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:

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**.

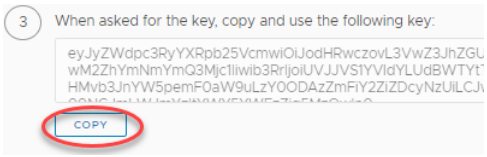
   f. Click **Select storage** and select a datastore from the list with enough free space for the OVA file. Click **Next**.

   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. Be sure to use the **Copy** control to ensure you are copying the entire key.



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.) When the connection has been made successfully, the **Next** button at the bottom of the screen becomes active.

8 Click **Next** to go to the **Configure Log Forwarding** page.

What to do next

Enable log and event forwarding to the data collector. See Port Requirements of Remote Data Collector.

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 specifying 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 on 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**.

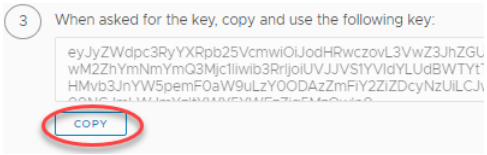
f Click **Select storage** and select a datastore from the list with enough free space for the OVA file. Click **Next**.

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 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 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.) When the connection has been made successfully, the **Next** button at the bottom of the screen becomes active.

9 Click **Next** to go to the **Configure Log Forwarding** page.

What to do next

Enable log and event forwarding to the data collector. See Port Requirements of Remote 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

Setting Up Event and Log Forwarding

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

Use the links in the following table to find information about setting up event and log forwarding from your source.

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

Extracted Fields

In a large environment with numerous log events, you cannot always locate the data fields that are important to you. VMware Log Intelligence provides runtime field extraction to address this problem.

You can also create custom extracted fields dynamically. You identify these fields with regular expressions.

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

You can use extracted fields to search and filter log events.

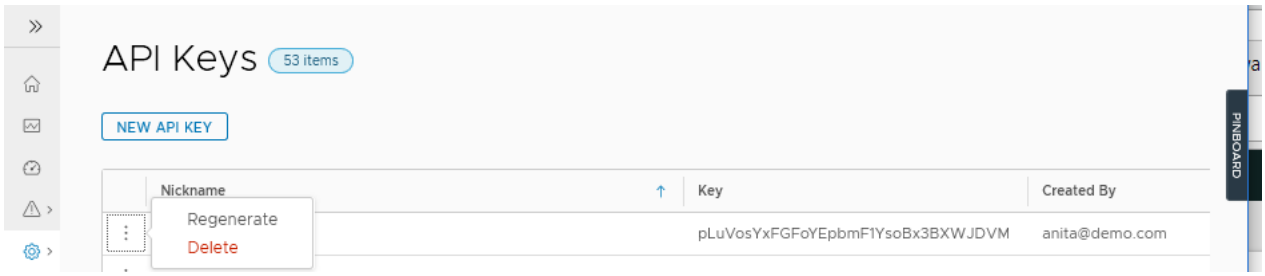
Extracted fields are shown in the Fields section of the Log Explorer window.

API Keys

VMware Log Intelligence uses API keys to ensure the security of logs ingested by the VMware Log Intelligence data collector.

Keys are generated and applied for you except for logs that you send to 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"
   }]'
```

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.