Using VMware vRealize Log Insight Cloud
You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/
# Contents

1 Using VMware vRealize Log Insight Cloud  6
   Sending Data  7
      Setting Up vRealize Log Insight Cloud  7
      Deploy a Cloud Proxy for vRealize Log Insight Cloud  7
      Deploying a Cloud Native Collector for vRealize Log Insight Cloud  9
      Port Requirements of Cloud Proxy and Cloud Native Collector  12
      Cloud Proxy Resource Limits  13
      Cloud Native Collector Resource Limits  14
   Syslog Agents for vRealize Log Insight Cloud  16
   Forwarding Events and Logs to vRealize Log Insight Cloud  16
   Explore and Modify the Home Page  17
   Searching for Logs  18
      Search for and Filter Logs  18
      Group Logs During Search  19
      Perform Numerical Functions on Log Results  20
      View the Context of a Log  20
      Chart Types for Logs  21
      Event Types  22
      Event Trends  23
   Fields in vRealize Log Insight Cloud  24
      Create an Extracted Field  25
      Clone a Field  26
      Modify an Extracted Field  26
      Delete a Field  27
      Managing Conflicting Fields  27
   Working with Queries  30
      Save a Query  30
      Modify or Clone a Saved Query  30
      Share a Query  31
      Mark a Query as Favorite  31
   Examples of Search Queries  32
      Export Logs  33
      Compare Logs  34
      Pin Queries to the Pinboard  35
   Extracting Metrics from Logs  36
      Configure Metric Extraction  36
   Explore Logs in Real Time  38
   Log Analytics  39
Explore KB Insights 39
Create and Manage a Log RCA Investigation 40

Working with Dashboards 42
Create a Dashboard 43
Modify a Dashboard 44
Add a Widget to a Dashboard 46
Share a Dashboard 48

Configuring Log Sources 48
Audit Logs for VMware Cloud on AWS 49
Logs for Azure VMware Solution 50

Alerts and Notifications 51
Define an Alert 52
Modify an Alert 54
Viewing Recent Alerts 56
Viewing System Alerts 57
Configure an Email Server to Send Alert Notifications 59
Configure a Webhook to Send Alert Notifications 60

Working with Content Packs 62
Enable or Deactivate a Content Pack 63
Export a Content Pack 64
Import a Content Pack 65
Remove a Content Pack 66

Forwarding, Retaining, and Archiving Logs 67
Forward Logs from vRealize Log Insight Cloud 67
Configure Log Retention 69
Configure Log Archiving 70
Download Archived Logs 71

Processing Logs 71
Tag Logs 72
Filter Logs 73
Mask Logs 74

Log Partitions 74
Create a Log Partition 75
View and Explore Logs in a Log Partition 77
Modify the Ingestion Order for Log Partitions 77
Modify a Log Partition 78
Decommission a Log Partition 79
Create a Recall Configuration for a Non-Indexed Log Partition 80

Upload Log Files 81

Securing Logs with API Keys 82
Create an API Key 83
Regenerate an API Key  84
Delete an API Key  84
Viewing Usage Reports  85
Working with vRealize Log Insight Agents  87
  Configure the SSL Connection Between the Cloud Proxy and Log Insight Agents  89
    Main SSL Functions  89
    Configure SSL Parameters for a Log Insight Agent  89
    Generate a Self-Signed Certificate for a Log Insight Agent  91
Integrating vRealize Log Insight Cloud with VMware Products and Services  91
  Integrating vRealize Log Insight Cloud with vSphere  91
    Cloud Proxy as a Syslog Server  92
    Connect vRealize Log Insight Cloud to a vSphere Environment  92
    Configure vRealize Log Insight Cloud to Pull Events, Tasks, and Alarms from a vCenter Server Instance  93
    Configure an ESXi Host to Forward Log Events to vRealize Log Insight Cloud  94
  Integrating vRealize Log Insight Cloud with vRealize Operations Cloud  97
Regional Log Support  97
Using VMware vRealize Log Insight Cloud

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
- Explore and Modify the Home Page
- Searching for Logs
- Extracting Metrics from Logs
- Explore Logs in Real Time
- Log Analytics
- Working with Dashboards
- Configuring Log Sources
- Alerts and Notifications
- Working with Content Packs
- Forwarding, Retaining, and Archiving Logs
- Processing Logs
- Log Partitions
- Upload Log Files
- Securing Logs with API Keys
- Viewing Usage Reports
- Working with vRealize Log Insight Agents
- Integrating vRealize Log Insight Cloud with VMware Products and Services
- Regional Log Support
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 or a Cloud Native Collector.

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. You can use a Cloud Proxy for an on-premise vCenter VM instance with a lower bandwidth (up to 100 MBps).

There are two initial setup tasks for Cloud Proxy.

- Deploy a Cloud Proxy.
  
  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 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.

Cloud Native Collector

The Cloud Native Collector is a Docker container that can be installed on any cloud VM. It provides log aggregation and configuration management, and can be configured to forward logs to vRealize Log Insight Cloud. You can use a Cloud Native Collector for an AWS or Azure VM instance with a higher bandwidth (greater than 100 MBps).

You can install a Cloud Native Collector on an AWS EC2 instance, an Azure VM, or a Google Cloud Platform (GCP) VM instance.

For more information, see Deploying a Cloud Native Collector for vRealize Log Insight Cloud.

Deploy a 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.

If you already have one or more Cloud Proxies, you can deploy an additional Cloud Proxy for your installation.
Prerequisites

- Verify that you have an IP address, a DNS entry, and permissions to deploy OVF templates in vSphere.
- Log in to vSphere and verify that you are connected to a vCenter Server system.
- Verify that outgoing HTTPS traffic is allowed for the Cloud Proxy.
- When you use a web browser to connect to VMware Cloud Services, ensure that the computer that runs the web browser has HTTPS port 443 open to outgoing traffic with access through the firewall to:
  - *.vmwareidentity.com
gaz.csp-vidm-prod.com
  - *.vmware.com
- When you connect to VMware Cloud Services from a data collector, ensure that the computer that the data collector is on has HTTPS port 443 open to outgoing traffic with access through the firewall to:
  - *.vmware.com
  - symphony-docker-external.jfrog.io
  - ci-data-collector.s3.amazonaws.com
- 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 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.

i  Return to vRealize Log Insight Cloud and collect the token key provided on the Install Cloud Proxy dialog box. Click Copy to copy the key. Use the Copy control to ensure you are copying the entire key.

Note  Token keys 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.

7  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 its state is Powered On.

9  Return to the vRealize Log Insight Cloud Install Cloud Proxy dialog box. Wait for a success message saying a connection has been made. (This may take several minutes.)

What to do next

Consult Port Requirements of Cloud Proxy and Cloud Native Collector and then enable log and event forwarding to the Cloud Proxy.

Deploying a Cloud Native Collector for vRealize Log Insight Cloud

The Cloud Native Collector is a Docker container that can be installed on any cloud VM. It provides log aggregation and configuration management, and can be configured to forward logs
to vRealize Log Insight Cloud. You can install a Cloud Native Collector on an AWS EC2 instance, an Azure VM, or a Google Cloud Platform (GCP) VM instance.

**Requirements**
Before installing a Cloud Native Collector, ensure that the following requirements are met.

- Verify that the VM host is supported by Docker.
- Verify that a resolvable host name is assigned for the VM instance in which the Cloud Native Collector is deployed.
- Verify that outgoing HTTPS traffic is allowed for the Cloud Native Collector.
- Verify that you have an API key unique to each Cloud Native Collector.
- When you connect to VMware Cloud Services from a data collector, ensure that the computer that the data collector is on has HTTPS port 443 open to outgoing traffic with access through the firewall to:
  - *.vmware.com
  - projects.registry.vmware.com
  - ci-data-collector.s3.amazonaws.com
- Log in to vRealize Log Insight Cloud by specifying the URL https://www.mgmt.cloud.vmware.com/li/ and entering your login credentials.

**Deployment**
For instructions to deploy a Cloud Native Collector, navigate to the Log Sources page and under Agents, click Cloud Native Collector.

To view the installed Cloud Native Collectors, navigate to Configuration > Cloud Proxies and open the Cloud Native Collectors tab.

**Supported Features**
The Cloud Native Collector supports the following features.

- Syslog and REST data ingestion
- Log aggregation
- Log Insight Agent lifecycle management
- System alerts

**Note** Cloud Native Collector is not supported on Kubernetes.

**Upgrade the Cloud Native Collector**
The Cloud Native Collector is a Docker container that can be configured to forward logs to vRealize Log Insight Cloud. You can upgrade the Cloud Native Collector to your desired version.
Procedure

1. Stop the running Docker container.
   
   ```
   $ docker stop log-forwarder
   ```

2. Remove the stopped container.
   
   ```
   $ docker rm log-forwarder
   ```

3. Run the `docker run` command with the updated version.
   
   ```
   ```

   `<CLOUD_NATIVE_COLLECTOR_VERSION>` is the version to which you are upgrading your Cloud Native Collector. You can find the latest version in the Log Sources page in vRealize Log Insight Cloud.

Troubleshooting the Cloud Native Collector

The Cloud Native Collector is a Docker container that can be configured to forward logs to vRealize Log Insight Cloud. You can share Cloud Native Collector logs if required. When the Cloud Native Collector is not running, you can troubleshoot and resolve the issue.

Sharing Cloud Native Collector Logs

To share Cloud Native Collector logs, follow these instructions.

1. Install the zip utility if it is not installed already.

   ```
   // On Ubuntu and Debian
   $ sudo apt install zip
   
   // On CentOS and Fedora
   $ sudo yum install zip
   ```
2 Run the following command.

```bash
$ zip -r data.zip /data1/ .
```

3 Share the zip file with customer support.

**Troubleshooting when the Cloud Native Collector is not Running**

The `docker ps` command might not show any container running, which can happen in the following scenarios.

**The `hostName` is not provided in the Docker arguments.**

**Error:** Check for the following error in logs under `/data1/log-forwarder/log-forwarder.log`.

```
2022-01-20 05:53:59 [main] ERROR c.v.l.f.h.LogForwarderHost:69 - hostName not provided in docker arguments. Please provide hostName.
2022-01-20 05:53:59 [main] INFO  c.v.l.f.h.LogForwarderHost:55 - Error in starting log-forwarder host:
java.lang.RuntimeException: hostName not provided in docker arguments
    at com.vmware.log.forwarder.host.LogForwarderHost.start(LogForwarderHost.java:70)
at com.vmware.log.forwarder.host.LogForwarderHost.main(LogForwarderHost.java:53)
```

**Solution:** Ensure that you provide the `--hostName=<NAME_OF_THE_HOST>` argument in the Docker run command, where `<NAME_OF_THE_HOST>` is the resolvable host name of the machine or VM in which the Cloud Native Collector is installed.

**The `accessKey` has already been used.**

**Error:** Check for the following error in logs under `/data1/log-forwarder/log-forwarder.log`.

```
java.lang.Exception: {
  "message": "Passed-in accessKey has already been used to register an agent",
  "statusCode": 409,
  "errorCode": 0
}
```

**Solution:** The `lemansAccessKey` is unique for each Cloud Native Collector and cannot be reused. Generate and use a new `lemansAccessKey` for `--lemansAccessKey=<API KEY>`.

**Port Requirements of Cloud Proxy and Cloud Native Collector**

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

**Port Requirements**

Before you configure event forwarding, become familiar with the port requirements for Cloud Proxy and Cloud Native Collector.
<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Ports</th>
<th>Protocol</th>
<th>Service Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard system log</td>
<td>Cloud Proxy or Cloud Native Collector</td>
<td>514</td>
<td>TCP, UDP</td>
<td>Syslog data over TCP or UDP</td>
</tr>
<tr>
<td>Standard system log</td>
<td>Cloud Proxy or Cloud Native Collector</td>
<td>6514</td>
<td>SSL</td>
<td>Syslog data over SSL</td>
</tr>
<tr>
<td>ESXi hosts in vCenter</td>
<td>Cloud Proxy or Cloud Native Collector</td>
<td>1514</td>
<td>SSL</td>
<td>Syslog data over SSL</td>
</tr>
<tr>
<td>vRealize Log Insight Agents or Server</td>
<td>Cloud Proxy or Cloud Native Collector</td>
<td>9000</td>
<td>HTTP</td>
<td>vRealize Log Insight log data in JSON format (CFAPI)</td>
</tr>
<tr>
<td>vRealize Log Insight Agents or Server</td>
<td>Remote Cloud Proxy</td>
<td>9543</td>
<td>HTTPS</td>
<td>vRealize Log Insight log data in JSON format (CFAPI)</td>
</tr>
<tr>
<td>Cloud Proxy or Cloud Native Collector</td>
<td>vRealize Log Insight Cloud</td>
<td>443</td>
<td>TCP</td>
<td>vRealize Log Insight Cloud data over HTTPS</td>
</tr>
<tr>
<td>Cloud Proxy or Cloud Native Collector</td>
<td>vCenter endpoint</td>
<td>80</td>
<td>HTTP</td>
<td>vCenter configuration requests over HTTP</td>
</tr>
<tr>
<td>Cloud Proxy or Cloud Native Collector</td>
<td>vCenter endpoint</td>
<td>443</td>
<td>HTTPS</td>
<td>vCenter configuration requests over HTTPS</td>
</tr>
</tbody>
</table>

### Cloud Proxy Resource Limits

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. While configuring a Cloud Proxy, you must stay at or below the supported maximums for HTTP and syslog requests.

The default configuration for Cloud Proxy is 4 vCPUs and 12 GB RAM. You can use a Cloud Proxy for an on-premise vCenter VM instance with a lower bandwidth (up to 100 MBps). The following resource limits are applicable.

**Note** The following values are for non-SSL ports. You will experience a 15% drop in throughput when you use SSL ports.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Maximums for HTTP Requests</th>
<th>Maximums for Syslog TCP Requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 CPU; 1 GB memory</td>
<td>1400 requests per second or 20 MBps</td>
<td>10,500 messages per second or 3.2 MBps</td>
</tr>
<tr>
<td>2 CPUs; 4 GB memory</td>
<td>2500 requests per second or 48 MBps</td>
<td>17,700 messages per second or 5.4 MBps</td>
</tr>
</tbody>
</table>
### Configuration

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Maximums for HTTP Requests</th>
<th>Maximums for Syslog TCP Requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 CPUs; 8 GB memory</td>
<td>3800 requests per second or 63 MBps</td>
<td>36,000 messages per second or 11 MBps</td>
</tr>
<tr>
<td>8 CPUs, 16 GB memory</td>
<td>5900 requests per second or 100 MBps</td>
<td>75,000 messages per second or 26 MBps</td>
</tr>
</tbody>
</table>

**Note**

- For a configuration of 4 CPUs and 8 GB memory, increase the Cloud Proxy configuration to at least 6 CPUs and 12 GB memory.

- For a configuration of 8 CPUs and 16 GB memory, increase the Cloud Proxy configuration to at least 10 CPUs and 18 GB memory.

### Cloud Native Collector Resource Limits

A Cloud Native Collector is a Docker container that can be installed on any cloud VM. It provides log aggregation and configuration management, and can be configured to forward logs to vRealize Log Insight Cloud. While configuring a Cloud Native Collector, you must stay at or below the supported maximums for HTTP and syslog requests.

**Note** The default configuration for Cloud Native Collector is 1 vCPU and 1 GB RAM. For a higher throughput, you can contact customer support to modify the resource limits.

If your Cloud Native Collector is running on an AWS or Azure VM instance, the following resource limits are applicable.

<table>
<thead>
<tr>
<th>Cloud Native Collector Configuration</th>
<th>Non-SSL Values</th>
<th>SSL Values</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Maximums for HTTP Requests</td>
<td>Maximums for Syslog TCP Requests</td>
</tr>
<tr>
<td>1 CPU; 1 GB memory</td>
<td>7000 requests per second or 26 MBps</td>
<td>38,500 requests per second or 15 MBps</td>
</tr>
<tr>
<td>2 CPUs; 4 GB memory</td>
<td>12,000 requests per second or 50 MBps</td>
<td>62,000 requests per second or 23 MBps</td>
</tr>
</tbody>
</table>
### Cloud Native Collector Configuration

<table>
<thead>
<tr>
<th></th>
<th>Non-SSL Values</th>
<th>SSL Values</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Maximums for HTTP Requests</td>
<td>Maximums for Syslog TCP Requests</td>
</tr>
<tr>
<td>4 CPUs; 8 GB memory</td>
<td>22,000 requests per second or 90 MBps</td>
<td>118,000 requests per second or 47 MBps</td>
</tr>
<tr>
<td>8 CPUs; 16 GB memory</td>
<td>36,500 requests per second or 145 MBps</td>
<td>200,000 requests per second or 85 MBps</td>
</tr>
</tbody>
</table>

**Note** These resource limits are certified on the following AWS and Azure VM instance types.

<table>
<thead>
<tr>
<th>Instance Property</th>
<th>Value for AWS Instance</th>
<th>Value for Azure Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance type</td>
<td>m5.4xlarge</td>
<td>Standard_D16_v3</td>
</tr>
<tr>
<td>Network bandwidth</td>
<td>Up to 10 GBps</td>
<td>8 GBps</td>
</tr>
<tr>
<td>vCPUs</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Memory</td>
<td>64 GiB</td>
<td>64 GiB</td>
</tr>
</tbody>
</table>

### Modify Resources for a Service Proxy

You can modify the CPU and memory resources for a service proxy. Modifying these resources lets you override the default configuration to accommodate higher log ingestion rates.

**Note** Once you modify the resources, vRealize Log Insight Cloud takes some time to apply the updated configuration to the service proxy.

### Prerequisites

Ensure that the OVA version of the corresponding Cloud Proxy is 7.2.0.55581 or later. You can find the OVA version under Summary when you open the Cloud Proxy from the Cloud Proxies page.

### 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. Locate the Cloud Proxy for which you want to modify the resources and click the name of the Cloud Proxy.
4. Under Service Proxies, locate the service for which you want to modify the resources. From the drop-down menu in the lower-right corner of the service details, select Manage Resources and click Execute.
5 In the **Manage Resources** dialog box, modify the memory and CPU details and click **Save**. Ensure that you enter values within the specified limits.

**Note** If only one service proxy is running in the Cloud Proxy, you can allocate resources up to the maximum CPUs and memory assigned to the Cloud Proxy. However, if other service proxies are running in the Cloud Proxy, ensure that you allocate resources according to the available CPUs and memory.

For example, consider a Cloud Proxy with resources of 4 CPUs and 12 GB memory, and you update the resources to 5 CPUs and 14 GB memory. After updating:

- If only one service proxy is running in the Cloud Proxy, you can increase its resources up to 5 CPUs and 14 GB memory.
- If two service proxies are running in the Cloud Proxy in which each proxy is allocated 2 CPUs and 6 GB memory, you can:
  - Increase the CPUs for either proxy by 1 or assign CPUs to each proxy such that they add up to 5.
  - Increase the memory for either proxy by 2 GB, increase the memory for each proxy by 1 GB, or assign memory to each proxy such that it adds up to 14 GB.

### 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**.
### 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:
  1. Enter keywords in the search text box.
  2. Optionally, click the calendar icon to provide a date range for the log results.
  3. 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.
  1. 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 and view logs in real time. 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.

To view logs in real time, in the Explore Logs page, enter a query and click Live Tail. You can also use a saved or favorite query. The logs corresponding to your query are streamed in the Live Tail page. For more information, see Explore Logs in Real Time.

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 one or more partitions next to the search text box to analyze logs in the partition. You can select multiple indexed partitions, multiple non-indexed partitions, or the recall partition, but not all at the same time.

For more information, see:

- Log Partitions
- View and Explore Logs in a Log Partition

Select a time range next to the partition drop-down menu 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.
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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time series</td>
<td>The results from the search time-frame are split into multiple subresults and for each subresult, a group-by is performed.</td>
</tr>
<tr>
<td>Non-time series</td>
<td>A group-by is performed for all the results across the search time-frame.</td>
</tr>
</tbody>
</table>

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

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:

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

**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**.

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:

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

**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=5f6e5elfaf93e4ce) in 11 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 06:41:20.136+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.
<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="增加" /></td>
<td>事件类型新增事件。</td>
</tr>
<tr>
<td><img src="image" alt="增加" /></td>
<td>事件类型事件增加率高。</td>
</tr>
<tr>
<td><img src="image" alt="增加" /></td>
<td>事件类型事件增加率中。</td>
</tr>
<tr>
<td><img src="image" alt="增加" /></td>
<td>事件类型事件增加率低。</td>
</tr>
<tr>
<td><img src="image" alt="增加" /></td>
<td>事件类型事件数量不变。</td>
</tr>
<tr>
<td><img src="image" alt="减少" /></td>
<td>事件类型事件减少率低。</td>
</tr>
<tr>
<td><img src="image" alt="减少" /></td>
<td>事件类型事件减少率中。</td>
</tr>
<tr>
<td><img src="image" alt="减少" /></td>
<td>事件类型事件减少率高。</td>
</tr>
<tr>
<td><img src="image" alt="减少" /></td>
<td>事件类型不再有事件。</td>
</tr>
</tbody>
</table>

**Fields in vRealize Log Insight Cloud**

在大型环境中有大量的日志事件，你不能总是找到对你重要的数据字段。vRealize Log Insight Cloud 支持创建字段来使用在查询和过滤中以解决此问题。字段是一种强大的方式来为无结构的事件添加结构，并允许对数据的文本和视觉表示进行操作。

字段是一种有用的正则表达式查询，用于复杂模式匹配。通过字段，你可以构建查询或构建过滤器，而无需了解、记住或学习复杂的正则表达式。

vRealize Log Insight Cloud 支持索引、内容和提取字段。索引字段是你 vRealize Log Insight Cloud 部署的一部分。内容字段是内容包安装的一部分。而提取，或自定义字段，是由用户创建的。

字段列表在 vRealize Log Insight Cloud 资源中，它们按两个组组织：查询结果和其它字段。字段卡片告诉你字段的类型，并包括用于字段的菜单的一系列可能的用户动作。

使用 VMware vRealize Log Insight Cloud

VMware, Inc. 24
### Table 1-1. Types of fields in vRealize Log Insight Cloud

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

**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.

Managing Conflicting Fields
vRealize Log Insight Cloud uses certain fields for internal processing. If such fields are detected during log ingestion, they conflict with the internal fields, resulting in some of the logs being dropped. To handle this conflict, vRealize Log Insight Cloud takes appropriate actions on such field names to ensure that the corresponding logs are not dropped.

The logs displayed on the Stream tab of the Explore Logs page appear with the incoming or remapped field names, depending on the action taken to avoid conflicts.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>This field appears as <code>id_message_payload</code>.</td>
</tr>
<tr>
<td><em>version</em></td>
<td>This field appears as <code>_version_message_payload</code>.</td>
</tr>
<tr>
<td>timestamp</td>
<td>This field appears as:</td>
</tr>
<tr>
<td></td>
<td>- <code>log_timestamp</code> if the field value can be parsed.</td>
</tr>
<tr>
<td></td>
<td>- <code>timestamp_message_payload</code> if the field value cannot be parsed.</td>
</tr>
<tr>
<td>log_timestamp</td>
<td>This field appears as:</td>
</tr>
<tr>
<td></td>
<td>- <code>log_timestamp</code> if the field value can be parsed.</td>
</tr>
<tr>
<td></td>
<td>- <code>log_timestamp_message_payload</code> if the field value cannot be parsed.</td>
</tr>
</tbody>
</table>

**Note**

- The field names are not case-sensitive.
- If a field with the same name appears multiple times within a single payload, the last value overrides the other values.
- If a payload contains `timestamp` and `log_timestamp` fields and both the field values can be parsed, the `log_timestamp` field displayed in the Explore Logs page is assigned the value of the incoming `log_timestamp` field from the payload.

The following formats are considered parsable for `timestamp` and `log_timestamp` fields:

- `yyyy-MM-dd'T'HH:mm:ss*SSSZZZZ`
- `yyyy MMM dd HH:mm:ss.SSS zzz`
- `MMM dd HH:mm:ss ZZZZ yyyy`
- `dd/MMM/yyyy:HH:mm:ss ZZZZ`
- `MMM dd, yyyy hh:mm:ss a`
- `MMM dd yyyy HH:mm:ss`
- `MMM dd HH:mm:ss yyyy`
- `MMM dd HH:mm:ss ZZZZ`
- `MMM dd HH:mm:ss`
- `yyyy-MM-dd't'HH:mm:ssZZZZ`
- `yyyy-MM-dd't'HH:mm:ss.SSS'Z'
- `yyyy-MM-dd HH:mm:ss ZZZZ`
- `yyyy-MM-dd HH:mm:ssZZZZ`
- `yyyy-MM-dd HH:mm:ss,SSS`
- `yyyy/MM/dd*HH:mm:ss`
Using VMware vRealize Log Insight Cloud

- yyyy MMM dd HH:mm:ss.SSS*zzz
- yyyy MMM dd HH:mm:ss.SSS
- yyyy-MM-dd HH:mm:ss,SSSZZZZ
- yyyy-MM-dd HH:mm:ss.SSS
- yyyy-MM-dd HH:mm:ss.SSSZZZZ
- yyyy-MM-dd'T'HH:mm:ss.SSS
- yyyy-MM-dd'T'HH:mm:ss
- yyyy-MM-dd'T'HH:mm:ss.Z
- yyyy-MM-dd'T'HH:mm:ss.SSS
- yyyy-MM-dd'T'HH:mm:ss
- yyyy-MM-dd+HH:mm:ss:SSS
- yyyy-MM-dd+HH:mm:ss
- yy-MM-dd HH:mm:ss,SSS ZZZZ
- yy-MM-dd HH:mm:ss,SSS
- yy-MM-dd HH:mm:ss
- yy/MM/dd HH:mm:ss
- yyMMdd HH:mm:ss
- yyyyMMdd HH:mm:ss.SSS
- MM/dd/yy*HH:mm:ss
- MM/dd/yy*HH:mm:ss
- MM/dd/yyyy*HH:mm:ss
- MM/dd/yyyy HH:mm:ss ZZZZ
- MM/dd/yyyy HH:mm:ss
- HH:mm:ss
- HH:mm:ss.SSS
- HH:mm:ss,SSS
- dd/MMM HH:mm:ss,SSS
- dd/MMM/yyyy:HH:mm:ss
- dd/MMM/yyyy HH:mm:ss
- dd/MMM/yyyy HH:mm:ss.SSS
- dd MMM yyyy HH:mm:ss
- dd MMM yyyy HH:mm:ss.SSS
- dd MMM yyyy HH:mm:ss*SSS
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. You can also compare logs that are based on the same query criteria but ingested at different times.

**Procedure**

1. Expand the main menu and navigate to **Analytics > Log Compare**.

   **Tip** You can also compare logs from the following pages:
   - **Explore Logs**: Do either of the following:
     - Enter a query and in the upper-right corner of the page, click the compare icon. Add more queries to compare logs.
     - Enter a query and in the upper-right corner of the page, click the pin icon. Pin multiple queries to the pinboard and then click **Compare Logs**.
   - **Analytics > KB Insights**: Select up to four queries and select **Actions > Compare as Queries**.
   - **Log Management > Log Upload**: Select two log bundles and click **Compare Logs**.

2. In the **Compare Logs** page, enter details for the first query.

   - Enter a name for the query.
   - Select the indexed partition on which you want to run the query and click **Apply**. If you do not select an indexed partition, vRealize Log Insight Cloud searches for logs in all the indexed partitions.
   - Enter a start date and time for querying the logs. vRealize Log Insight Cloud uses the start date and time and the duration in the upper-right corner of the page to calculate the time range for the query. When the query runs, it searches for logs within the time range.
   - Add one or more filters for more specific query results. For more information, see **Searching for Logs**.

3. Click **Add Query** to add another query and enter the details described in step 2. You can compare logs for up to four queries.

   **Tip** You can copy an existing query by clicking the copy icon next to the query name.
4 In the upper-right corner of the page, enter the common duration for the added queries. vRealize Log Insight Cloud uses the start date and time in a query and the common duration to calculate the time range for the query. When a query runs, it searches for logs within the time range.

**Note** You can enter a maximum duration of 29 days, 23 hours, and 59 minutes.

5 Click **Compare**.

**Results**

The log comparison is displayed as a stacked line chart and the log results appear side by side in query tabs under the chart. You can select a query tab on the left side and a query tab on the right side to compare the log results.

By default, the chart is based on the logs corresponding to the selected query tabs. However, to view the chart for all the queries, in the upper-right corner of the chart, click **Show All**.

The chart is plotted based on the common time range for the queries. To view the specific time at which a log was ingested, you can hover over the data point in 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/](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/](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](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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the metric extraction configuration.</td>
</tr>
<tr>
<td>Enabled</td>
<td>A toggle that enables or disables the metric extraction configuration. The</td>
</tr>
<tr>
<td></td>
<td>toggle is green when the configuration is enabled and gray when it is</td>
</tr>
<tr>
<td></td>
<td>disabled. If disabled, the metrics for the configuration are not sent to the</td>
</tr>
<tr>
<td></td>
<td>metric store.</td>
</tr>
<tr>
<td>Send To</td>
<td>The metric store URL.</td>
</tr>
<tr>
<td>API Key</td>
<td>The API token from the metric store.</td>
</tr>
<tr>
<td>Source Type</td>
<td>The log filtering criteria.</td>
</tr>
<tr>
<td>Pattern</td>
<td>When you select a log in the <strong>Explore Logs</strong> page to configure metric</td>
</tr>
<tr>
<td></td>
<td>extraction, the system recommends matching grok patterns in this drop-</td>
</tr>
<tr>
<td></td>
<td>down menu. A grok pattern is a named regular expression pattern for parsing</td>
</tr>
<tr>
<td></td>
<td>logs.</td>
</tr>
<tr>
<td></td>
<td>You can select one of the recommended grok patterns. If none of the</td>
</tr>
<tr>
<td></td>
<td>recommended patterns match your log, you can write your own grok pattern</td>
</tr>
<tr>
<td></td>
<td>in the text area under the drop-down menu.</td>
</tr>
<tr>
<td></td>
<td>After defining the grok pattern, click <strong>Parse</strong> to see the metrics that</td>
</tr>
<tr>
<td></td>
<td>can be extracted from your log based on the pattern. The system displays the</td>
</tr>
<tr>
<td></td>
<td>list of numeric metrics that you can send to the metric store, for example,</td>
</tr>
<tr>
<td></td>
<td><code>avgbandwidth</code>, <code>avgIops</code>, and <code>avglatencyinms</code>. You can configure each of</td>
</tr>
<tr>
<td></td>
<td>these metrics in the <strong>Metric Values to Send</strong> section.</td>
</tr>
<tr>
<td>Sample Message</td>
<td>This text area is auto-populated with the text from your selected log.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Select a field from the drop-down menu whose value is sent to the metric</td>
</tr>
<tr>
<td></td>
<td>store.</td>
</tr>
<tr>
<td>Name</td>
<td>The name for the metric in the metric store.</td>
</tr>
</tbody>
</table>
### Option | Description
---|---
**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.

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

9 Click **Save**.

### Explore Logs in Real Time

Use live tail to view logs as they come into vRealize Log Insight Cloud.

**Procedure**

1 Expand the main menu and click **Live Tail**.

**Tip**  To use live tail from the **Explore Logs** page, enter a query and then click **Live Tail** to stream logs corresponding to your query.

2 Type a query and press Enter. You can use multiple keywords and filters. You can also:

- Use a saved query by clicking **Open Saved Query**.
- Use a favorite query by clicking the star icon next to the search text box.
- Select one or more partitions next to the search text box to stream logs from the partition. You can select multiple indexed partitions or non-indexed partitions, but not both at the same time.
For more information about log search, see Search for and Filter Logs.

**Note** Because live tail does not support extracted fields:
- You cannot enter a query with extracted fields.
- When you select a saved or favorite query, the queries with extracted fields are hidden.

The logs corresponding to your query start streaming in real time.

3 Click **Stop Live Tail** to stop streaming the logs and **Start Live Tail** to continue streaming the logs.

4 (Optional) To update the live tail session and stream logs based on a different criteria, do either of the following:
- Type a query and press Enter.
- Type a query, click **Stop Live Tail**, and then click **Start Live Tail**.
- Select a saved or favorite query.

**Log Analytics**

vRealize Log Insight Cloud uses machine learning to perform a Root Cause Analysis (RCA) on your logs. RCA helps you investigate and troubleshoot incidents for a potential root cause in an environment. Additionally, vRealize Log Insight Cloud uses a combination of a set of processes and machine learning methods to provide insights into logs with errors and exceptions, and suggests solutions for these problems.

**Explore KB Insights**

vRealize Log Insight Cloud provides KB articles as solutions for problems in logs. The suggested solutions use the documentation created by various internal and external experts when they solved similar problems in the past.

Navigate to **Analytics > KB Insights** to view insights with severities, chart visualizations, and suggested KB solutions.

**Procedure**

- The **KB Insights** page displays insights for six hours, up to the time you open the page. To refresh the insights for the latest six hours, click the refresh icon in the upper-right corner of the page.
- To modify the interval for which the insights are displayed, click the time range in the upper-right corner of the page.
- To search for insights, enter keywords in the search text box.
- You can compare the queries for multiple insights. Select up to four insights and then select **Actions > Compare as Queries**.
To view the query for an insight in the Explore Logs page, click the three dots icon against the insight and then select Run Query. The query is filtered by the event type corresponding to the insight.

To define an alert based on the query corresponding to an insight, click the three dots icon against the insight and then select Save as Alert. The alert details are pre-populated. You can modify the details and save the alert. For more information, see Define an Alert.

To save the query corresponding to an insight, click the three dots icon against the insight and then select Save as Query. The query is saved with the insight name and opens in the Explore Logs page.

You can sort the insights alphabetically, insights with the most solutions first, and so on.

You can filter insights by severity.

To view detailed information about an insight, click the insight. In addition to the summary, description, severity, and event occurrences of the insight, you can view a chart that shows the trend followed by the insight within the interval selected in the KB Insights page. One or more KB articles are suggested as solutions for the insight. These articles are most likely to contain issues similar to yours, which occurred in the past. These issues were solved by experts and the steps are documented in the KB articles. Under the suggested solutions, the log messages corresponding to the insight are displayed.

- To view the latest insights within the interval highlighted in the upper-right corner above the chart, click the refresh icon next to the interval.
- To modify the time period for which the insight information is displayed, click the interval in the upper-right corner above the chart.
- You can change the graph type and resize or collapse the chart for the insight.
- To explore a solution for the insight, click the link to a KB article and follow the instructions in the article. Click the like button if the article solves your problem, and the dislike button if it does not. This feedback will ensure more accurate solutions for future insights.
- To view the query for the insight in the Explore Logs page with detailed information about the log messages, click Explore Logs in the upper-right corner of the page. The query is filtered by the event type corresponding to the insight.

Create and Manage a Log RCA Investigation

You can create a log RCA (Root Cause Analysis) investigation to troubleshoot logs and identify the root cause for major issues in an environment. Each investigation variation automatically scans all the logs in a user-defined period to find the few significant ones.

The algorithm detects anomalous logs by assessing their frequency, mean, and variance and groups them into log clusters based on their significance.
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 Analytics > Log RCA.
3. In the upper-right corner of the Log RCA page, click New Investigation.
   If you are using log RCA for the first time, click Get Started Now to activate the feature.

   **Note**
   - The log RCA service needs a few minutes to process logs, and a longer time to produce meaningful results. The accuracy of log RCA increases with the amount of time the service runs.
   - You cannot run an RCA for an issue that occurred before you activated the log RCA feature.

4. Enter a name and optionally, a description for the investigation.
5. Select the context for the investigation from the drop-down menu. The default context is the Org Level Context, which indicates the current organization.
   If there is only one context to choose from, the drop-down menu is not displayed.
6. Enter a date and time for the investigation.
7. Select a scan period for the investigation. This period is the duration before the incident date and time within the logs are scanned. You can select a scan period of 2 minutes or 5 minutes.
   For example, if you select the period as 5 minutes and the investigation date and time is August 17, 2021, 11:10 am, the logs within the time frame from August 17, 2021, 11:05 am to August 17, 2021, 11:10 am will be scanned.
8. Select a sensitivity level to detect anomalous logs.
   For example, select the High sensitivity level to focus on minor deviations from the baseline. Select the Low sensitivity level to focus on major deviations for more concise results.
9. Click Start to begin the log RCA investigation.

Results

The details of your investigation and its status appear in the Log RCA page. A green tick mark in the Variations and Status column indicates a successful RCA and a red exclamation mark indicates a failed RCA.

If you cannot locate your investigation in the page, use the search functionality and filters to find it.
Click the investigation name to view the significant log clusters. The clusters with the highest score are displayed at the top, and have a higher probability of being relevant to the root cause. In addition to the score, you can see the number of log messages and key terms in each cluster. The top activity for each cluster is also displayed. To view the logs in a cluster, click See All Activities. To view the logs in the Explore Logs page, click the three dots icon against the log cluster and click View in Explore Logs. This information can help you identify the root cause for your issue.

All your investigations and their related data are retained for a period displayed at the bottom of the Log RCA page. Click Change to update the retention period. In the Investigation Retention Period dialog box, select a retention period and click Save. You can select a minimum retention period of 7 days and maximum retention period of 180 days. When you start using log RCA, the default retention period is 30 days.

To retain an investigation for a longer period, in the Log RCA page, click the three dots icon against the investigation name and then click Save for Future.

To remove an investigation, click the three dots icon against the investigation name and then click Delete Investigation.

Optionally, you can create a variant of an investigation. Click the investigation name and then click New Variation. Update the scan period and log sensitivity level, and click Start. This variant is displayed when you open the investigation. Click each variant to view the corresponding log clusters and other information. The number of variants for each investigation is displayed in the Log RCA page, in the Variations and Status column.

What to do next

After viewing the results of your investigation and identifying the root cause, you can take the required steps to prevent similar issues in the future. You can also improve your monitoring by creating alert rules based on the discovered logs from the Explore Logs page.

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.
   - 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**  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**.

### Add a Widget to a Dashboard

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.

Configuring Log Sources
Log sources such as agents, applications, and application development platforms generate logs. Installing log sources lets vRealize Log Insight Cloud ingest and analyze logs from these sources.
In the **Log Sources** page:

- Click the log source and follow the steps to configure it on the **Setup** tab.
  
  **Tip** To find a log source, enter one or more keywords in the **Search** text box. You can also list the log sources belonging to a category by clicking the category name below the **Search** text box.

- Click the log source and then click the **Content Pack** tab to view the corresponding content pack. On this tab, you can view the details for the content pack. You can also enable, deactivate, or export the content pack. For more information, see **Working with Content Packs**.

- After configuring a log source, click the log source and view the logs on the **Logs** tab.

**Audit Logs for VMware Cloud on AWS**

If you are a VMware Cloud on AWS user with a trial subscription or VMware Cloud core subscription for vRealize Log Insight Cloud, vRealize Log Insight Cloud collects and analyzes audit logs generated in your Software-Defined Data Center (SDDC).

For information about configuring your NSX-T for VMware Cloud on AWS log source, navigate to the **Log Sources** page and under **VMware Cloud**, click **NSX-T for VMware Cloud on AWS**.

For information about vRealize Log Insight Cloud subscriptions, see **vRealize Log Insight Cloud Subscriptions and Billing**.

For information about using VMware Cloud on AWS, see the **VMware Cloud on AWS documentation**.

vRealize Log Insight Cloud classifies SDDC events matching the following rules as audit logs.

**ESXi Audit Events**

```
"text=(esx AND audit)"
"text=(hostd AND vmsvc AND vm AND snapshot)"
"text=(vim.event.HostConnectionLostEvent)"
```

**vCenter Audit Events**

```
"text = (vpxd AND event AND vim AND NOT originator)"
```

**NSX-T Audit Events**

```
"text = (nsx AND audit AND true AND comp AND reqid)"
```

**NSX-T Firewall and Packet Log Events**

```
"text = (nsx AND firewall AND inet)"
"text = (firewall_pktlog AND inet)"
```
User-Driven Activity Events

| log_type Contains Activity |

VMC Notification Gateway Events

| log_type Contains Notification |

VMware Site Recovery Events

| log_type Contains vmw_vmc_srm_logs |

VMware Cloud Services Audit Events

| log_type Contains csp-audit |

NSX-T IDS/IPS Events

| appname Contains IDPS_EVT |

Logs for Azure VMware Solution

If you are an Azure VMware Solution (AVS) user with a paid subscription or VMware Cloud core subscription for vRealize Log Insight Cloud, vRealize Log Insight Cloud collects and analyzes logs generated in your AVS Software-Defined Data Center (SDDC).

For information about configuring your AVS log source, navigate to the Log Sources page and under VMware Cloud, click Azure VMware Solution (AVS).

For information about vRealize Log Insight Cloud subscriptions, see vRealize Log Insight Cloud Subscriptions and Billing.

vRealize Log Insight Cloud classifies AVS SDDC events matching the following rules as logs.

Overview Events

| Event_provider contains "AZURE_AVS" |

Firewall Source Events

| Event_provider contains "AZURE_AVS" |
| vmw_vmc_audit_nsxt_firewall_action exists |
| vmw_vmc_audit_nsxt_firewall_src exists |

Firewall Destination Events

| Event_provider contains "AZURE_AVS" |
| vmw_vmc_audit_nsxt_firewall_action exists |
| vmw_vmc_audit_nsxt_firewall_dst exists |
Application Ports Permitted

- Event_provider contains "AZURE_AVS"
- vmw_vmc_audit_nsxt_firewall_dst_ip_port exists
- vmw_nsxt_firewall_client_to_server_bytes exists
- vmw_vmc_audit_nsxt_firewall_dst_port exists
- text contains 'inet term'

Application Ports Denied

- Event_provider contains "AZURE_AVS"
- vmw_vmc_audit_nsxt_firewall_dst_ip_port exists
- vmw_vmc_audit_nsxt_firewall_dst_port exists
- text contains 'drop' OR text contains 'reject'
- text contains 'inet match'

Severity Events

- Event_provider contains "AZURE_AVS"
- Severity Exists

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. Navigate to Alerts > Alert Definitions.
3. In the upper-right corner of the page, click Create New.

Tip  Alternatively you can navigate to the Explore Logs page and create an alert based on a new or saved query.

- To create an alert based on a new query, run the query and click the exclamation mark icon in the upper-right corner.
  
  You can select a time period and use filters for more specific query results. For more information, see Searching for Logs.

- To create an alert based on a saved query, click the three dots icon in the upper-right corner and click Open Saved Query. Click a saved query and click the exclamation mark icon in the upper-right corner.

4. Enter the following information:

   - A name for the alert.

     You can customize the alert name by including a field in the format ${field_name}, for example, ${hostname}. In the notification title, ${hostname} is replaced with the actual hostname value, for example, vcenter.

   - A short meaningful description of the event that triggers the alert.

     You can customize the alert description by including a field in the format ${field_name}, for example, ${log_type}. In the notification message, ${log_type} is replaced with the actual log type value, for example, audit.
- The query on which the alert is based and a name for the query. You can enter a query or select a favorite query. You can also select one or more indexed partitions to query logs from the partition.

- The trigger conditions for the alert and the severity based on each condition. You can add multiple trigger conditions and set a severity for each trigger condition to Critical, Immediate, Warning, or Info. For each severity, you can send email or webhook notifications in the Choose Notification drop-down menu. To send email notifications, in the Email Recipients text box, enter a recipient email address and click the plus icon. To send webhook notifications, select the check boxes for the webhooks that you want to notify.

<table>
<thead>
<tr>
<th>Trigger Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On every match</td>
<td>This alert query is matched with every log that is ingested. The time period is not relevant.</td>
</tr>
<tr>
<td>Note</td>
<td>You can set this trigger condition when you select Real Time in the time period drop-down menu.</td>
</tr>
<tr>
<td>When total count of events is applied with operation $X$ for threshold $Y$</td>
<td>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.</td>
</tr>
<tr>
<td>When unique count of field $F$ is applied with operation $X$ for threshold $Y$</td>
<td>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.</td>
</tr>
<tr>
<td>When aggregation operation $A$ on field $F$ is applied with operation $X$ for threshold $Y$</td>
<td>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.</td>
</tr>
</tbody>
</table>

- (Optional) Click the Run RCA Investigation toggle button to run a Root Cause Analysis (RCA) on all logs in a five minute window before the time when the alert is triggered. For more information about log RCA, see Create and Manage a Log RCA Investigation.

**Note** When you click the toggle button, it takes a few minutes for the log RCA service to start processing logs.

- (Optional) A recommendation for the alert, which is included in the notification message when the alert is sent.

- (Optional) One or more tags for the alert. You can use existing tags or create new tags. These tags help you group alerts according to your requirement.
(Optional) Customize your alert notification message.

<table>
<thead>
<tr>
<th>Alert Customization</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom fields</td>
<td>Select whether you want to include all the logs or custom fields in the name and description of your alert notification message. If you choose to include custom fields, enter up to 10 custom fields in the text box. To include the custom fields in email notification messages, select a JSON or Table output format. Note: To include the custom fields in webhook notification messages, ensure that the ${customFieldsJson} parameter is included in the payload of the selected webhooks. For more information, see Configure a Webhook to Send Alert Notifications.</td>
</tr>
</tbody>
</table>

- The alert is disabled indefinitely by default. To enable the alert, click the toggle button next to the alert name.

5 Click Save.

Results

The alert definition appears in Alerts > Alert Definitions.

Modify an Alert

You can view the details of an alert and modify an alert definition. You can also add tags to one or more alerts, disable or enable alerts, remove an alert, and add alerts to a dashboard.

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.
3 Locate one or more alerts that you want to view or modify. You can search for alerts by entering keywords in the search text box or by using the sort or filter functionalities. You can filter alerts by severity, type, origin, and tags.

Do either of the following:

- View an alert by clicking the alert name. You can examine alert details such as the query on which the alert is based, the alert definition, the alert instances, and whether the alert is enabled or disabled.
- Modify an alert definition. Click the alert name and click the pencil icon in the upper-right corner. Edit the required details and click Save.
- Enable or disable one or more alerts.

**Note** Each alert listed in the Alerts Definitions page displays information about whether it is enabled or disabled. The toggle button against the alert name is green when the alert is enabled and grey when the alert is disabled.

To enable an alert, click the toggle button, or click the three dots icon against the alert name and click Enable. To enable multiple alerts, select the check boxes against the alert names and click Actions > Enable.

To disable an alert indefinitely, click the toggle button. To disable an alert for a specific period, click the three dots icon against the alert name and click Disable. To disable multiple alerts, select the check boxes against the alert names and click Actions > Disable. Select the period for which you want to disable one or more alerts.

- To disable one or more alerts for the next 30 minutes, one hour, and so on, select the relevant option.
- To disable one or more alerts indefinitely, select Forever.
- To disable one or more alerts for a custom period, such as a maintenance window, select Custom Range and define the period. The alerts are disabled during the period and enabled before and after the period.

- Add tags to one or more alerts. You can select existing tags or create new tags. Tags help you group alerts according to your requirement.

To add tags to an alert, click Add tags or the plus icon under the alert name.

To add tags to multiple alerts, select the check boxes against the alert names and click Actions > Add tags.

**Note** To view all the alert tags and manage them, in the Alert Definitions page, click the three dots icon in the upper-right corner and click Manage Tags. You can create new tags and delete existing tags.

- Add one or more alerts to a dashboard. Select the check boxes against the alert names and click Actions > Add to Dashboard.
  - For information about adding alerts to a new dashboard, see Create a Dashboard.
For information about adding alerts to an existing dashboard, see Add a Widget to a Dashboard.

A widget based on the selected alerts is added to the dashboard.

Remove the alert. Click the three dots icon against the alert name and click Delete.

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 > Triggered Alerts. You can search for alerts by entering keywords in the search text box or by using the filter. You can filter alerts by severity, type, and tags. Alerts appear in a time-line view and a detailed view.

Time-Line View

The first panel displays a graphical time-line view of the recent alerts. You can do the following:

- Click a period in the upper-right corner of the panel to view the alerts triggered during the period.
- Hover over each alert in the time-line to view the time at which the alert was triggered.
- Select a grouping and a graph type based on the grouping.
- Expand the panel for a better view of the alert graph. You can also collapse the panel if required.

Detailed View

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

- Name and description of the alert
- Tags associated with the alert
- Severity of the alert
- The alert type

Note: Periodic alerts are of the type "Total Count" and real-time alerts are of the type "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 do the following:

- Click Details to view the data and threshold with which the alert was triggered.
Click **Definition** to view the alert definition, the query on which the alert is based, and the alert instances. You can also modify, enable or disable, or remove the alert definition.

**Tip** To view the triggered alerts for a specific alert definition, open an alert definition in **Alerts > Alert Definitions** and click the **Alert Instances** tab.

**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:
<table>
<thead>
<tr>
<th>Alert</th>
<th>Description</th>
<th>Action Required</th>
</tr>
</thead>
</table>
| **Cloud Proxy Dropping Logs** | The Cloud Proxy or Cloud Native Collector configured to send logs to the vRealize Log Insight Cloud service is dropping logs. Logs are dropped because of a latency between the Cloud Proxy or Cloud Native Collector and the service, or because the Cloud Proxy or Cloud Native Collector is under a heavy load. | Ensure that:  
  - The Cloud Proxy or Cloud Native Collector is resourced correctly.  
  - There is no high latency between the Cloud Proxy or Cloud Native Collector 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, verify the following:  
  - The log forwarding endpoint configuration is correct.  
  - If the destination for the log forwarding configuration is **Cloud**, ensure that the log forwarding endpoint is accessible across the Internet.  
  - If the destination for the log forwarding configuration is **On Premise**, ensure that the log forwarding endpoint is accessible to the Cloud Proxy configured to forward logs. |
| **Inactive Cloud Proxy**      | The connection between the Cloud Proxy or Cloud Native Collector and the vRealize Log Insight Cloud service is broken.                                                                                           | Ensure that:  
  - The Cloud Proxy or Cloud Native Collector is resourced correctly.  
  - The Cloud Proxy or Cloud Native Collector can connect to the vRealize Log Insight Cloud service. |
| **Inactive Log Insight Agent**| The Log Insight Agent cannot communicate with vRealize Log Insight Cloud.                                                                                                                                       | If you are an administrator, ensure that:  
  - The Cloud Proxy or Cloud Native Collector is up and running.  
  - The Log Insight Agent is running.  
  - The Log Insight Agent is able to reach the Cloud Proxy or Cloud Native Collector. |
| **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.                                                                                               |
### 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:

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

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification Type</td>
<td>Select whether the webhook configuration is for an alert notification or a system alert notification.</td>
</tr>
</tbody>
</table>
| 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.  
  In addition to the listed parameters, you can also add the following parameters to the payload:  
  - "Tags": "${tagsJson}" to view all the tags associated with an alert definition  
  - "allLogs": "${allLogsJson}" to view all the logs associated with an alert definition  
  - "customFields": "${customFieldsJson}" to view the custom fields associated with an alert definition |

6 Click **Save**.

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

**What to do next**

When you create an alert definition, you can select your webhook to send alert notifications.
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 deactivate 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.

You can view content packs that have one or more enabled versions on the **Enabled** tab.

All tabs display only one version of each content pack. To select a different version, in the content pack card, click the version drop-down menu and select the desired version. The absence of a version drop-down menu indicates that the content pack has only one version.

To view the details of a content pack, locate the content pack on a tab in the **Content Packs** page. You can use the search functionality to find the content pack. In the content pack card, optionally select a version and click **Details**. The information for the selected version of 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.

**vRLI Agents**
- The list of Log Insight Agent configurations in the content pack.

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

Enable or Deactivate a Content Pack

Enable a content pack to start using its dashboards, queries, and other resources. Deactivate a content pack when you no longer need it.

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 relevant tab, locate the content pack that you want to enable or deactivate. You can use the search functionality to find the content pack.

3  (Optional) If the content pack has more than one version, in the content pack card, click the version drop-down menu to select the version that you want to enable or deactivate.

4  Do either of the following:
   - To enable the content pack, click Enable.
   - To deactivate the content pack, click Actions > Disable.

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 deactivate a content pack, if the elements of the content pack are used by users in your organization, a pop-up window appears, which describes where the elements are used. You cannot deactivate the content pack until you remove the dependent elements.
Results

- When you enable a content pack, the content pack appears on the Enabled tab of the Content Packs page with information such as the content pack name, description, and enabled versions in the content pack card.

**Note**  If the content pack has more than one version and:
  
  - If you select an enabled version from the version drop-down menu, you can see the Actions and Details buttons in the content pack card.

- If you select a deactivated version from the version drop-down menu, you can see the Enable and Details buttons in the content pack card.

Enabled elements of the content pack appear in respective pages such as Alerts and Dashboards. You can click each element to for more information.

- When you deactivate a content pack:
  
  - If the content pack has only one version or if all the versions of the content pack are deactivated, the content pack no longer appears on the Enabled tab.

- If the content pack has more than one version and has other enabled versions, the content pack appears on the Enabled tab. However, selecting the deactivated version displays the Enable and Details buttons in the content pack card, which indicates that the selected version of the content pack is no longer enabled.

- In the content pack card, you can select the deactivated version and click Details to view the elements of the content pack such as dashboards, alerts, and queries. However, you cannot click each element for more information.

Export a Content Pack

Export a 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 the queries, charts, and alerts selected for export are included in the exported 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 relevant tab, locate the content pack that you want to export. You can use the search functionality to find the content pack.

3. If the content pack has more than one version, in the content pack card, click the version drop-down menu to select the version that you want to export.
4 Click **Actions > Export**.

**Note** You can export only an enabled version of a content pack.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the content pack.</td>
</tr>
<tr>
<td>Namespace</td>
<td>Enter any user-driven namespace such as com.mycompany.content.</td>
</tr>
<tr>
<td>Version</td>
<td>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.</td>
</tr>
</tbody>
</table>

6 Select the user-defined elements that you want to export.

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

**Results**

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. 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 you import the same content pack with a different version, the version drop-down menu also appears in the private content pack card.

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, locate the content pack that you want to remove. You can use the search functionality to find the content pack.

3 In the content pack card, click Actions > Delete.

Note When you remove 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 remove 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique display name for the log forwarding configuration.</td>
</tr>
<tr>
<td>Destination</td>
<td>Select <strong>Cloud</strong> if the endpoint can be accessed from WAN, else select <strong>On Premise</strong>.</td>
</tr>
<tr>
<td>Cloud Proxy</td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Endpoint Type</td>
<td>The endpoint to which messages are forwarded, such as:</td>
</tr>
<tr>
<td></td>
<td><strong>vRealize Log Insight</strong></td>
</tr>
<tr>
<td></td>
<td>The destination is a vRealize Log Insight server.</td>
</tr>
<tr>
<td></td>
<td><strong>Splunk</strong></td>
</tr>
<tr>
<td></td>
<td>The destination is a Splunk server or cloud.</td>
</tr>
<tr>
<td></td>
<td>To forward all fields to Splunk, select the <strong>Forward all fields</strong> check box.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you do not select the check box, only these fields are forwarded - <code>log_timestamp</code>, <code>source</code>, <code>host</code>, <code>event</code>, and <code>sddc_id</code>.</td>
</tr>
<tr>
<td></td>
<td><strong>UDP</strong></td>
</tr>
<tr>
<td></td>
<td>The destination is listening on a UDP port. Select the format in which the messages are forwarded.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>TCP</strong></td>
</tr>
<tr>
<td></td>
<td>The destination is listening on a TCP port. Select the format in which the messages are forwarded.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong></td>
</tr>
<tr>
<td></td>
<td>All other scenarios.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Endpoint URL</td>
<td>The URL for the destination endpoint in the relevant format:</td>
</tr>
<tr>
<td><strong>vRealize Log Insight</strong></td>
<td>The URL is in the format <code>log-insight-server/api/v1/events/ingest/log-intelligence</code>, where <code>log-insight-server</code> is the host address or host name of the vRealize Log Insight server.</td>
</tr>
<tr>
<td>Splunk</td>
<td>The Splunk server or forwarder URL.</td>
</tr>
<tr>
<td>UDP</td>
<td>The URL is in the format <code>udp://10.197.11.148:514</code>.</td>
</tr>
<tr>
<td>TCP</td>
<td>The URL is in the format <code>tcp://10.197.11.148:514</code>.</td>
</tr>
<tr>
<td>Query</td>
<td>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.</td>
</tr>
<tr>
<td>Headers (optional)</td>
<td>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.</td>
</tr>
<tr>
<td>Tags (optional)</td>
<td>A tag name and predefined value. Tags let you query events more easily. You can add multiple comma-separated tags.</td>
</tr>
</tbody>
</table>

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 Provide the following information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique display name for the log retention configuration.</td>
</tr>
<tr>
<td>Query</td>
<td>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.</td>
</tr>
<tr>
<td>Retention Days</td>
<td>The number of days for which you want to retain the logs.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique display name for the log archival configuration.</td>
</tr>
<tr>
<td>Query</td>
<td>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.</td>
</tr>
<tr>
<td>Retention Days</td>
<td>The number of days for which you want to retain the logs.</td>
</tr>
</tbody>
</table>

Note vRealize Log Insight Cloud can retain log data for a minimum period of 90 days, up to a maximum period of seven years.

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.
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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the log tagging configuration.</td>
</tr>
<tr>
<td>Fields</td>
<td>Key-value pairs that need to be tagged to the logs. You can add multiple key-value pairs to the logs.</td>
</tr>
<tr>
<td>Apply to all logs / Apply to specific logs</td>
<td>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.</td>
</tr>
</tbody>
</table>

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. 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.

Log Partitions

Log partitions store logs based on the routing filter that you configure for each partition in the Log Partitions page. You can query and analyze logs from specific partitions in the Explore Logs page.

To create and manage log partitions, you must have a premium or trial subscription for vRealize Log Insight Cloud. For information about subscriptions, see vRealize Log Insight Cloud Subscriptions and Billing.
According to your requirement, you can create indexed or non-indexed log partitions.

**Indexed partitions**

In an indexed partition, you are billed only for the volume of logs stored in the partition. You can search and analyze logs with quick results and without incurring additional costs. Use indexed partitions to store logs that you plan to query regularly.

Indexed partitions retain logs for up to 30 days.

**Non-indexed partitions**

In a non-indexed partition, you are billed for the volume of logs and also for searching the logs. Querying logs renders slower results than indexed partitions. Use non-indexed partitions to store logs that you do not plan to query regularly.

Non-indexed partitions retain logs for up to seven years. If you intend to query the logs frequently, you can move all or specific logs to a common recall partition for 30 days. In this partition, you can search and analyze the logs with quicker results and at no extra cost.

**Note** Alerts and dashboard widgets are not operational in non-indexed partitions.

You can change the order in which logs are ingested into log partitions, based on their routing filters. Logs are ingested into non-indexed partitions first, followed by indexed partitions. The logs that do not match the routing filters in any of the indexed or non-indexed partitions go to the default indexed partition, which is read-only and stores logs for 30 days.

**Note** You can create a maximum of 10 log partitions in an organization.

**Create a Log Partition**

Create a log partition to ingest logs based on a routing filter.

**Prerequisites**

Verify that you have a premium or trial subscription for vRealize Log Insight Cloud.

- If you have a trial subscription, you must activate log partitions before using them. To activate partitions, go to Log Management > Log Partitions and click Enable Partitions.
- If you have a free subscription, you cannot use log partitions.
- If you have a premium subscription, log partitions are available by default, and you do not have to activate the feature.

For information about subscriptions, see vRealize Log Insight Cloud Subscriptions and Billing.

**Procedure**

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

4 Provide the following information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique display name for the log partition.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the log partition.</td>
</tr>
<tr>
<td>Type</td>
<td>Select whether you want to create an indexed or a non-indexed partition.</td>
</tr>
<tr>
<td></td>
<td>- An indexed partition stores logs for up to 30 days. Use indexed partitions to store logs that you plan to query regularly. You are billed for the ingested log volume, but not for querying the logs.</td>
</tr>
<tr>
<td></td>
<td>- A non-indexed partition stores logs for up to seven years. Use non-indexed partitions to store logs that you do not plan to query regularly.</td>
</tr>
<tr>
<td></td>
<td>You are billed for both the ingested log volume and for querying the logs.</td>
</tr>
<tr>
<td>Retention</td>
<td>Enter the number of days for which you want to retain logs in the log partition.</td>
</tr>
<tr>
<td>Data Groups</td>
<td>If you are creating a non-indexed partition, you can group the log data by fields.</td>
</tr>
<tr>
<td></td>
<td>Select the <strong>Group Data By</strong> check box and select the field by which you want to group the data.</td>
</tr>
<tr>
<td></td>
<td>Grouping log data by the relevant field helps store the logs effectively in sub-folders, and displays quicker results when you query logs from your partition in the <strong>Explore Logs</strong> page.</td>
</tr>
<tr>
<td>Routing Filter</td>
<td>Add one or more routing filters to ingest logs corresponding to the filters into your partition. You can also use a favorite query.</td>
</tr>
<tr>
<td></td>
<td>Optionally, click <strong>Show Logs</strong> to preview the filtered log results and <strong>Show Chart</strong> to view a graphical representation of the log results.</td>
</tr>
<tr>
<td>Data Forwarding to Non-Indexed Partitions</td>
<td>If you are creating a non-indexed partition, you can select the <strong>Forward Data to Indexed Partitions</strong> check box to store the logs in both your partition and in indexed partitions.</td>
</tr>
<tr>
<td></td>
<td>You can select either of the following options:</td>
</tr>
<tr>
<td></td>
<td>- Forward all the logs in your partition.</td>
</tr>
<tr>
<td></td>
<td>- Add one or more filters to forward specific logs in your partition.</td>
</tr>
<tr>
<td></td>
<td>If some or all the forwarded logs match the filters defined in certain indexed partitions, these logs are stored in the relevant partitions, based on the ingestion order. The forwarded logs that are not stored in any indexed partition go to the default indexed partition.</td>
</tr>
</tbody>
</table>

5 Click **Create**.

**Results**

The partition appears in the **Log Partitions** page, under the relevant section. Logs flowing into vRealize Log Insight Cloud that match your routing filter will be ingested into this partition.

**What to do next**

You can query and analyze the logs in your partition. For more information, see View and Explore Logs in a Log Partition.
View and Explore Logs in a Log Partition

You can view the details for a log partition and analyze the logs in the partition from the Explore Logs page.

Prerequisites

Verify that you have a premium or trial subscription for vRealize Log Insight Cloud.

- If you have a trial subscription, you must activate log partitions before using them. To activate partitions, go to Log Management > Log Partitions and click Enable Partitions.
- If you have a free subscription, you cannot use log partitions.
- If you have a premium subscription, log partitions are available by default, and you do not have to activate the feature.

For information about subscriptions, see vRealize Log Insight Cloud Subscriptions and Billing.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
3. Locate the partition that you want to view in the Indexed Partitions or Non-Indexed Partitions section.
   
   **Tip** You can also search for the partition by entering keywords in the search text box.

4. Click the partition name to view details such as the partition description, log volume, retention period, routing filter, and so on.

   Under Routing Filters, click Show Logs to view the latest logs ingested into the partition. Click Show Chart to view a graphical representation of the logs in the partition.

5. To analyze the logs in the partition from the Explore Logs page, in the upper-right corner, click Explore Logs.

   To analyze logs in multiple partitions, open the Explore Logs page and select one or more partitions next to the search text box. You can select multiple indexed partitions, multiple non-indexed partitions, or the recall partition, but not all at the same time.

   For more information, see Search for and Filter Logs.

Modify the Ingestion Order for Log Partitions

Modify the order in which routing filters are evaluated for log ingestion into indexed or non-indexed partitions. Routing filters for non-indexed partitions are evaluated first, followed by indexed partitions. The default indexed partition is always the last partition into which logs are ingested, if no other routing filter matches.
Prerequisites

Verify that you have a premium or trial subscription for vRealize Log Insight Cloud.

- If you have a trial subscription, you must activate log partitions before using them. To activate partitions, go to Log Management > Log Partitions and click Enable Partitions.
- If you have a free subscription, you cannot use log partitions.
- If you have a premium subscription, log partitions are available by default, and you do not have to activate the feature.

For information about subscriptions, see vRealize Log Insight Cloud Subscriptions and Billing.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
3. Click Ingestion Order and then click Indexed Partitions or Non-Indexed Partitions.
4. Click a partition and drag it to the position that you want.
   
   **Note** You cannot modify the ingestion order of a decommissioned partition.

5. Click Save.

Modify a Log Partition

Modify the details for a log partition such as the name, description, retention period, routing filter, and so on.

**Note** You cannot modify the default indexed partition.

Prerequisites

Verify that you have a premium or trial subscription for vRealize Log Insight Cloud.

- If you have a trial subscription, you must activate log partitions before using them. To activate partitions, go to Log Management > Log Partitions and click Enable Partitions.
- If you have a free subscription, you cannot use log partitions.
- If you have a premium subscription, log partitions are available by default, and you do not have to activate the feature.

For information about subscriptions, see vRealize Log Insight Cloud Subscriptions and Billing.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
3 Locate the partition that you want to modify in the Indexed Partitions or Non-Indexed Partitions section.

**Tip** You can also search for the partition by entering keywords in the search text box.

4 Click the three dots icon against the partition name and click **Edit Partition**.

5 Modify the relevant information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Modify the display name for the log partition.</td>
</tr>
<tr>
<td>Description</td>
<td>Modify the description for the log partition.</td>
</tr>
<tr>
<td>Retention</td>
<td>Modify the number of days for which you want to retain logs in the log partition. You can retain logs for up to 30 days in an indexed partition and up to seven years in a non-indexed partition.</td>
</tr>
<tr>
<td>Routing Filter</td>
<td>Modify the routing filters to ingest the logs corresponding to the filters into your partition. You can also use a favorite query. Optionally, click <strong>Show Logs</strong> to preview the filtered log results and <strong>Show Chart</strong> to view a graphical representation of the log results.</td>
</tr>
</tbody>
</table>
| Data Forwarding to Non-Indexed Partitions | If you are modifying a non-indexed partition, do either of the following:  
  - Select the **Forward Data to Indexed Partitions** check box to store the logs in both your partition and in indexed partitions. You can either forward all the logs in your partition or add filters to forward specific logs in your partitions.  
    - If some or all the forwarded logs match the routing filters defined in certain indexed partitions, these logs are stored in the relevant partitions, based on the ingestion order. The forwarded logs that are not stored in any indexed partition go to the default indexed partition.  
  - Clear the **Forward Data to Indexed Partitions** check box if you do not want to forward the log data in your partition to indexed partitions. |

**Note**

- You cannot modify the partition type.
- If you are modifying a non-indexed partition for which you have selected the data grouping option, you cannot modify the fields by which the log data is grouped.

6 Click **Update**.

**Decommission a Log Partition**

You can decommission a partition to stop the ingestion of new logs into the partition.

**Note** You cannot decommission the default indexed partition.
Prerequisites

Verify that you have a premium or trial subscription for vRealize Log Insight Cloud.

- If you have a trial subscription, you must activate log partitions before using them. To activate partitions, go to Log Management > Log Partitions and click Enable Partitions.
- If you have a free subscription, you cannot use log partitions.
- If you have a premium subscription, log partitions are available by default, and you do not have to activate the feature.

For information about subscriptions, see vRealize Log Insight Cloud Subscriptions and Billing.

Procedure

1. Click the two arrows icon in the upper-left corner of the screen to expand the main menu.
3. Locate the partition that you want to decommission in the Indexed Partitions or Non-Indexed Partitions section.

   **Tip** You can also search for the partition by entering keywords in the search text box.

4. Click the three dots icon against the partition name and click Decommission Partition.
5. In the pop-up window, click Decommission.

Results

Decommissioning stops the ingestion of new logs into the partition. The partition is active for its retention period starting from the last ingestion date and time. When the partition is active, you can view the partition in the Log Partitions page and query its logs, but you cannot edit the partition. After the retention period, the partition is removed permanently.

Create a Recall Configuration for a Non-Indexed Log Partition

In a non-indexed partition, querying logs renders slow results. If you intend to query the logs frequently, you can move all or specific logs to a common recall partition for 30 days. In this partition, you can search and analyze the logs with quicker results. Create a configuration to copy logs from a non-indexed partition to the common recall partition.

Prerequisites

- Verify that you have a premium or trial subscription for vRealize Log Insight Cloud.
  - If you have a trial subscription, you must activate log partitions before using them. To activate partitions, go to Log Management > Log Partitions and click Enable Partitions.
  - If you have a free subscription, you cannot use log partitions.
  - If you have a premium subscription, log partitions are available by default, and you do not have to activate the feature.
For information about subscriptions, see vRealize Log Insight Cloud Subscriptions and Billing.

- Verify that you have at least one non-indexed log partition in the system.

**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 Partitions**.
3. In the upper-right corner, click **Recall Logs**.
4. Provide the following information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique display name for the recall configuration.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the recall configuration.</td>
</tr>
<tr>
<td>Select Partition</td>
<td>Select the non-indexed partition for which you want to recall logs.</td>
</tr>
<tr>
<td>Time Range and Filters for Recalling</td>
<td></td>
</tr>
</tbody>
</table>
  - Select a time range to recall logs within the range.  
  - Select the option to recall all the logs in the partition or add filters to recall specific logs. |
| Notify                      | Optionally, you can notify certain users when the recall process for your configuration is finished. |

5. Click **Recall**.

The recall process takes some time to finish, depending on the volume of logs being recalled. You can view the recall status of your configuration when you expand the **Recalled Logs** section in the **Log Partitions** page and click the name of the common recall partition.

**Upload Log Files**

When you start using vRealize Log Insight Cloud and you do not have any logs to analyze, you can upload log files from your local system to the default partition. You can also upload log files to examine logs from various third-party sources.

After uploading the log files, you can query the logs in the **Explore Logs** page, create dashboards, define alerts, and so on.

**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 Upload**.
3. Click **Upload Logs**.
In the **Upload Log Files** dialog box, upload log files by browsing your local system or from the command line.

- To upload log files by browsing your local system, do the following:
  a. Click **Browse Log Files**.
  b. Select up to 10 files of 10 MB each from your system and click **Open**.
  
  **Note** The supported file formats are `.log` and `.txt`.
  
  The log files are listed in the dialog box.
  c. Optionally, you can remove the log files that you do not want to upload.
  d. Click **Upload**.

- To upload log files from the command line, do the following:
  a. Click **Copy cURL Command**.
     
     The cURL command appears.
  b. Click the copy icon against the cURL command to copy the command.
  c. Open your Command Prompt window and paste the command in the window.
  d. In the command, replace `<<FILE-PATH>>` with the location of the log files.
  e. Run the command.

**Results**

The uploaded log bundles appear in the **Log Upload** page, along with the upload status, log volume, and so on. You can click the refresh icon to view the latest upload status. As soon as you upload a log bundle, its upload status is **Uploaded**. When vRealize Log Insight Cloud starts ingesting logs from the bundle, its upload status is **Ingesting**. When ingestion is finished, the upload status is **Success**, and you can start analyzing the logs.

**What to do next**

To query the uploaded logs, click the three dots icon against the corresponding log bundle and click **Open in Explore Logs**.

To compare the uploaded logs in different log bundles, select two log bundles and click **Compare Logs**.

**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 \\nhttps://data.mgmt.cloud.vmware.com/le-mans/v1/streams/ingestion-pipeline-stream \\n-H 'Authorization:Bearer wj32145ROzycKFvsIh34aSfz8cONRmZ' \\n-H 'Content-Type:application/json' \\n-H 'structure:default' \\n-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 volume of log data ingested and stored, 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:

#### Ingestion & Storage Summary

This tab displays details about the amount of log data streamed into the system, the log volume in indexed and non-indexed storage, and the volume of non-billable logs ingested in the last 7-30 days. You can select the period for which the data is displayed. You must select a minimum period of seven days. You can select up to a maximum period of 30 days.

**Usage Summary**

This section displays the following information:

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Today's Ingestion</td>
<td>The volume of logs ingested since 00:00 UTC.</td>
</tr>
<tr>
<td>Ingestion Volume</td>
<td>The volume of logs ingested within the selected period.</td>
</tr>
<tr>
<td>Indexed Storage</td>
<td>The volume of logs ingested into indexed storage within the selected period.</td>
</tr>
<tr>
<td>Non-indexed Storage</td>
<td>The volume of logs ingested into non-indexed storage within the selected period.</td>
</tr>
<tr>
<td>Non-indexed Scan</td>
<td>The volume of logs parsed for queries run on non-indexed storage, including recalled logs.</td>
</tr>
<tr>
<td>Non-billable Logs</td>
<td>The volume of logs that are not billed.</td>
</tr>
</tbody>
</table>

**Ingestion**

This chart displays the volume of logs ingested daily within the selected period. You can choose to view billable logs, non-billable logs, or both.

**Top 5 Partitions (by Storage)**
This chart displays the top five partitions with the largest volume of logs ingested within the selected period. You can choose to view the log volume in the top five indexed partitions, non-indexed partitions, or both.

**Storage**

This chart displays the daily ingestion of non-billable logs and logs in indexed and non-indexed storage, within the selected period. You can choose to view logs in indexed storage, logs in non-indexed storage, non-billable logs, or all of them. In the upper-right corner of the chart, you can select the partitions for which you want to view the log data. You can select multiple indexed partitions, multiple non-indexed partitions, or both.

To download a report of the ingestion and storage within the selected period in CSV format, click **Download CSV** in the upper-right corner of the tab.

**Queries**

This tab displays information about the log volume scanned, the total number of queries executed, and the number of unique users executing queries. You can view charts with details about the logs examined over time, the logs examined per page, and the number of queries executed over time. Additionally, the tab also displays a table with more information about each query such as the query filter, the partitions in which the query is executed, the time range used in the query, and so on. By default, this information is displayed for indexed storage and a time range of the last 30 minutes. However, you can change the storage type to non-indexed and select a different time range.

**Queries Summary**

This section displays the following information:

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume Scanned</td>
<td>The volume of logs examined in the selected storage type within the selected time range.</td>
</tr>
<tr>
<td>Total Queries</td>
<td>The total number of queries executed in the selected storage type within the selected time range.</td>
</tr>
<tr>
<td>Unique Users</td>
<td>The number of unique users who have executed queries in the selected storage type within the selected time range.</td>
</tr>
</tbody>
</table>

**Data Scanned over Time**

This chart displays the volume of logs (in GB) examined in the selected storage type over the selected period of time.

**Data Scanned per Page**

This chart displays the volume of logs (in GB) examined per page in the selected storage type within the selected time range.

**Total Queries over Time**
This chart displays the number of queries executed in the selected storage type over the selected period of time.

Queries

This table displays the following information about the queries executed in the selected storage type within the selected time range.

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query</td>
<td>The filter used to execute the query. If a filter was not used, No Filter is displayed. You can filter this column to narrow the results.</td>
</tr>
<tr>
<td>Partitions</td>
<td>The partitions in which the query was executed.</td>
</tr>
<tr>
<td>Time Window</td>
<td>The time range used while executing the query.</td>
</tr>
<tr>
<td>Data Scanned</td>
<td>The volume of logs examined when the query was executed.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the query, whether it is finished or still running.</td>
</tr>
<tr>
<td>Triggered By</td>
<td>The user who executed the query.</td>
</tr>
<tr>
<td>Triggered At</td>
<td>The time at which the query was executed.</td>
</tr>
<tr>
<td>Query Page</td>
<td>The source of the query.</td>
</tr>
</tbody>
</table>

You can sort the queries by the most recent queries or by the queries with the most logs scanned.

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.
Configure the SSL Connection Between the Cloud Proxy and Log Insight Agents

You can use the SSL function to provide SSL-only connections between Log Insight Agents and the Cloud Proxy through the secure flow of the Ingestion API. You can also configure various SSL parameters for Log Insight Agents.

**Note** The Cloud Proxy has a self-signed certificate that is used for the secure transmission of data between the Cloud Proxy and Log Insight Agents.

Main SSL Functions

Understanding the main SSL functions can help you configure the Log Insight Agents accurately.

The Log Insight Agent stores certificates and uses them to verify the identity of the Cloud Proxy during all but the first connection to the Cloud Proxy. If the identity cannot be confirmed, the Log Insight Agent rejects the connection and writes an appropriate error message to the log. Certificates received by the agent are stored in the `cert` folder.

- For Windows, go to `C:\ProgramData\VMware\Log Insight Agent\cert`.
- For Linux, go to `/var/lib/loginsight-agent/cert`.

When the Log Insight Agent establishes a secure connection with the Cloud Proxy, the agent checks the certificate received from the Cloud Proxy for validity. The Log Insight Agent uses system-trusted root certificates.

- The Linux agent loads trusted certificates from `/etc/pki/tls/certs/ca-bundle.crt` or `/etc/ssl/certs/ca-certificates.crt`.
- The Windows agent uses system root certificates.

If the Log Insight Agent has a locally stored self-signed certificate and receives a different valid self-signed certificate with the same public key, the agent accepts the new certificate. This can happen when a self-signed certificate is regenerated using the same private key but with different details, such as a new expiration date. Otherwise, the connection is rejected.

Configure SSL Parameters for a Log Insight Agent

You can edit the Log Insight Agent configuration file to change the SSL configuration, add a path to the trusted root certificates, and say whether the agent accepts certificates.

If a certificate is not available, you can generate a self-signed certificate by following the instructions in Generate a Self-Signed Certificate for a Log Insight Agent.

The procedure for configuring SSL parameters applies to the Log Insight Agents for Windows and Linux.

Prerequisites

For the Linux agent:

- Log in as `root` or use `sudo` to run console commands.
- Log in to the Linux machine on which you installed the Log Insight Agent, open a console, and run `pgrep liagent` to verify that the Linux agent is installed and running.

For the Windows agent:

- Log in to the Windows machine on which you installed the Log Insight Agent and start the Services manager to verify that the Windows agent service is installed.

Procedure

1. Navigate to the folder containing the `liagent.ini` file.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td><code>/var/lib/loginsight-agent/</code></td>
</tr>
<tr>
<td>Windows</td>
<td><code>%ProgramData%\VMware\Log Insight Agent</code></td>
</tr>
</tbody>
</table>

2. Open the `liagent.ini` file in any text editor.

3. Add the following keys to the `[server]` section of the `liagent.ini` file.

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ssl_ca_path</code></td>
<td>Overrides the default storage path for root Certificate Authority-signed certificates, which are used to verify connection peer certificates. <strong>Linux</strong>: If no value is specified, the agent uses the value assigned to the <code>LI_AGENT_SSL_CA_PATH</code> environment variable. If the value is not present, the agent attempts to load trusted certificates from the <code>/etc/pki/tls/certs/ca-bundle.crt</code> file or from the <code>/etc/ssl/certs/ca-certificates.crt</code> file. <strong>Windows</strong>: If no value is specified, the agent uses the value specified by the <code>LI_AGENT_SSL_CA_PATH</code> environment variable. If the value is not present, the agent loads certificates from the Windows root certificate store.</td>
</tr>
<tr>
<td><code>ssl_accept_any</code></td>
<td>Defines whether any certificates are accepted by the Log Insight Agent. The possible values are yes, 1, no, or 0. When the value is set to yes or 1, the agent accepts any certificate from the Cloud Proxy and establishes a secure connection for sending data. The default value is no. <strong>Note</strong>: Because Cloud Proxy presents a self-signed certificate by default, you must set the value of <code>ssl_accept_any</code> to 1.</td>
</tr>
</tbody>
</table>

4. Save and close the `liagent.ini` file.
Example: Configuration

The following is an example of the SSL configuration.

```
proto=cfapi
port=9543
ssl=yes
ssl_ca_path=/etc/pki/tls/certs/ca.pem
ssl_accept_any=no
```

Generate a Self-Signed Certificate for a Log Insight Agent

You can generate a self-signed certificate for a vRealize Log Insight Windows or Linux agent by using the OpenSSL tool.

Prerequisites

Download the appropriate installer for OpenSSL from https://www.openssl.org/community/binaries.html. Use the downloaded OpenSSL installer to install it on Windows.

Procedure

1. Create a certificate folder in the path mentioned for `ssl_ca_path` in the `liagent.ini` file.
2. Open the Command Prompt and run the following command.

   ```
   /etc/pki/tls/certs/ > openssl req -newkey rsa:2048 -new -nodes -x509 -days 3650 -keyout key.pem -out ca.pem
   ```

   OpenSSL prompts you to supply certificate properties, including country, organization, and so on.

Results

Two files are created, `key.pem` and `ca.pem`.

- `key.pem` is the private key.
- `ca.pem` is a certificate signed by `key.pem`.

Integrating vRealize Log Insight Cloud with VMware Products and Services

vRealize Log Insight Cloud can integrate with other VMware products and services to use events and log data, and to provide better visibility into events that occur in a virtual environment.

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.

**Note** The maximum size supported for UDP syslog messages is 1024 bytes.

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 Cloud Proxy and Cloud Native Collector.

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.

<table>
<thead>
<tr>
<th>Level of Integration</th>
<th>Required Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events, tasks, and alarms collection</td>
<td>System.View</td>
</tr>
</tbody>
</table>

**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.

**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.

For the vSphere integration to function correctly, ensure that the Cloud Proxy virtual machine is set up with a host name that meets the following criteria:
- The host name is valid.
- The host name can be resolved through DNS.
- The host name is reachable from the ESXi host.

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** or **SSL** as the protocol to send logs.

**Note**

- The transmission speed with SSL is lower than TCP.
- If the protocol is SSL, ESXi hosts do not accept the log forwarder's certificates automatically. Ensure that you add the log forwarder's self-signed certificate to the ESXi host's truststore. For more information, see [Add a Log Forwarder Certificate to an ESXi Host Truststore](#).

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.

Add a Log Forwarder Certificate to an ESXi Host Truststore

While configuring an ESXi host, if you select SSL as the protocol to forward log events to vRealize Log Insight Cloud, you must add the log forwarder’s certificate to the ESXi host’s truststore. You need to add the certificate because ESXi hosts do not accept the log forwarder’s certificate automatically.

Prerequisites

Download the appropriate installer for the OpenSSL tool from https://www.openssl.org/community/binaries.html. Use the downloaded OpenSSL installer to install it on Windows.

Procedure

- Open the Command Prompt and run the following commands.

```
openssl s_client -connect <CLOUD_PROXY_IP_HOSTNAME>:1514 < /dev/null | openssl x509 -outform PEM >> /etc/vmware/ssl/castore.pem
esxcli system syslog reload
esxcli network ip connection list | grep 1514
```

Integrating vRealize Log Insight Cloud with vRealize Operations Cloud

When vRealize Log Insight Cloud is integrated with vRealize Operations Cloud, you can send logs for supported objects to vRealize Log Insight Cloud. In vRealize Operations Cloud, you can search for these logs, view the logs for an object, and launch the vRealize Log Insight Cloud service.

For more information, see Integration of vRealize Operations Cloud and vRealize Log Insight Cloud in VMware vRealize Operations Cloud Getting Started Guide.

Regional Log Support

VMware Cloud on AWS SDDCs can forward vRealize Log Insight Cloud logs to the Asia-Pacific (Sydney) and Europe (Frankfurt) regions, in addition to the US West (Oregon) region. Once applied, this configuration becomes an organization-level change and all the SDDC logs point to the new region. You can select only one vRealize Log Insight Cloud region for an organization. To enable this feature, open a service request or contact customer support.

**Note** Log regionalization is an optional process and involves an operational overhead. Request for the transition only if it is an essential requirement for your business or organization.
Prerequisites

- Before requesting for log regionalization, back up the following data. After the transition, re-import this data in the new region.
  - Alert definitions and webhooks to deliver the alerts
  - Log forwarding rules
  - Log archiving rules
  - Log processing rules (masking, filtering, and tagging logs)
  - End-point API configuration for your logs, if you are a non-VMware Cloud on AWS user
  - Access control roles and users
- Log regionalization is a permanent transfer of logs to the specified region and you lose access to any existing logs after the transition.

For example, if you request to switch the region for your vRealize Log Insight Cloud tenancy from the default region of US West (Oregon) to Asia-Pacific (Sydney) or Europe (Frankfurt), you lose access to the US West (Oregon) tenancy and any associated logs and configuration.

Optionally, if you want to save the logs from your prior tenancy, use the Forward Logs from vRealize Log Insight Cloud. Because log regionalization forwards logs as they are ingested and does not look at historical data, you must configure log forwarding in advance.

For example, Acme Inc uses VMware Cloud on AWS with an SDDC deployed in Frankfurt. Acme Inc is using the included version of vRealize Log Insight Cloud with VMware Cloud on AWS, with 7 days worth of retention, or 30 days if they are on a paid subscription. This tenancy is provisioned in US West (Oregon). If Acme Inc wants to switch the vRealize Log Insight Cloud region to Europe (Frankfurt) and they want a backup of their data, they must start forwarding or archiving the logs 7 days before requesting for log regionalization.

If you do not need the historical logs, you can raise a request for log regionalization without forwarding the logs.
After Log Regionalization

Once the log regionalization process is finished, the new regional tenancy works like a brand new vRealize Log Insight Cloud instance, and has only the logs beginning from the time of the transition. Because the transition is immediate, you do not lose any new log data and all the new logs go to the new instance, which is provided to you automatically.

**Note**

- Any vRealize Log Insight Cloud Proxies of agents managed by you and deployed from the previous instance of vRealize Log Insight Cloud are redeployed and pointed to the new instance of vRealize Log Insight Cloud in the new region. If you are collecting logs from other sources, you will experience some data loss from these log sources during the transition.

- You must accept the vRealize Log Insight Cloud trial for the new instance after the transition, for which you will receive a notification. You can accept the trial by logging in to the new vRealize Log Insight Cloud instance. Log ingestion begins after you accept the trial. The logs are retained only for one day between VMware Cloud on AWS finishing the change and you accepting the trial, so you must initiate the trial as soon as you are notified.

- The complete ETA from the time of request to request fulfillment is up to five US business days. The maximum ETA to get the new instance of vRealize Log Insight Cloud when the old instance is taken away is up to 24 hours.