Using VMware Log Intelligence

VMware Log Intelligence

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

Introduction to VMware Log Intelligence

1

Log Intelligence provides visibility across public and private cloud environments including AWS. Log Intelligence 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:

Working with Your VMware Cloud Service Account and Organization for VMware Log Intelligence

VMware Log Intelligence is a VMware Cloud service. To use it, you must have a VMware Cloud service account that is contained within an organization.

For information about organizations and service accounts, see https://docs.vmware.com/en/VMware-Cloud-services/services/Using-VMware-Cloud-Services/GUID-20D62AFF-024B-4901-976D-69BFD71BECC8.html.

Setting Up VMware Log Intelligence

Before you begin using VMware Log Intelligence, you must install a data collector and configure connections for receiving data from log and event sources.

There are two initial setup tasks.

- Download and install a data collector.

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

  For more information, see Deploy a First Data Collector for VMware Log Intelligence.

- Configure event forwarding for the data collector.

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

Deploy a First Data Collector for VMware Log Intelligence

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

Prerequisites

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

Procedure

1. Click **Add Collector** in the Event Observations widget on the VMware Log Intelligence home screen.

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

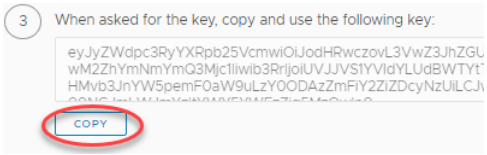
2. You can deploy a data collector locally or deploy a data collector as an Amazon Machine Image on AWS.
   - To deploy the data collector locally, click **Download OVA**.
   - To deploy the data collector with AWS, click **Deploy AMI** and following the instructions that appear.
3. Navigate to your VMware vSphere Web Client data center and click on the name of your vCenter cluster. In the drop-down menu, select **Deploy OVF Template**.
4. In the Deploy OVF Template form, perform the following actions.
   a. Click **Select template**, then **Local File**. Paste in the path to the OVA data collector 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 data collector, and click **Next**.
   c. Click **Select a resource** and the cluster where you want to run the data collector, and then click **Next**.
   d. Review the details of your data collector deployment. Notice the **Size on disk** text box. The location where you deploy the data collector in the following steps must have enough space available. Click **Next**.
   e. **Accept** the License Agreement. Click **Next**.
   f. Click **Select storage** and select a datastore from the list with enough free space for the OVA file. Click **Next**.

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

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

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

i Return to VMware Log Intelligence and collect the token key provided on the Setup a Data Collector Virtual Appliance form. Click **Copy** to copy the key. Use the **Copy** control to ensure you are copying the entire key.



Token keys are should be used within 24 hours and should be used for only one data collector.

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 data collector is installed.

5 Click the green arrow at the top of your page to run the data collector.

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

7 Return to the VMware Log Intelligence **Set Up a Data Collector Virtual Appliance** form. Wait for a success message saying a connection has been made. (This may take several minutes.)

What to do next

Deploy additional data collectors for VMware Log Intelligence

You can deploy additional data collectors for your installation.

Prerequisites

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

Procedure

1 Open the menu on the left side of the home page and select **Manage>Data Collectors** to display the Data Collectors page.

2 Click **Add New** under the Data Collectors page heading.

3 You can deploy a data collector locally or deploy a data collector as an Amazon Machine Image on AWS.

- To deploy the data collector locally, click **Download OVA**.
- To deploy the data collector with AWS, click **Deploy AMI** and following the instructions that appear.

4 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**.

5 In the Deploy OVF Template form, perform the following actions.

a Click **Select template**, then **Local File**. Paste in the path to the OVA data collector 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 data collector, and click **Next**.

c Click **Select a resource** and the cluster where you want to run the data collector, and then click **Next**.

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

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

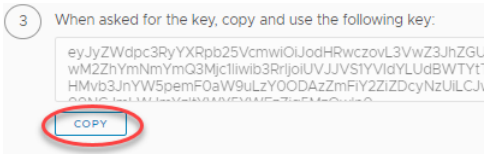
f Click **Select storage** and select a datastore from the list with enough free space for the OVA file. Click **Next**.

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

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

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

i Return to VMware Log Intelligence and collect the token key provided on the Setup a Data Collector Virtual Appliance form. Click **Copy** to copy the key. Be sure to use the **Copy** control to ensure that you are copying the entire key.



Token keys are good for 24 hours and should be used for only one data collector.

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

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

The data collector is installed.

6 Go to the vSphere Web Client and click the green arrow at the top of your page to run the data collector.

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

8 Return to the VMware Log Intelligence **Set Up a Data Collector Virtual Appliance** form. Wait for a success message saying a connection has been made. (This may take several minutes.)

What to do next

Consult Port Requirements of Remote Data Collector and then enable log and event forwarding to the data collector.

Port Requirements of Remote Data Collector

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

Port Requirements

Before you configure event forwarding, become familiar with port requirements for the data collector.

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

Recommended Syslog Agents for VMware Log Intelligence

Remote Data Collector supports any agent sending syslog RFC 3195 or RFC 5424 compliant messages.

While any agent meeting these criteria is supported, the following agents are recommended for use as a best practice for syslog:

- Rsyslog
- Syslog-ng
- NXLOG
- Fluentd

Forwarding events and logs to Log Intelligence

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

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 Recommended Syslog Agents for VMware Log Intelligence.

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

Service Roles in Log Intelligence

VMware Log Intelligence supports two service roles, Log Intelligence Administrator and Log Intelligence User.

Table 1-1. Log Intelligence Roles and Permissions

Role	Rights/Permissions
Log Intelligence Administrator	All
Log Intelligence User	Full access for the following actions: ■ Create and save queries ■ Create and modify private dashboards Read access for other information

Assigning Roles

Roles are assigned from the **Identity & Management** screen in VMware Cloud Service.

For more information about role assignment, see Add Users to Your Organization in *Using VMware Cloud*.

Fields in VMware Log Intelligence

In a large environment with numerous log events, you cannot always locate the data fields that are important to you.VMware Log Intelligence supports the creation of fields to use in queries and filters to address this concern. Fields are a powerful way to add structure to unstructured events and allow the manipulation of both the textual and visual representation of data.

Fields are a type of regular expression query useful for complex pattern matching. With fields, you can construct queries or build filters without needing to know, remember, or learn complicated regular expressions.

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

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

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

Table 1-2. Types of fields in VMware Log Intelligence

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

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

Create an extracted field

You can manually create an extracted field.

Procedure

1 Go to the **Explore Logs** page.

2 On the **Stream** tab, click the three dots icon to the left of any log message.

The **Add Filter** menu appears.

3 Click **Extract Field** on the **Add Filter** menu.

The **Create Custom Field** form appears.

4 Fill in values for the field.

5 Click **Save**.

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 if you have admin permissions.

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, VMware Log Intelligence 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.

Procedure

1. Click the Explore Logs icon on the left-hand menu to go to the Explore Logs page
2. Click the menu icon on the right side in the Fields list to open the Fields page. The Fields page lists all VMware Log Intelligence fields organizing them into two groups, those found in queries and those found in other fields.
3. Locate the field you want to clone. You can use the **Filter** field to search.
4. Left-click the three dots icon on the field's card and click **Clone**.

   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.
5. (Optional) Modify the Extracted value regular expression in the Fields pane.
6. (Optional) Modify the Pre and post context regular expressions in the Fields pane.
7. Modify any other fields as needed.
8. Click **Clone** to create the new field.

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.

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

Procedure

1. Click the Explore Logs icon on the left-hand menu to go to the Explore Logs page
2. Click the menu icon on the right side in the Fields list to open the Fields page.
3. Locate the field you want to modify.
4. Left-click the three dots icon on the fields card and click **Edit** on the drop-down menu.
5. Modify the values as needed.

6 Click **Save**.

Delete a field

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

Prerequisites

You must have administrator permissions to delete an extracted field.

Procedure

1 Click the Explore Logs icon on the left-hand menu to go to the **Explore Logs** page

2 Click the menu icon on the right side in the Fields list to open the **Fields** page.

3 Locate the field you want to delete.

4 Left-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.

5 Click **Delete** in the confirmation pop-up to finish the deletion.

Forward log events from Log Intelligence to other endpoints

2

You can configure the Log Intelligence service to forward incoming events to vRealize Log Insight, Splunk, or another destination.

For example, you might want to send all logs to VMware Log Intelligence and then have Log Intelligence 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 VMware Log Intelligence .

Prerequisites

To ensure that no events are dropped, verify that the destination can handle the number of events that are forwarded.

Procedure

1 Click the Manage menu on the main menu on the left of the screen.

2 Click **Log Forwarding** to open the Log Forwarding page.

3 Click **New Configuration**.

4 Provide the following information:

Name	Description
Name	A display name for this log forwarding configuration.
Data Collector	The data collector from which you want to forward messages. Select a data collector from the drop-down menu.
Endpoint Type	The endpoint to which messages are forwarded. Select one of the following items on the drop-down menu. ■ Default ■ vRealize Log Insight ■ Splunk
Endpoint URL	The URL for the destination endpoint.
Tags (optional)	A tag name and predefined value. Tags permit you to more easily query events. You can add multiple comma-separated tags.

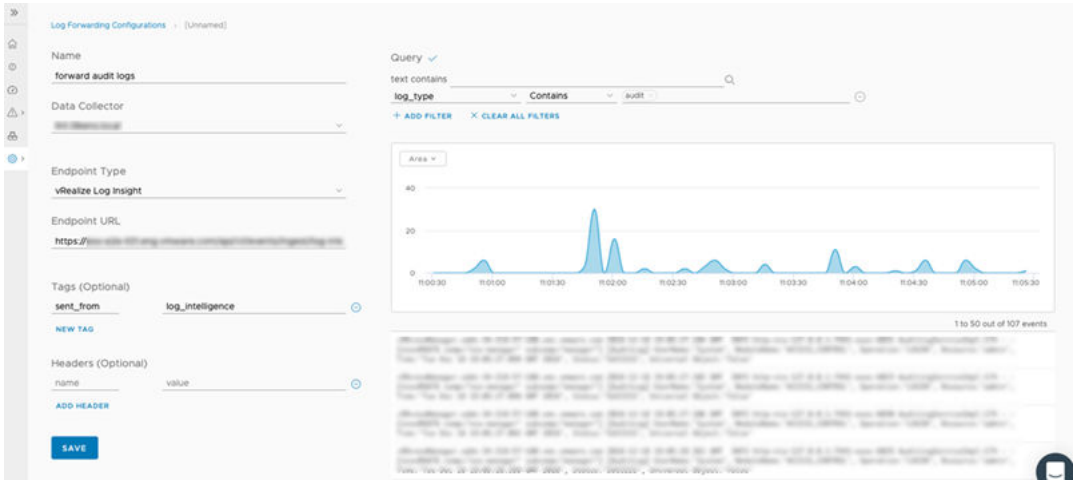
Name	Description
Headers (optional)	Authorization information for the destination end-point.
Query	Filters messages to send only those that contain the text you specify. At least one filter is required. Click the pen icon to display the query form. Multiple filters are supported.

5 Click the magnifying glass icon to preview the filtered results, which are displayed in the graph and list of events on the **Log Forwarding Configurations** page.

6 Click **Save**.

Example: Example

The following example illustrates a log forwarding configuration for audit logs, filtering and directing them to an instance of vRealize Log Insight.



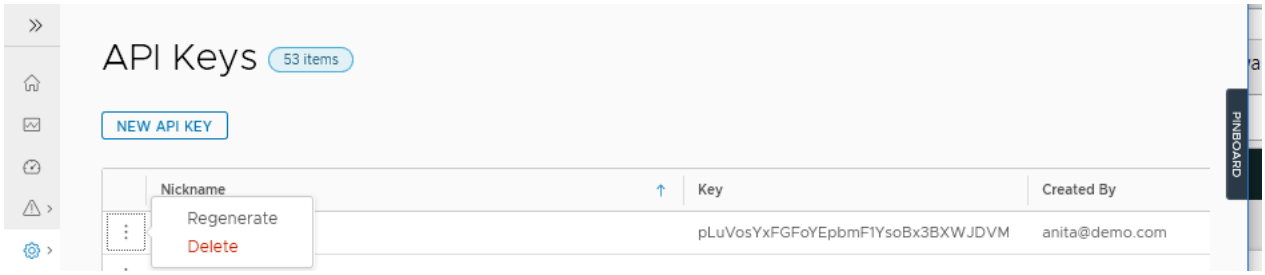
API keys

3

VMware Log Intelligence uses API keys to ensure the security of logs ingested by the VMware Log Intelligence cloud proxy server.

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

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



Specifying an API Key for a Log Source

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

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

This chapter includes the following topics:

- Create an API key for VMware Log Intelligence
- Regenerate an API key for VMware Log Intelligence

- Delete an API Key for VMware Log Intelligence

Create an API key for VMware Log Intelligence

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. Select **Home>Manage>API Keys>New API Key** to display the New API Key window.
2. Enter a name for the key.

   Names cannot contain spaces and must be unique.
3. 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.
4. Optionally, click **Copy Key** to save the key value for easy reuse.
5. Click **Close**.

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 for VMware Log Intelligence

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, Log Intelligence 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. Select **Home>Manage>API Keys** to open the **API Keys** window.
2. 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.
3. 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 for VMware Log Intelligence

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. Select **Home > Manage > API Keys** to open the **API Keys** window.
2. 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.
3. Click **Delete**.

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