**. If the configured remote web server requires authorization to POST/PUT the webhook notification, enter the user name and password to authenticate with the server in the **Authorization User** and **Authorization Password** text boxes.
Webhook Payload	This area is auto-populated based on your selection in the **Endpoint** drop-down menu. You can customize the payload, which is the template of the body sent as a part of the POST/PUT webhook notification request. The body can be in XML or JSON format. For a custom endpoint, you can select the **Use vRealize Log Insight Template** check box.
Parameters	You can use the list of parameters to construct the webhook payload. The parameters are replaced with the actual values while sending the webhook notification.

6 Click **Save**.

7 To verify the connection, click **Send Test**.

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. You can enable or disable a content pack, export or import a content pack, and remove a content pack.

To view the content packs that are loaded on your system, expand the main menu and select **Content Packs**.

Content packs are categorized into tabs as public and private. Public content packs are provided by VMware and third-party partners and are already installed. Private content packs are provided by external sources and you need to install them.

To view the details of a content pack, on a tab in the **Content Packs** page, click any of the content packs displayed. The information for the content pack is displayed in the following subtabs:

Info

Detailed information about the content pack.

Dashboards

The list of dashboards in the content pack. Click each dashboard to view it on the **Content Pack Dashboards** tab of the **Dashboards** page. Click each widget in the dashboard to view the query associated with the widget in the **Explore Logs** page.

Queries

The list of queries in the content pack. Click each query to view the query details in the **Explore Logs** page.

Alerts

The list of alerts in the content pack. Click each alert to view the alert details in the **Alert Definitions** page.

Extracted Fields

The list of extracted fields in the content pack. Click each extracted field to view the query to which the field is added in the **Explore Logs** page.

Note

- You can view the details for a content pack only if it is enabled.
- Content pack dashboards are read-only. You cannot delete or rename them. However, you can clone content pack dashboards to your custom dashboard.

Enable a Content Pack

Enable a private content pack to view its information or to export the content pack.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Cloud web user interface as an administrator.

Procedure

1 Expand the main menu and click **Content Packs**.

2 On the **Public** tab, click the toggle next to the title of the content pack to enable or disable it. The toggle is green when the content pack is enabled and gray when the content pack is disabled.

Note

- When you enable a content pack, the alerts from the content pack are not enabled by default. You can enable the alerts in the **Alert Definitions** page.
- When you disable a content pack, if the elements of the content pack are used by any user in your organization, a pop-up window appears, which describes where the elements are used. You cannot disable the content pack until you remove the dependent elements.

Results

The enabled elements of the content pack appear in pages such as **Alerts** and **Dashboards**.

Export a Content Pack

Export a private content pack to share content between vRealize Log Insight Cloud instances or with vRealize Log Insight Cloud users on the community. All fields that are used in queries, charts, and alerts that you export are included in the exported content pack. You can also export the user-defined elements in your organization such as alerts, dashboards, queries, and extracted fields as a content pack JSON file, even if these elements are not a part of content packs.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Cloud web user interface as an administrator.

Procedure

◆ To export a content pack:

a Expand the main menu and click **Content Packs**.

b On the relevant tab, click the **Download** icon next to the title of the content pack.

Note You can export a content pack only if it is enabled.

c In the pop-up window, enter the following metadata for the content pack:

Option	Description
Name	Enter a name for the content pack.
Namespace	Enter any user-driven namespace such as com.mycompany.content.
Version	Version this exported content pack as it can be reimported in the same product as a private content pack, which is visible only in the same organization.

d Click **Export** and save the file to a location on your computer.

The exported file with extension .lint is stored in the specified location. The details of the content packs in this file are JSON formatted.

- To export the user-defined elements in your organization as a content pack JSON file:
  a Expand the main menu and click **Content Packs**.
  b In the upper-right corner of the **Content Packs** page, click **Export Content**.
  c In the left section of the pop-up window, enter metadata for the content pack as described in step 3 of exporting a content pack.
  d In the right section of the pop-up window, select the user-defined elements that you want to include in the content pack.
  e Click **Export** and save the file to a location on your computer.

  The exported file with extension .lint is stored in the specified location. The details of the content packs in this file are JSON formatted.

Import a Content Pack

Import content as a private content pack or into your organization by using a JSON file with the details of the content pack elements.

The JSON file for import is created by exporting a content pack or user-defined elements. For more information, see Export a Content Pack.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Cloud web user interface as an administrator.

Procedure

1. Expand the main menu and click **Content Packs**.
2. On the **Private** tab, click **Import Content**.
3. In the pop-up window, select the import method:
   - To import content as a private content pack, select **Import as content pack**.This content is read-only and visible to all users.

     For information about content pack dashboards, see Working with Dashboards.

- To import content into your organization, select **Import content**. This content is visible to all the members of your organization, but editable only by administrators.

  Note

  - Content pack metadata, such as name, author, icon, and so on, are not displayed in this mode.
  - Agent groups are not imported in this mode.
  - Once the content is imported into your organization, you can individually edit or remove the imported elements, such as dashboards, queries, alerts, and fields.
  - Once the content is imported into your organization, you can modify it by updating the JSON file and reimporting it. A dialog box with duplicate elements appears and you can choose to overwrite the elements.

4. Click **Select File**.
5. Browse for a content pack JSON file and click **Open**.
6. Click **Import**.
7. If you selected the option to import the content into your organization, a dialog box appears and you are prompted to select what content to import. Select the content items and click **Import** again.
8. Some content packs require additional setup steps. Instructions for these steps appear after the import is finished. Finish these steps before you use the content pack.

Results

If the content is imported as a content pack, the content pack appears on the **Private** tab of the **Content Packs** page. If the content is imported into your organization, the elements such as dashboards, queries, and alerts appear in the relevant pages.

Remove a Content Pack

You can remove a private content pack that you imported into vRealize Log Insight Cloud.

For information about importing a content pack, see Import a Content Pack.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Cloud web user interface as an administrator.

Procedure

1. Expand the main menu and click **Content Packs**.

2 On the **Private** tab, click the trash icon next to the name of the content pack and then click **Delete** in the pop-up window.

Note When you delete a content pack, if the elements of the content pack are used by any user in your organization, a pop-up window appears, which describes where the elements are used. You cannot delete the content pack until you remove the dependent elements.

Forwarding, Retaining, and Archiving Logs

You can forward incoming events to vRealize Log Insight, Splunk, or another destination. You can retain certain logs for a lesser number of days than the default retention period. If you want to retain logs for a longer period, you can archive the logs and download them to an Amazon S3 bucket.

Forward Logs from vRealize Log Insight Cloud

You can configure vRealize Log Insight Cloud to forward all or a subset of incoming log events to a syslog or HTTP endpoint. The endpoint can be a SaaS endpoint such as Splunk or an on-premise endpoint such as vRealize Log Insight. You can use log forwarding to support existing logging tools such as SIEM and to consolidate logging over different networks such as DMZ or WAN.

For example, you might want to send all logs to the vRealize Log Insight Cloud service and then have the service forward any log events it receives related to security to the endpoint used by your security team. When you configure log forwarding, you specify a filter to select which events are forwarded. You can also forward the SDDC audit logs that are automatically sent to vRealize Log Insight Cloud .

Prerequisites

- Verify that you are logged in to the vRealize Log Insight Cloud web user interface as an administrator.
- To ensure that no events are dropped, verify that the destination can handle the number of events that are forwarded.

Procedure

1 Click the two arrows icon in the upper-left corner of the screen to expand the main menu.

2 Navigate to **Log Management > Log Forwarding**.

3 Click **New Configuration**.

4 Provide the following information:

Option	Description
Name	A unique display name for the log forwarding configuration.
Destination	Select **Cloud** if the endpoint can be accessed from WAN, else select **On Premise**.
Cloud Proxy	**Note** This configuration is required only if the destination is an on-premise endpoint. Select a Cloud Proxy that the system uses to forward logs to the destination.
Endpoint Type	The endpoint to which messages are forwarded, such as: **vRealize Log Insight** The destination is a vRealize Log Insight server. **Splunk** The destination is a Splunk server or cloud. **UDP** The destination is listening on a UDP port. Messages are forwarded in JSON format. **TCP** The destination is listening on a TCP port. Messages are forwarded in JSON format. **Default** All other scenarios.
Endpoint URL	The URL for the destination endpoint in the relevant format: **vRealize Log Insight** The URL is in the format *log-insight-server/api/v1/events/ingest/log-intelligence*, where *log-insight-server* is the host address or host name of the vRealize Log Insight server. **Splunk** The Splunk server or forwarder URL. **UDP** The URL is in the format *udp://10.197.11.148:514*. **TCP** The URL is in the format *tcp://10.197.11.148:514*.
Query	Filters log messages to forward the logs that contain the text you enter. At least one filter is required. To add more filters, click **Add Filter**. Optionally, click the magnifying glass icon to preview the filtered results.

Option	Description
Headers (optional)	One or more headers with predefined values. The headers contain authorization information for the endpoint and are added to the HTTP request when forwarding logs to the endpoint URL. **Note** You cannot add headers for TCP and UDP endpoints.
Tags (optional)	A tag name and predefined value. Tags let you query events more easily. You can add multiple comma-separated tags.

5 To test your configuration, click **Verify**.

6 Click **Save**.

Configure Log Retention

You can configure vRealize Log Insight Cloud to retain certain logs for a lesser number of days that the default retention period, which is 30 days. By retaining logs for a less number of days, you can remove logs with short life spans or sensitive information. The system runs log retention configurations as periodic tasks.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Cloud web user interface as an administrator.

Procedure

1 Click the two arrows icon in the upper-left corner of the screen to expand the main menu.

2 Navigate to **Log Management > Log Processing Rules**.

3 On the **Variable Retention** tab, click **New Configuration**.

4

Option	Description
Name	A unique display name for the log retention configuration.
Query	Filters log messages to retain the logs that contain the text you enter. At least one filter is required. To add more filters, click **Add Filter**. Optionally, click the magnifying glass icon to preview the filtered results.
Retention Days	The number of days for which you want to retain the logs.

5 Click **Save**.

Results

The variable retention configuration is displayed on the **Variable Retention** tab. You can modify or remove a configuration. If you modify the retention days, the new value is considered from the next periodic task onwards.

Configure Log Archiving

You can configure vRealize Log Insight Cloud to archive log data if you want to retain logs older than 30 days, which is the default retention period. For example, production logs are more crucial and you can retain them for a longer period, such as a year, and you can retain test logs for a shorter period, such as six months.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
2. Navigate to **Log Management > Log Archival**.
3. Click **New Configuration**.
4. Provide the following information:

Option	Description
Name	A unique display name for the log archival configuration.
Query	Filters log messages to archive the logs that contain the text you enter. At least one filter is required. To add more filters, click **Add Filter**. Optionally, click the magnifying glass icon to preview the filtered results.
Retention Days	The number of days for which you want to retain the logs.

5. Click **Save**.

Results

vRealize Log Insight Cloud saves the logs from the log archival configuration in Amazon S3. To view the archived logs, you can download them to an Amazon S3 bucket of your choice.

Download Archived Logs

You can download the archived logs from a log archival configuration in vRealize Log Insight Cloud to an Amazon S3 bucket of your choice.

Note You cannot view or search archived logs in vRealize Log Insight Cloud. You can only view the logs in the Amazon S3 bucket to which you download them.

Prerequisites

- Provide write permissions to the AWS account for vRealize Log Insight Cloud.
- Ensure that you have an Amazon S3 bucket to which you can download the archived logs.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
2. Navigate to **Log Management > Log Archival**.

3 Click the three dots icon to the left of a log archival configuration and click **View Archives**.

4 In the **Archives** section, select the archived logs that you want to download.

Tip To view the logs according to the time during which they were archived, click the text in the upper-right corner of the section. You can also perform this action in the **Downloads** section to view the logs based on the time during which they were downloaded.

5 In the **S3 Bucket** text box, enter the name of the Amazon S3 bucket to which you want to download the selected logs.

6 Select the relevant check boxes under the **S3 Bucket** text box.

7 Click **Download**.

Results

vRealize Log Insight Cloud asynchronously downloads the archived log files into the specified Amazon S3 bucket. This process can take 3–5 hours. The **Downloads** section displays the log files that you selected for download, with the location of each file in Amazon S3 and its download status. After the log files are downloaded, you can see the files in your Amazon S3 bucket.

Processing Logs

You can configure log processing rules for tagging, filtering, and masking the logs that are ingested by vRealize Log Insight Cloud. For example, you can tag logs that contain a sent notification by using additional metadata such as `sent-notification: true`, drop logs that are of no use by filtering them, or mask entire logs or fields such as *password* within logs.

Tag Logs

You can create log processing rules to tag logs. Tagging lets you add additional fields to log messages. For example, you can tag logs that contain a sent notification by adding metadata such as `sent-notification: true`.

Note

- Log processing rules are applied only to the logs that are ingested after you create and enable these rules.
- All the actions that you perform on log processing configurations - create, modify, remove, disable, or enable, need about a minute to reflect in the system.

Procedure

1 Expand the main menu and navigate to **Log Management > Log Processing Rules**.

2 On the **Tag Logs** tab, click **New Configuration**.

3 Provide the following information:

Option	Description
Name	A name for the log tagging configuration.
Fields	Key-value pairs that need to be tagged to the logs. You can add multiple key-value pairs to the logs.
Apply to all logs / Apply to specific logs	Apply the tagging configuration to all the logs or to specific logs. If you apply the configuration to specific logs, you can add query criteria for single or multiple fields, so that only the logs that match the criteria are tagged.

4 Click **Save**.

What to do next

On the **Tag Logs** tab, you can:

- Modify or remove the configuration. Click the three dots icon to the left of the configuration and select **Edit** or **Delete**.
- Enable or disable the configuration. Click the toggle to the left of the configuration. The toggle is green when the configuration is enabled and gray when it is disabled.

Filter Logs

You can create log processing rules to filter logs. Filtering lets you drop irrelevant fields from log messages or entire log messages that are of no use.

Note

- Log processing rules are applied only to the logs that are ingested after you create and enable these rules.
- All the actions that you perform on log processing configurations - create, modify, remove, disable, or enable, need about a minute to reflect in the system.

Procedure

1 Expand the main menu and navigate to **Log Management > Log Processing Rules**.

2 On the **Filter Logs** tab, click **New Configuration**.

3

Option	Description
Name	A name for the log filtering configuration.
Fields	Drop all the logs or specific logs in the filtering configuration. If you drop specific logs, you can add query criteria for multiple fields, so that only the logs that match the criteria are filtered.
Apply to all logs / Apply to specific logs	Apply the filtering configuration to all the logs or to specific logs. If you apply the configuration to specific logs, you can add query criteria for single or multiple fields, so that only the logs that match the criteria are filtered.

Note You cannot select **Drop entire log** and **Apply to all logs** at the same time, as a combination of these selections drops all the logs that are ingested.

4 Click **Save**.

What to do next

On the **Filter Logs** tab, you can:

- Modify or remove the configuration. Click the three dots icon to the left of the configuration and select **Edit** or **Delete**.
- Enable or disable the configuration. Click the toggle to the left of the configuration. The toggle is green when the configuration is enabled and gray when it is disabled.

Mask Logs

You can create log processing rules to mask logs. Masking lets you hide fields completely or partially in log messages, for example, fields such as *password*.

Note

- Log processing rules are applied only to the logs that are ingested after you create and enable these rules.
- All the actions that you perform on log processing configurations - create, modify, remove, disable, or enable, need about a minute to reflect in the system.

Procedure

1 Expand the main menu and navigate to **Log Management > Log Processing Rules**.

2 On the **Mask Logs** tab, click **New Configuration**.

3

Option	Description
Name	A name for the log masking configuration.
Fields	The fields that you want to mask in the log messages. You can mask multiple fields in a configuration. After entering a field name, you must enter the regex selector for the field value, which indicates the part of the field that you want to mask. You can also enter a value to replace the masked content of the specified fields, the default value for which is ***** .
Apply to all logs / Apply to specific logs	Apply the masking configuration to all the logs or to specific logs. If you apply the configuration to specific logs, you can add query criteria for single or multiple fields, so that only the logs that match the criteria are masked.

4 Click **Save**.

What to do next

On the **Mask Logs** tab, you can:

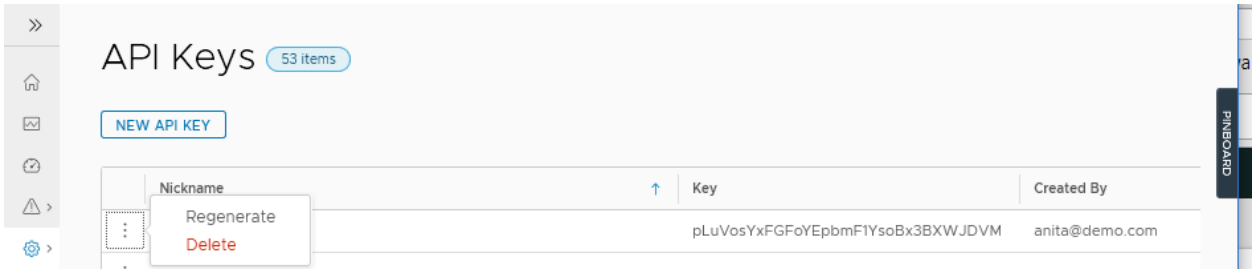
- Modify or remove the configuration. Click the three dots icon to the left of the configuration and select **Edit** or **Delete**.
- Enable or disable the configuration. Click the toggle to the left of the configuration. The toggle is green when the configuration is enabled and gray when it is disabled.

Securing Logs with API Keys

vRealize Log Insight Cloud uses API keys to ensure the security of logs ingested by the vRealize Log Insight Cloud cloud proxy server.

Keys are generated and applied for you except for logs that you send to vRealize Log Insight Cloud through an HTTP POST API call. For these you must create the API key and use the key as an authorization header.

API keys are made up of a nickname and a key value. You can create, regenerate, or delete API keys. The same API key can be used with multiple authorization headers for multiple sources.



Specifying an API Key for a Log Source

The following curl script illustrates how a key is specified as part of a POST operation. The key shown on the Authorization line has been copied from an API key list on the API Key page:

```
curl -X POST \
  https://data.mgmt.cloud.vmware.com/le-mans/v1/streams/ingestion-pipeline-stream \
  -H 'Authorization:Bearer wj32145ROzycKFvsIh34aSfz8cONRmZ' \
  -H 'Content-Type:application/json' \
  -H 'structure:default' \
  -d '[{
       "text": "Thu, 01 Mar 2018 20:41:42 GMT Test Payload-test",
       "source": "myhost.vmware.com"
   }]'
```

Create an API Key

You must create and apply an API key to your log source when you send logs or messages through an HTTP POST operation.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
2. Navigate to **Configuration > API Keys**.
3. Click **New API Key** to display the **New API Key** window.
4. Enter a name for the key.

   Note Names cannot contain spaces and must be unique.

5. Click **Create** to create a key and open the **Generate API Key** window.

   The **Generate API Key** window displays the key name you specified and the generated key value.
6. Optionally, click **Copy Key** to save the key value for easy reuse.
7. Click **Close**.

Results

The new key is listed on the **API Keys** page.

What to do next

Use the key to establish a secure connection to your data source. For an example, see Specifying an API Key for a Log Source.

Regenerate an API key

You can regenerate the key value for an API key. When you regenerate a key, the nickname for the key is kept and the key value is replaced.

Key regeneration can be used for the following purposes.

- Periodic key regeneration is a good security practice to safeguard your site's API keys.
- You can regenerate a key as a shortcut to halt logs from all sources using that API key. When you regenerate the key without configuring for the new key value, vRealize Log Insight Cloud no longer recognizes the log source and stops receiving messages from the source.

After you regenerate a key, you must reconfigure connections to use new API key value.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
2. Navigate to **Configuration > API Keys**.
3. Locate the key whose value you want to regenerate and click the three dots icon to the left of its key name to open the **Regenerate API Key** window.
4. Click **Regenerate**.

   A new key value is created for the named key.

What to do next

Reestablish a connection to data sources that use the key, updating configuration with the new key value. See Specifying an API Key for a Log Source.

Delete an API Key

Delete API keys when they are no longer used or as a way to stop the ingestion of log data from a source that uses the key.

When you delete a key, its name and value are expunged and it no longer appears in the list of API keys.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
2. Navigate to **Configuration > API Keys**.
3. Locate the key to delete and click the three dots icon to the left of the key name to open the **Delete API Key** window.
4. Click **Delete**.

Results

The key is removed from the list of API keys and any sources configured for ingestion with the key are rejected.

Viewing Usage Reports

Usage reports show how vRealize Log Insight Cloud is used across the organization - the amount of data streamed, log statistics, recent queries, and active users.

You can view usage reports when you expand the main menu and select **Configuration > Usage Reports**. The reports are categorized into the following tabs:

Data Intake

This tab displays details about the amount of data streamed into the system in the last 30 days:

Data used

The total amount of data used in the current month, irrespective of the subscription type.

Retention

The number of days for which the logs are retained. The retention period varies by subscription type. For more information about subscriptions, see vRealize Log Insight Cloud Subscriptions and Billing.

To download a report of the data intake in the last 30 days, you can click the download icon in the upper-right corner of the tab.

Log Statistics

This tab displays statistics about how the system is being used. Statistics for the last 24 hours is displayed by default. However, you can select a different time range.

For example, the **Logs Ingested per second** panel shows the number of logs streamed into the system per second.

Note This tab is available for administrators only.

Recent Queries

This tab displays the queries executed in the last one hour. These queries are executed by a user or by the system to evaluate alerts.

If you click the signpost icon (i) for a query, you can view more information about the query, such as:

- When the query was triggered.
- How long the query took for execution.
- Whether the query is finished or still running.
- The records fetched by the query.
- Origin of the query.

You can sort the queries by triggered time, time spent, status, total records, and origin. You can also filter the queries by status or by the origin of the query.

Note This tab is available for administrators only.

Active Sessions

This tab displays a list of users who are logged into the system. It also shows more information about these users, such as active sessions and time of logging in. You can sort and filter the users by their email addresses.

Note This tab is available for administrators only.

Working with vRealize Log Insight Agents

A vRealize Log Insight Agent collects events from log files and forwards them to a vRealize Log Insight Cloud server or any third-party syslog destination.

Note This topic contains links to the documentation for vRealize Log Insight, which is an on-premise log management solution. These links provide information for installing and configuring agents. Use only the information that is relevant to agents in vRealize Log Insight Cloud.

Configuring Agents

Before configuring a Log Insight Agent, you must finish the following tasks:

- Deploy a Cloud Proxy.
- Install the Log Insight Agent. You can follow the relevant instructions in the vRealize Log Insight documentation for installing an agent.

After deploying a Cloud Proxy and installing the agent, expand the main menu and click **Log Sources**. Click **Log Insight Agent** and follow the instructions on the screen to configure the agent.

To configure agents, you can follow the relevant instructions in the vRealize Log Insight documentation for agent configuration.

Managing Agent Configuration

As an administrator, you can centrally manage multiple Log Insight Agent configurations. Select **Configuration > vRLI Agents** to modify the configuration in the **Agent Configuration** section and click **Save**. You can modify the configuration for all agents or select agent groups and filter agents in the group to modify their configuration.

To understand how a central configuration works, you can refer the vRealize Log Insight documentation for centralized agent configuration.

Enabling Auto-Update and Auto-Upgrade

Enabling auto-update lets the active agents automatically download and update their configurations. Enabling auto-upgrade lets the active agents automatically upgrade to the latest available version. To see the latest agent version, in the **Log Sources** page, click **Log Insight Agent**. Auto-upgrade supports the upgrade of MSI packages for Windows and RPM and DEB packages for Linux.

For auto-update and auto-upgrade to work for an agent, ensure that the following conditions are met:

- The agent has an active status.
- The agent version is 4.3 or later.
- The agent is not of a Linux BIN package type.
- The client-side agent configuration has the *auto_update* flag set to 'yes'.

To enable auto-update and auto-upgrade for all agents, expand the main menu and select **Configuration > vRLI Agents**. Enable the auto-update of the configuration and auto-upgrade of the version by using the respective toggle buttons in the upper-right corner of the page.

Note Once enabled, auto-upgrade takes about an hour to finish.

Integrating vRealize Log Insight Cloud with vSphere

As an administrator, you can set up vRealize Log Insight Cloud to connect to vCenter Server systems at two-minute intervals and collect data for events, alarms, and tasks. You can also configure ESXi hosts in vRealize Log Insight Cloud via the vCenter Server.

Cloud Proxy as a Syslog Server

A Cloud Proxy receives log and event information from monitored sources and sends this information to vRealize Log Insight Cloud, where it can be queried and analyzed. The Cloud Proxy includes a built-in syslog server that is constantly active when the Cloud Proxy is running.

Messages that the syslog server ingests become searchable in the vRealize Log Insight Cloud web user interface near real time.

For port information about the Cloud Proxy, see Port Requirements of Remote Cloud Proxy.

For syslog formats, see Syslog Agents for vRealize Log Insight Cloud.

Connect vRealize Log Insight Cloud to a vSphere Environment

Before you configure vRealize Log Insight Cloud to collect alarms, events, and tasks data from a vSphere environment, you must connect vRealize Log Insight Cloud to one or more vCenter Server systems.

vRealize Log Insight Cloud can collect two types of data from vCenter Server instances and the ESXi hosts that they manage.

- Events, tasks, and alerts are structured data with specific meaning. If configured,vRealize Log Insight Cloud pulls events, tasks, and alerts from the registered vCenter Server instances.
- Logs contain unstructured data that can be analyzed in vRealize Log Insight Cloud. ESXi hosts or vCenter Server Appliance instances can push their logs to vRealize Log Insight Cloud through syslog.

Prerequisites

- For the level of integration that you want to achieve, verify that you have user credentials with enough privileges to perform the necessary configuration on the vCenter Server system and its ESXi hosts.

Level of Integration	Required Privileges
Events, tasks, and alarms collection	■ **System.View** **Note** **System.View** is a system-defined privilege. When you add a custom role and do not assign any privileges to it, the role is created as a Read Only role with three system-defined privileges: **System.Anonymous**, **System.View**, and **System.Read**.
Syslog configuration on ESXi hosts	■ **Host.Configuration.Change settings** ■ **Host.Configuration.Network configuration** ■ **Host.Configuration.Advanced Settings** ■ **Host.Configuration.Security profile and firewall**

  Note You must configure the permission on the top-level folder within the vCenter Server inventory, and verify that the **Propagate to children** check box is selected.

- Verify that you know the IP address or domain name of the vCenter Server system.
- Verify that you are logged in to the vRealize Log Insight Cloud web user interface as an administrator.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
2. Navigate to **Configuration > vSphere Integration**.
3. Click **Add vCenter Server**.
4. In the **Hostname** text box, enter the IP address for the vCenter Server.
5. In the **Username** text box, enter the user name for the vCenter Server service account.
6. In the **Password** text box, enter the password for the vCenter Server service account.
7. From the **Cloud Proxy** drop-down menu, select an installed Cloud Proxy.
8. Click **Test Connection**.

9 Click **Save**.

10 (Optional) To register another vCenter Server, click **Add vCenter Server** and repeat steps 1 through 9.

Note Do not register vCenter Server systems with duplicate names or IP addresses. vRealize Log Insight Cloud does not check for duplicate vCenter Server names. You must verify that the list of registered vCenter Server systems does not contain duplicate entries.

What to do next

- Collect events, tasks, and alarms data from the vCenter Server instance that you registered. See Configure vRealize Log Insight Cloud to Pull Events, Tasks, and Alarms from a vCenter Server Instance.
- Collect syslog feeds from the ESXi hosts that the vCenter Server manages. See Configure an ESXi Host to Forward Log Events to vRealize Log Insight Cloud.

Configure vRealize Log Insight Cloud to Pull Events, Tasks, and Alarms from a vCenter Server Instance

Events, tasks, and alerts are structured data with specific meaning. You can configure vRealize Log Insight Cloud to collect alarms, events, and tasks data from one or more vCenter Server systems.

You use the vRealize Log Insight Cloud interface to configure vRealize Log Insight Cloud to connect to vCenter Server systems. The information is pulled from the vCenter Server systems by using the vSphere Web Services API and appears as a vSphere content pack in the vRealize Log Insight Cloud web user interface.

Note vRealize Log Insight Cloud can pull alarms, events, and tasks data only from vCenter Server 5.5 and later.

Prerequisites

- Verify that the vCenter Server that manages the ESXi host is registered with your vRealize Log Insight Cloud service. Or, you can register the ESXi host and configure vCenter Server in a single operation.
- In vSphere, verify that you have user credentials with **System.View** privileges.

  Note You must configure the permission on the top-level folder within the vCenter Server inventory, and verify that the **Propagate to children** check box is selected.
- Verify that you are logged in to the vRealize Log Insight Cloud web user interface as an administrator.

Procedure

1 Click the two arrows icon in the upper-left corner of the screen to expand the main menu.

2 Navigate to **Configuration > vSphere Integration**.

3 Locate the vCenter Server instance from which you want to collect data, and click the instance.

4 Select the **Collect vCenter Server events, tasks, and alarms** check box.

5 Click **Save**.

Results

The Cloud Proxy connects to the vCenter Server every two minutes and ingests all new information since the last successful poll. The events, tasks, and alarms of the vCenter Server instance are sent to vRealize Log Insight Cloud and show up as searchable events in the **Explore Logs** page. However, vCenter Server logs must be sent separately via a Log Insight Agent.

What to do next

- Analyze vSphere events using the vSphere content pack or custom queries.
- Enable vSphere content pack alerts or custom alerts.

Configure an ESXi Host to Forward Log Events to vRealize Log Insight Cloud

ESXi hosts or vSphere Appliance instances generate unstructured log data that can be analyzed in vRealize Log Insight Cloud.

You use the vRealize Log Insight Cloud interface to configure ESXi hosts on a registered vCenter Server to push syslog data to vRealize Log Insight Cloud.

Caution Running parallel configuration tasks might result in incorrect syslog settings on the target ESXi hosts. Verify that no other administrator is configuring the ESXi hosts that you intend to configure.

For information about filtering syslog messages on ESXi hosts before messages are sent to vRealize Log Insight Cloud, see Configure Log Filtering on ESXi Hosts in the *VMware ESXi Installation and Setup* guide.

For information about configuring syslog feeds from a vCenter Server Appliance, see Configuring the vCenter Server to Forward Log Events to vRealize Log Insight Cloud.

Note vRealize Log Insight Cloud can receive syslog data from ESXi hosts version 6.x and later.

Prerequisites

- Verify that the vCenter Server that manages the ESXi host is registered with your vRealize Log Insight Cloud service. Or, you can register the ESXi host and configure vCenter Server in a single operation.

- Verify that you have user credentials with enough privileges to configure syslog on ESXi hosts.
  - **Host.Configuration.Advanced settings**
  - **Host.Configuration.Security profile and firewall**

  Note You must configure the permission on the top-level folder within the vCenter Server inventory, and verify that the **Propagate to children** check box is selected.
- Verify that you are logged in to the vRealize Log Insight Cloud web user interface as an administrator.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
2. Navigate to **Configuration > vSphere Integration**.
3. Locate the vCenter Server instance that manages the ESXi host from which you want to receive syslog feeds, and click the instance.
4. Select the **Configure ESXi hosts to send logs to vRealize Log Insight Cloud** check box.

   By default, vRealize Log Insight Cloud configures all reachable ESXi hosts of version 6.x and later to send their logs through UDP. ESX is not supported, and existing syslog targets on these hosts are not removed.
5. (Optional) To modify the default configuration values, click **Advanced Options**. The ESXi hosts are listed with additional information such as host name, version, build, and whether they have been configured.

   Do the following:
   a. Select the **Automatic** or **Manual** option to configure hosts. If you select **Automatic** and then configure all the hosts, new hosts are automatically configured when added. If you select **Manual** and then configure all the hosts, you have to configure new hosts manually when added.
   b. Optionally, select **TCP** as the protocol to send logs.
   c. Select one or more hosts and click **Configure**. If you configure all the hosts, newly added hosts are configured automatically or need manual configuration, based on your selection.

      You can also undo host configurations by clicking **Unconfigure**.
6. Click **Save**.

What to do next

The ESXi host configurations are shown in the **ESXi hosts configured** column of the vCenter Server table. If the hosts are configured, you can click **View details** to view detailed information for the configured ESXi hosts.

Configuring the vCenter Server to Forward Log Events to vRealize Log Insight Cloud

The vSphere integration collects task and events from vCenter Server, but not the low-level internal logs from each vCenter Server component. These logs are used by the vSphere content pack.

The configuration for vCenter Server 6.5 and later releases is done through the vCenter Server Appliance Management Interface. For more information about how to forward log events from vCenter Server, see the vSphere documentation about redirecting vCenter Server Appliance log files to another machine.

For earlier versions of vSphere, although the vCenter Server Appliance contains a syslog daemon that can be used to route logs, the preferred method is to install a Log Insight Agent.

For information about installing a Log Insight Agent, see Working with vRealize Log Insight Agents.

The vSphere content pack contains agent groups defining specific log files to collect from vCenter Server installations.

For information about vCenter Server log file locations, see `http://kb.vmware.com/kb/1021804` and `http://kb.vmware.com/kb/1021806`.