VMware vCenter Log Insight Installation and Administration Guide

vCenter Log Insight 1.0

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

EN-001130-00

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

VMware vCenter Log Insight Installation and Administration Guide

The *VMware vCenter Log Insight Installation and Administration Guide* provides information about installing, configuring, and administering VMware® vCenter™ Log Insight™, including how to deploy and configure the Log Insight vApp to receive log messages from other applications, how to import log files, how to modify the log storage policy, and how to switch log archiving on and off.

To help you set up your environment so that Log Insight can receive logs from ESXi hosts or vCenter Server vApp, this guide contains a section on how to configure forwarding of log messages to Log Insight.

Intended Audience

This information is intended for anyone who wants to install, configure, or maintain Log Insight. The information is written for experienced Linux system administrators who are familiar with virtual machine technology and datacenter operations.

1 Installing Log Insight

Log Insight is delivered as a vApp that you must deploy in your environment.

To deploy the Log Insight vApp, follow the standard OVF deployment procedure.

This chapter includes the following topics:

Security Requirements

To ensure that your virtual environment is protected from external attacks, you must ensure that you observe certain rules.

- Always install Log Insight in a trusted network.
- Always save Log Insight support bundles in a secure location.

IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of Log Insight must visit the VMware vCenter Log Insight documentation page and search for the latest version of the *VMware vCenter Log Insight Security Guide*.

The Security Guide contains concise reference to the security features of Log Insight. Topics include the product external interfaces, ports, authentication mechanisms, and options for configuration and management of security features.

For more details about securing your virtual environment, refer to the *VMware vSphere Security Guide* and to the Security Center on the VMware Web site.

Supported Log Files and Archive Formats in Log Insight

You can use Log Insight to analyse historic data from imported log files.

In Log Insight 1.0, you can import only log files that were archived by Log Insight.

NOTE Although Log Insight can handle historic data and real-time data simultaneously, you are advised to deploy a separate instance of Log Insight to process imported log files.

Product Compatibility

Log Insight can collect data by using syslog or vSphere API, and can integrate with vCenter Operations Manager to send notification events and enable Launch in Context . Check the *VMware vCenter Log Insight Release Notes* for latest updates on supported product versions.

Syslog Feeds

Log Insight collects and analyses syslog data from arbitrary logs, and from the following VMware components.

- ESXi 4.1, 5.0, and 5.1
- vCenter Server Appliance 5.1

NOTE Earlier ESXi versions and other products might work, but have not been tested. The content specific to vSphere might be unreliable for earlier versions of ESXi.

The vSphere support includes pre-constructed queries and field definitions.

You must configure the ESXi host or the vCenter Server Appliance to push their syslog feeds to Log Insight. See "Forwarding vSphere Log Files to Log Insight," on page 19.

vSphere API

You can configure Log Insight to pull data for tasks, events, and alarms that occurred in your virtual environment. Log Insight uses the vSphere API to connect to vCenter Server 5.1.x systems.

You can configure Log Insight to pull data from one or more vCenter Server systems. See the topic *Connect Log Insight to vCenter Server 5.1.x Systems* in the in-product help.

vCenter Operations Manager Integration

Log Insight and vCenter Operations Manager vApp or Installable can be integrated in two independent ways.

- Log Insight can send notification events to vCenter Operations Manager.
- The launch in context menu of vCenter Operations Manager can display actions related to Log Insight.

The following table contains the versions of vCenter Operations Manager that support notifications and launch in context.

Product Deliverable	Notification Events	Launch in Context
vCenter Operations Manager vApp	5.6, 5.7, and 5.7.1	5.7.1
vCenter Operations Manager Installable	5.6, 5.7, and 5.7.1	5.7.1

Deploy the Log Insight vApp

Download and deploy the Log Insight virtual appliance by using the vSphere Client . VMware distributes the Log Insight virtual appliance as a `.ova` file.

Prerequisites

- Verify that you have permissions to deploy OVF templates to the inventory.

- Verify that your environment has enough resources to accommodate the minimum requirements of the Log Insight virtual appliance. See GUID-4E3853AA-EFBF-4004-B182-DF5F6DC3826F#GUID-4E3853AA-EFBF-4004-B182-DF5F6DC3826F.

Procedure

1 In the vSphere Client, select **File > Deploy OVF Template**.

2 Follow the prompts in the Deploy OVF Template wizard.

3 On the Disk Format page, select a disk format.

- **Thick Provision Lazy Zeroed** creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. The data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time, on first write from the virtual appliance.
- **Thick Provision Eager Zeroed** creates a type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. it might take much longer to create disks in this format than to create other types of disks.

  Deploy the Log Insight virtual appliance with thick provisioned eager zeroed disks whenever possible for better performance and operation of the virtual appliance.
- **Thin Provision** creates a disk in thin format. The disk grows as the data saved on it grows. If your storage device does not support thick provisioning disks or you want to conserve unused disk space on the Log Insight virtual appliance, deploy the virtual appliance with thin provisioned disks.

NOTE Shrinking disks on the Log Insight virtual appliance is not supported and might result in data corruption or data loss.

4 (Optional) On the Properties page, set the networking parameters for the Log Insight virtual appliance.

If you do not provide network settings, such as IP address, DNS servers, and gateway, Log Insight utilizes DHCP to set those settings.

CAUTION Do not specify more than two domain name servers. If you specify more than two domain name servers, all configured domain name servers are ignored in the Log Insight virtual appliance.

5 Follow the prompts to complete the deployment.

For information on deploying virtual appliances, see the *User's Guide to Deploying vApps and Virtual Appliances*.

After you power on the virtual appliance, an initialization process begins. The initialization process might take up to 10 minutes. At the end of the process, the virtual appliance restarts.

What to do next

Log in to the Log Insight Web interface to verify that the application is installed properly, and apply the initial configuration.

The Log Insight Web interface is available at http://*log_insight-host*/. The HTTPS-based secure Web interface is available at https://*log_insight-host*/ where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Configure Log Insight

When you access the Log Insight Web interface for the first time after the virtual appliance deployment, you must complete the initial configuration steps.

All settings that you modify during the initial configuration are also available in the Administration Web interface. You can change any setting at a later stage.

Prerequisites

- In the vSphere Client, check the IP address of the Log Insight virtual appliance.
- For information about the trace data that Log Insight might collect and send to VMware if you choose to participate in the Customer Experience Improvement Program, see Chapter 4, "The Customer Experience Improvement Program," on page 29.

Procedure

1 Use a supported browser to navigate to the Web user interface of Log Insight.

   The URL format is https:// *log_insight-host*/, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

   The initial configuration wizard opens.

2 Set the email and password for the admin user, and click **Save and Continue**.

3 Type the license key, click **Set Key**, and click **Continue**.

   You obtain an evaluation license key when you download the Log Insight installation package.

4 On the General Configuration page, type the email address to receive system notifications from Log Insight.

5 If you want to participate in the Customer Experience Improvement Program, select **Send weekly Trace Data to VMware as part of the Customer Experience Improvement Program**.

6 Click **Save and Continue**.

7 On the Time Configuration page, set how time is synchronized on the Log Insight virtual appliance and click **Test**.

   Synchronize time with a list of public NTP servers. If an external NTP server is not accessible due to firewall settings, you can use the internal NTP server of your organization. If no NTP servers are available, you can sync the time with the ESXi host where you deployed the Log Insight virtual appliance.

8 Click **Save and Continue**.

9 (Optional) Specify the properties of an SMTP server to enable outgoing alert and system notification emails.

10 Click **Save and Continue**.

11 (Optional) Configure the integration between Log Insight and other VMware applications.

   a To allow Log Insight pull events data from a vCenter Server, specify the IP address and user credentials for the vCenter Server system, and click **Test** to verify the connection.

   b To allow Log Insight to send alert notifications triggered by your custom rules, specify the IP address and user credentials for the vCenter Operations Manager vApp, and click **Test** to verify the connection.

   c To allow Log Insight to start from the Custom user interface of vCenter Operations Manager, click **Enable Launch in Context**.

      This operation might take a few minutes.

12 Click **Save and Continue**.

13 (Optional) To archive outdated log data to an NFS location, select **Enable Data Archiving**, type the path to the storage location, and click **Test** to verify that Log Insight can connect to that storage.

14 Click **Save and Continue**.

15 Click **Restart** to complete the initial setup of Log Insight.

After the virtual appliance restarts, the Web user interface of Log Insight opens .

What to do next

Work with Log Insight to import log files and content packs, query log messages, set up alert notifications, and more.

Assign a Permanent License to Log Insight

You can use Log Insight only with a valid license key.

You obtain an evaluation license when you download Log Insight from the VMware Web site. This license is valid for 60 days. When the evaluation license expires, you must assign a permanent license to continue using Log Insight.

You use the Administration section of the Log Insight Web user interface to check the Log Insight licensing status and manage your license.

Prerequisites

- Verify that you obtained a valid license key from My VMware™.
- Verify that you are logged in to the Log Insight Web user interface as an administrator. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 From the configuration drop-down menu, select **Administration**.

2 Under Management, select **License**.

3 In the **License Key** text box, type your license key and click **Update**.

4 Verify that the license status is Active, and the license type and expiry day are correct.

Install the Log Insight Adapter in vCenter Operations Manager Standalone

You install the Log Insight adapter in vCenter Operations Manager standalone to enable the launch in context functionality .

The Log Insight adapter provides the necessary information for vCenter Operations Manager to launch Log Insight. This adapter does not collect data.

The Log Insight adapter is installed as part of the vCenter Operations Manager 5.7.1 vApp, but not installed as part of the standalone version of vCenter Operations Manager. Therefore, in the standalone version, you must install the Log Insight adapter manually .

VMware distributes the Log Insight adapter as a `.tgz` archive that contains the installation utilities for both Windows and Linux.

Prerequisites

- Download the adapter installation TGZ file anonymously from ftp://ftp.integrien.com/.
- Make a note of the build number in the TGZ file name. The build number appears after the adapter name, for example, *`adaptername-buildnumber`*`.tgz`.
- Verify that you have access to the server where vCenter Operations Manager runs, and that you have permissions to install software on the server.
- Verify that the version of vCenter Operations Manager is 5.7.1 or later.
- Verify that you know the IP address or domain name of the target vCenter Operations Manager instance.
- Verify that you have administrator user credentials for vCenter Operations Manager.

Procedure

1. Open the TGZ file and extract the TAR file to a temporary folder on your vCenter Operations Manager server.
2. In the temporary folder, open the TAR file and extract and run the installer for your operating system platform.
3. Log in to the Custom user interface as an administrator.
4. Select **Admin > Support**.
5. On the **Info** tab, find the Adapters Info pane and click the **Describe** icon ( ).

   The **Describe** icon is located at the top right of the Adapters Info pane.
6. Click **Yes** to start the describe process and click **OK**.

   The Custom user interface finds the adapter files, gathers information about the abilities of the adapter, and updates the user interface with information about the adapter. If you have remote collectors, it installs the adapter on the remote collectors.

   The describe process might take several minutes. When the describe process is finished, the adapter appears in the Adapters Info pane. The build number is in the Adapter Version column.
7. Verify that the build number in the Adapter Version column for the adapter matches the build number in the TGZ file that you downloaded.

What to do next

After you install the adapter, you must enable launch in context from the Administration Web user interface of Log Insight. See the Log Insight help topic *Enable Launch in Context for Log Insight in vCenter Operations Manager*.

Administering Log Insight 2

Administrator users can accomplish standard administration tasks by using the Administration section of the Log Insight Web user interface .

The standard administration options are documented in the Log Insight in-product help .

Advanced Linux users with administrator credentials can apply changes to the configuration through SSH connection or through the console of the Log Insight virtual appliance. The advanced configuration options are documented in *Log Insight Installation and Administration Guide*.

NOTE You can apply configuration changes through SSH or the virtual appliance console only after VMware Support Services authorize them.

Changes to the configuration of Log Insight are applied only after you restart the Log Insight service.

This chapter includes the following topics:

Configure the Root SSH Password for the Log Insight Virtual Appliance

Most advanced administration tasks require that you establish an SSH connection to the Log Insight virtual appliance.

By default the SSH connection to the virtual appliance is disabled. To enable SSH connections, you must configure the root SSH password from the VMware Remote Console

Prerequisites

Verify that the Log Insight virtual appliance is deployed and running.

Procedure

1 In the vSphere Client inventory, click the Log Insight virtual appliance, and open the Console tab.

2 In the console, type **root**, leave the password empty, and press Enter twice.

The following message is displayed in the console: `Password change requested. Choose a new password.`

3 Leave the Old password empty and press Enter.

4 Type the new password for the root user, press Enter, and type the new password again.

The password must consist of 8 characters, and must include at least one upper case letter, one lower case letter, one digit, and one special character.

NOTE You cannot repeat the same character more than 4 times.

The following message is displayed: `Password changed.`

What to do next

You can use the root password to establish SSH connections to the Log Insight virtual appliance.

NOTE SSH operations must be authorized by VMware Support Services.

Log Storage Policy

By default, the Log Insight vApp uses a constant storage policy. Log Insight uses a total of 140GB of persistent storage for all incoming logs.

When the volume of logs imported into Log Insight reaches the 140GB limit, old log messages are automatically and periodically retired on a first-come first-retired basis. 40GB of storage space is enough to store the logs from the last 48 hours at an incoming log volume of approximately 1GB per hour.

NOTE While generally 140GB of persistent storage maps roughly to 140GB of raw incoming log volume, the ratio is not generalizable. It depends on the variety of log messages that are imported into Log Insight.

Data stored by Log Insight is immutable. After a log has been imported, it can not be removed until it is automatically retired.

Because the Log Insight index remains at a constant size, the oldest messages get removed from the searchable index. To preserve old messages, you can enable the archiving feature of Log Insight.

Increase the Storage Capacity of the Log Insight Virtual Appliance

You can increase the storage resources allocated to Log Insight as your needs grow.

You increase the storage space by adding a new virtual disk to the Log Insight virtual appliance. You can add as many disks as you need, and as your environment permits.

Prerequisites

Verify that you are logged in the vSphere Client and that you have privileges to modify the hardware of virtual machines in your environment.

Verify that the Log Insight virtual appliance is safely shut down. See "Power Off the Log Insight vApp," on page 19.

Procedure

1 In the vSphere Client inventory, right-click the Log Insight virtual machine and select **Edit Settings**.

2 Click the **Hardware** tab and click **Add**.

3 Select **Hard Disk** and click **Next**.

4 Select **Create a new virtual disk** and click **Next**.

   a Type the disk capacity.

   b Select a disk format.

   - **Thick Provision Lazy Zeroed** creates a virtual disk in the default thick format. Space required for the virtual disk is allocated when the virtual disk is created. The data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time, on first write from the virtual appliance.
   - **Thick Provision Eager Zeroed** creates a type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. it might take much longer to create disks in this format than to create other types of disks.

     Create thick provisioned eager zeroed disks whenever possible for better performance and operation of the Log Insight virtual appliance.
   - **Thin Provision** creates a disk in thin format. Use this format to save storage space.

   NOTE Snapshots can negatively affect the performance of a virtual machine. Do not use snapshots whenever possible.

   c (Optional) To select a datastore, browse for the datastore location and click **Next**.

5 Accept the default virtual device node and click **Next**.

6 Review the information and click **Finish**.

7 Click **OK** to save your changes and close the dialog box.

When you power on the Log Insight virtual appliance, the virtual machine discovers the new virtual disk and automatically adds it to the built-in 140GB data volume.

CAUTION After you add a disk to the virtual appliance, you cannot remove it safely. Removing disks from the Log Insight virtual appliance results in complete data loss.

Enable Data Archiving in Log Insight

Data archiving allows Log Insight to preserve old logs that would have rotated out of the index.

Data archiving is disabled by default. You enable data archiving by selecting the NFS partition where old logs will be saved.

NOTE Log Insight does not verify the availability of storage space in the location that you specify.

Prerequisites

- Verify that TCP port 22 is open to enable SSH connections.
- Verify that you have the root user credentials to log in to the Log Insight virtual appliance.
- Verify that you have access to an NFS partition that meets the following requirements
  - The NFS partition must allow reading and writing operations for guest accounts.
  - The mount must not require authentication.

- The NFS server must support NFS v3.

Procedure

1 Establish an SSH connection to the Log Insight virtual appliance and log in as the root user.

2 Open the `/usr/lib/loginsight/application/etc/loginsight-config-base.xml` file for editing.

3 Locate the `archive-directory` string and specify a valid value.

```
<repository>
<archive-directory value="" />
</repository>
```

For example, you can specify `/mnt/archive/`.

4 Save and exit the editing mode.

5 To restart the Log Insight service, run `service loginsight restart`.

NOTE Restarting the Log Insight service interrupts the log processing for a short period.

6 Close the SSH connection.

You enabled the archiving of logs in Log Insight.

What to do next

Because Log Insight does not verify the availability of storage space in the archiving location, you must ensure to remove old data as needed.

NOTE Archived logs are preserved, but not searchable. If you want to search archived logs, you must import them back into Log Insight.

Disable Data Archiving in Log Insight

You can stop data archiving to save storage space on the Log Insight virtual appliance.

By default, data archiving is disabled. If you modified the Log Insight configuration to enable archiving, but no longer need it, you can disable data archiving by deleting the archiving directory from the configuration file.

Prerequisites

- Verify that TCP port 22 is open to enable SSH connections.
- Verify that you have the root user credentials to log in to the Log Insight virtual appliance.

Procedure

1 Establish an SSH connection to the Log Insight virtual appliance and log in as the root user.

2 Open the `/usr/lib/loginsight/application/etc/loginsight-config-base.xml` file for editing.

3 Locate the `archive-directory` string and clear the value within the quotes.

The modified string should be as follows.

```
<archive-directory value="" />
```

4 Save and exit the editing mode.

5 To restart the Log Insight service, run `service loginsight restart`.

NOTE Restarting the Log Insight service interrupts the log processing for a short period.

6 Close the SSH connection.

Power Off the Log Insight vApp

To avoid data loss when powering off Log Insight, the virtual appliance must be powered off by strictly following the sequence of steps.

You must power off the Log Insight virtual appliance before making changes to the virtual hardware of the appliance.

You can power off the Log Insight vApp by using the **Power > Shut Down Guest** command in the vSphere Client, or by establishing an SSH connection to the Log Insight virtual appliance.

Prerequisites

- Verify that TCP port 22 is open to enable SSH connections.
- Verify that you have the root user credentials to log in to the Log Insight virtual appliance.

Procedure

1 Establish an SSH connection to the Log Insight virtual appliance and log in as the root user.

2 To power off the Log Insight virtual appliance, run `shutdown –h now`.

What to do next

You can safely modify the virtual hardware of the Log Insight virtual appliance.

Log Insight as a Syslog Server

Log Insight includes a built-in syslog server that is constantly active when the Log Insight service is running.

The syslog server listens on ports 514/TCP, 1514/TCP, and 514/UDP, and is ready to ingest log messages that are sent from other hosts. Messages that are ingested by the syslog server become searchable in the Log Insight Web user interface almost in real-time.

Forwarding vSphere Log Files to Log Insight

You can forward log events from ESXi hosts or vCenter Server Appliance to Log Insight for analysis.

Configure an ESXi Hypervisor to Forward Log Files to Log Insight

You can configure an ESXi host to in several ways forward log events to Log Insight.

Use the configure-esxi Script

The `configure–esxi` script is included in the Log Insight virtual appliance.

The `configure–esxi` script configures all ESXi hosts of version 4.x and later that are connected to a vCenter Server to send their logs to Log Insight.

NOTE User names and passwords in the scripts must be surrounded in single quotes.

If your user name or password contains one or more single quotes, you must escape them in the scripts. For example, if your password is ben's pa$$word, in the script you must type `'ben\'s pa$$word'`.

You must adapt the task to your environment.

Prerequisites

- Verify that you know the credentials for the vCenter Server.
- Verify that you know the host name or IP address of the vCenter Server.
- Verify that you know the host name or IP address of the Log Insight vApp.
- Verify that the ports required for communication between the ESXi host and the Log Insight virtual appliance are open through the firewalls and switches on your network.
- Verify that you have established an SSH connection to the Log Insight virtual appliance and you are logged in as the root user.

Procedure

1 Configure all ESXi 5.x hosts nondestructively to send their logs to myloginsight.mydomain.com.

```
configure-esxi --username 'my-vc-user' --server myvc.mydomain.com --target
udp://loginsight.mydomain.com:port
```

Existing remote logging configurations are preserved, so logs are sent to multiple locations.

NOTE With this example, ESXi 4.x hosts are configured only if they do not already have a remote syslog target.

2 Configure all ESXi 5.x and ESXi 4.x hosts to send their logs.

```
configure-esxi --username 'my-vc-user' --server myvc.mydomain.com --target
udp://loginsight.mydomain.com:port -f
```

Because ESXi 4.x does not support sending logs to multiple targets, this command overwrites any existing settings for 4.x servers.

3 Reload syslog on all ESXi hosts.

```
configure-esxi --username 'my-vc-user' --server myvc.mydomain.com -r
```

If you are running certain versions of ESXi 5.x, you must reload syslog each time the destination syslog server restarts.

4 Query the current remote syslog configurations on all ESXi 4.x and 5.x hosts attached to a vCenter Server.

```
configure-esxi --username 'my-vc-user' --server myvc.mydomain.com -q
```

5 (Optional) Remove a specific syslog target from the list of remote syslog targets.

```
configure-esxi --username 'my-vc-user' --server myvc.mydomain.com --remove
udp://loginsight.mydomain.com:port
```

You can run this command to undo any previous settings that you applied, or remove existing targets that are no longer valid.

What to do next

For complete information about using the `configure-esxi` script, establish and SSH connection to the Log Insight vApp and run `configure-esxi --help`.

Configure Syslog Manually

Instead of using the `configure-esxi` utility to forward logs to Log Insight, you can set up syslog manually.

You can run the `esxcli` command in the console of an ESXi host, in the vSphere CLI, or in the vSphere Management Assistant.

Prerequisites

- If you want to configure an ESXi host version 5.x, read and understand the information in the VMware Knowledge Base article Configuring syslog on ESXi 5.x (KB 2003322).
- If you want to configure an ESXi host version 3.5 or 4.x, read and understand the information in the VMware Knowledge Base article Enabling syslog on ESXi 3.5 and 4.x (KB 1016621).

Procedure

1 Open an ESXi Shell console session where the `esxcli` command is available.

For example, you can use vMA or open the session directly on the ESXi host.

2 To view the existing configuration options on the host, run the following command.

```
esxcli system syslog config get
```

3 To set a new host configuration, specify the options to change by running the following command.

```
esxcli system syslog config set --loghost=tcp|udp://log_insight-host:514
```

NOTE You must use `udp` or `tcp`, but not both.

For example, the following command configures remote syslog using `udp` on port 514.

```
esxcli system syslog config set --loghost=udp://10.11.12.13:514
```

To configure your ESXi host to forward logs to multiple endpoints, you can list the endpoints, separated by commas, in the command.

```
esxcli system syslog config set --loghost=udp://10.11.12.13:514,tcp://192.168.100.101:514
```

4 To ensure that the ESXi firewall is configured to allow syslog traffic to leave the host, run the following commands.

```
esxcli network firewall ruleset set --ruleset-id=syslog --enabled=true
esxcli network firewall refresh
```

5 Load the new configuration by running the `esxcli system syslog reload` command.

NOTE If you do not run this command, the configuration change does not take effect.

Use the vSphere Web Client to Configure Syslog

You can use the vSphere Web Client to configure syslog on an ESXi host to forward log messages to Log Insight.

To forward log messages from multiple ESXi hosts within the vCenter Server to Log Insight, you must configure each ESXi host.

Prerequisites

- Verify that you have privileges to modify the settings of ESXi hosts on the vCenter Server.
- Verify that you are logged in the vCenter Server that manages the ESXi host that you want to configure.

Procedure

1 From the object navigator, select the ESXi host that you want to configure, and click the **Manage** tab.

2 On the **Settings** tab, click **Advanced Settings**.

3 Click **Edit** and locate the Syslog.global.logHost property .

4 Modify the Syslog.global.logHost property to point to the Log Insight IP address or host name.

The format is `tcp|udp|ssl://log_insight-host:514|1514`, where *log_insight-host* is the IP address or host name of the Log Insight vApp.

NOTE You must use `tcp` or `udp`, but not both. Use port 514 for udp and tcp communication, and port 1514 for ssl protocol.

5 Open an ESXi Shell console session where the `esxcli` command is available.

For example, you can use vMA or open the session directly on the ESXi host.

6 To ensure that the ESXi firewall is configured to allow syslog traffic to leave the host, run the following commands.

```
esxcli network firewall ruleset set --ruleset-id=syslog --enabled=true
esxcli network firewall refresh
```

7 Load the new configuration by running the `esxcli system syslog reload` command.

NOTE If you do not run this command, the configuration change does not take effect.

Configure a vCenter Server Appliance to Forward Log Files to Log Insight

You can configure a vCenter Server Appliance to send log messages to Log Insight trough syslog.

Prerequisites

- Verify that you have the root user credentials to log in to the vCenter Server Appliance.
- Verify that TCP port 22 is open to enable SSH connections.

Procedure

1 Establish an SSH connection to the vCenter Server Appliance host and log in as the root user.

2 Navigate to `/etc/syslog-ng/`.

3 Open the `syslog-ng.conf` file for editing and add the following text at the end of the file.

```
source vpxd {
file("/var/log/vmware/vpx/vpxd.log" follow_freq(1) flags(no-parse));
file("/var/log/vmware/vpx/vpxd-alert.log" follow_freq(1) flags(no-parse));
file("/var/log/vmware/vpx/vws.log" follow_freq(1) flags(no-parse));
file("/var/log/vmware/vpx/vmware-vpxd.log" follow_freq(1) flags(no-parse));
file("/var/log/vmware/vpx/inventoryservice/ds.log" follow_freq(1) flags(no-parse));
};
destination loginsight { udp("<loginsight-host>"); };
log { source(vpxd); destination(loginsight); };
```

NOTE You can use `tcp` instead of `udp`.

4 Run `service syslog restart` to load the new configuration.

Import a Log File or Directory in Log Insight

You can use the command line to import old logs that have been archived in Log Insight.

NOTE Although Log Insight can handle historic data and real-time data simultaneously, you are advised to deploy a separate instance of Log Insight to process imported log files.

By default, Log Insight imports directories that contain archived log files. The log_importer utility provides additional options that you can use to filter which files are imported.

Prerequisites

- Verify that you have the root user credentials to log in to the Log Insight virtual appliance.
- Verify that you have access to the FTP server where Log Insight logs are archived.

Procedure

1 Establish an SSH connection to the Log Insight virtual appliance and log in as the root user.

2 Mount the shared folder on the NFS server where the archived data resides.

3 To import a directory of archived Log Insight logs, run the following command.

```
/usr/lib/loginsight/application/bin/loginsight repository import Path-To-Archived-Log-Data-Folder.
```

NOTE Re-importing archived data can take log time, depending on the size of the imported folder.

4 (Optional) To view all options that the log_importer utility supports, run the following command.

```
/usr/lib/loginsight/application/bin/loginsight repository import --help
```

You can use the optional commands to filter the files to import, add fields to imported log messages, and select the parser to use when importing log messages in Log Insight.

5 Close the SSH connection.

6 Log in to the Log Insight Web user interface.

The Log Insight Web interface is available at http://*log_insight-host*/. The HTTPS-based secure Web interface is available at https://*log_insight-host*/ where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

7 Verify that the imported log events appear as expected.

What to do next

You can search, filter, and analyze the imported log events.

Install a Custom SSL Certificate for Log Insight

By default, Log Insight installs a self-signed SSL certificate on the vApp.

The self-signed certificate generates security warnings when you connect to the Log Insight Web user interface. If you do not want to use a self-signed security certificate, you can install a custom SSL certificate. The use of a custom SSL certificate is optional and does not affect the features of Log Insight.

NOTE Log Insight uses the same certificate to receive syslog and SSL messages.

Prerequisites

- Verify that your custom SSL certificate meets the following requirements.
  - The certificate file contains both a valid private key and a valid certificate chain.
  - The private key is generated by the RSA or the DSA algorithm.
  - The private key is not encrypted by a pass phrase.
  - If the certificate is signed by a chain of other certificates, all other certificates are included in the certificate file that you plan to import.

  - All the certificates and the private key that are included in the certificate file are PEM-encoded. Log Insight does not support DER-encoded certificates and private keys.
  - All the certificates and the private key that are included in the certificate file are in the PEM format. Log Insight does not support certificates in the PFX, PKCS12, PKCS7, or other formats.
- Verify that TCP port 22 is open to enable SSH connections.
- Verify that you have the root user credentials to log in to the Log Insight virtual appliance.
- Verify that you are logged in to the Log Insight Web user interface as an administrator. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 Establish an SSH connection to the Log Insight virtual appliance and log in as the root user.

2 Copy the custom SSL certificate to the `/usr/lib/loginsight/etc/` folder.

The file extension of the certificate file that you want to import does not matter. However, the certificate must contain both a valid private key and a valid certificate chain.

3 To restart the Log Insight service, run `service loginsight restart`.

NOTE Restarting the Log Insight service interrupts the log processing for a short period.

The custom certificate replaces the default self-signed certificate that Log Insight has installed.

Disable the Web Authentication for Log Insight

You can configure the Log Insight virtual appliance to disable the Web authentication.

NOTE Disabling the Web authentication results in serious security risks. Do not disable Web authentication unless advised by VMware Support Services.

Prerequisites

- Verify that TCP port 22 is open to enable SSH connections.
- Verify that you have the root user credentials to log in to the Log Insight virtual appliance.

Procedure

1 Establish an SSH connection to the Log Insight virtual appliance and log in as the root user.

2 Open the `/usr/lib/loginsight/application/etc/loginsight-config-base.xml` file for editing.

3 Locate the `webui-authentication` string and modify the value to **`none`**.

By default, the Web authentication is set to **`full`**.

```
<authentication>
<webui-authentication type="full" />
</authentication>
```

4 Save and exit the editing mode.

5 To restart the Log Insight service, run `service loginsight restart`.

NOTE Restarting the Log Insight service interrupts the log processing for a short period.

6 Close the SSH connection.

Download the Runtime Log File of Log Insight

The Log Insight service runs its own internal logging system that writes messages to a log file.

It is useful to view the contents that file to better understand the system internals. You might be requested by VMware Support Services to provide a copy of this file, or a subset of messages from the relevant timeline, to further troubleshoot an issue.

Prerequisites

- Verify that you have the root user credentials to log in to the Log Insight virtual appliance.
- Verify that TCP port 22 is open to enable SSH connections.

Procedure

1. Establish an SSH connection to the Log Insight virtual appliance and log in as the root user.
2. Navigate to the *PROJECTS_ROOT*/var/ directory and locate the `runtime.log` file.
3. To copy the `runtime.log` file, run `cp runtime.log` *`dest-folder`*`\runtime.log`, where *dest-folder* is a Windows share mounted on the Log Insight virtual machine .
4. On the Windows shared folder, verify that the `runtime.log` file is copied correctly.

What to do next

You can review the contents of the log file for error messages, and use them for troubleshooting.

Remove the Log Insight Adapter from a vCenter Operations Manager vApp

When you enable launch in context on a vCenter Operations Manager vApp, Log Insight creates an instance of the Log Insight adapter on the vCenter Operations Manager vApp.

This instance of the adapter remains in the vCenter Operations Manager vApp when you uninstall Log Insight. As a result, the launch in context menu items continue to appear in the actions menus, and point to a Log Insight instance that no longer exists.

To disable the launch in context functionality in vCenter Operations Manager, you must remove the Log Insight adapter from the vCenter Operations Manager vApp.

You can use the command line utility cURL to send HTTP POST requests to vCenter Operations Manager.

Prerequisites

- Verify that cURL is installed on your system.
- Verify that you know the IP address or domain name of the target vCenter Operations Manager instance.
- Verify that you have administrator user credentials for vCenter Operations Manager.

Procedure

1 In cURL, run the following query on the vCenter Operations Manager virtual appliance to find the Log Insight adapter.

```
curl –k ––user admin username:passwd
https://URL:443/HttpPostAdapter/OpenAPIServlet –d
"action=getRelationships&resourceName=Log Insight
Server&adapterKindKey=LogInsight&resourceKindKey=LogInsightLogServer&
getChildren=true&getParents=false"
```

Where *admin username* and *passwd* are the administrator user credentials, and *URL* is the IP address of the vCenter Operations Manager vApp.

The query returns a result in the following format.

```
resourceName=Log Insight Server&adapterKindKey=LogInsight&resourceKindKey=LogInsightLogServer

Parents:

Children:
resourceName=Log Insight Serverlog insight location&
adapterKindKey=LogInsight&
resourceKindKey=LogInsightLogServerHost&
identifiers=HOST::log insight location
```

Where *log insight location* is the HOST value of the child object of the queried resource. You can use this value in the command that removes the adapter instance.

2 Run the following command to remove the Log Insight adapter.

```
curl –k ––user ––user admin username:passwd https://URL:443/HttpPostAdapter/OpenAPIServlet –
d
"action=addRemoveParentChildRelationship&parentResource=Log Insight
Server&adapterKindKey=LogInsight&
resourceKindKey=LogInsightLogServer&addFlag=false&
childResources=Log Insight Serverlog insight
location,LogInsight,LogInsightLogServerHost,HOST::log insight location"
```

Where *admin username* and *passwd* are the administrator user credentials, *URL* is the IP address of the vCenter Operations Manager vApp, and *log insight location* is the host location of the child resource of the relationship to be removed.

Log Insight launch in context items are removed from the menus in vCenter Operations Manager. For more information about launch in context, see the topic *Log Insight Launch in Context* of the Log Insight in-product help.

Troubleshooting Log Insight 3

You can try solving these common problems before calling VMware Support Services.

This chapter includes the following topics:

ESXi Logs Stop Arriving in Log Insight

After restarting the Log Insight service, syslog messages from ESXi hosts stop arriving in Log Insight.

Problem

Configuration changes in Log Insight require that you restart the Log Insight service. After the restart, syslog feeds from ESXi are no longer available.

Cause

Certain versions of ESXi stop sending logs if the connectivity to the remote syslog listener is interrupted, even briefly. This problem affects the following ESXi versions, depending on the communication protocol that is used.

Table 3-1. ESXi Versions That Stop Sending Syslog Messages

Communication Protocol	Affected ESXi Version
TCP	■ ESXi 5.0.x ■ ESXi 5.1.x
UDP	ESXi 5.0 and 5.0 Update 1

Solution

◆ Reload the syslog server on each ESXi host that stops sending log messages.

a Establish an SSH connection to theESXi host and log in as the root user.

b Use ESXi Shell to reload the syslog server.

```
esxcli system syslog reload
```

You must repeat the procedure on the affected ESXi hosts every time you restart Log Insight. For details about syslog problems and solutions, see VMware ESXi 5.0 host stops sending syslogs to remote server (2003127).

Log Insight Runs Out of Disk Space

Log Insight might run out of disk space if you are using a small virtual disk, and archiving is not enabled.

Problem

Log Insight runs out of disk space if the rate of incoming logs exceeds 3% of the storage space per minute.

Cause

In normal scenarios, Log Insight never runs out of disk because every minute it checks if the free space is less than 3%. If the free space on the Log Insight virtual appliance drops below 3%, old data buckets are retired.

However, if the disk is small and log ingestion rate is so high that the free space (3%) is filled out within 1 minute, Log Insight runs out of disk.

If archiving is enabled, as a bucket has to be archived before it can be retired, if the free space is filled out before the old bucket can be archived and then retired, Log Insight runs out of disk.

Solution

- Increase the storage capacity of the Log Insight virtual appliance. See "Increase the Storage Capacity of the Log Insight Virtual Appliance," on page 16.
- Reduce the number of data buckets that Log Insight stores, and enable archiving.

The Customer Experience Improvement Program

4

You can configure Log Insight to collect data that will help improve your user experience with VMware products. The following section contains important information about the Customer Experience Improvement Program.

The goal of the Customer Experience Improvement Program is to quickly identify and address problems that might be affecting your experience. If you choose to participate in VMware's Customer Experience Improvement Program, Log Insight will regularly send encrypted trace data to VMware. You can use trace data for product development and troubleshooting purposes. Log Insight anonymizes and encrypts any personal identification information from your systems or servers before transferring any trace data to VMware.

If you have any questions or concerns regarding the Customer Experience Improvement Program for Log Insight, contact loginsight-info@vmware.com.

Trace Data that Log Insight Collects

To provide the benefits of the Customer Experience Improvement Program, Log Insight collects trace data directly from log files stored on your Log Insight virtual appliance and transfers the data to VMware on a weekly basis.

Categories of Information in Trace Data

Trace data contains the following categories of information.

runtime.log Contains information about low-level system trace activities conducted by Log Insight, including indexing, garbage collection, and monitoring activities. If an error occurs while Log Insight is processing data or a query, information about the error appears in the `runtime.log` file.

ui.log Contains information regarding interactions with user interface components and parameters, such as which buttons were pressed or which options were selected from a drop-down menu.

usage.log	Contains information regarding the queries that the query engine runs. Each line has the exact query that the search engine runs, including the time it was started, the length of time it ran, and if an error occurred during its execution.
watchdog.log	Contains information from the watchdog process that monitors Log Insight and restarts the application if it fails or becomes unresponsive. The `watchdog.log` file contains information documenting when such failures are detected.

Personal Information in Trace Data

Trace data can also contain personal information, including:

- Email addresses
- MAC addresses
- Internet protocol addresses
- User names
- Host names
- Query content
- Search word content

Personal information found inside trace data files is anonymized and encrypted inside your Log Insight virtual appliance before being transferred to VMware. Trace data is encrypted using public key cryptography and sent through email using your SMTP server. Trace data is stored in the VMware internal secured network and is not shared with third parties.

You can view the files at any time by remotely logging in to your Log Insight virtual appliance using SSH, and navigating to `/storage/var/loginsight/feedback`.

You can stop the transfer of trace data to VMware at any time. See "Stop Sending Trace Data to VMware," on page 30.

If you have any questions or concerns regarding the Customer Experience Improvement Program for Log Insight, contact loginsight-info@vmware.com.

Stop Sending Trace Data to VMware

If you no longer want to participate in the Customer Experience Improvement Program, you can discontinue the transfer of anonymized trace data to VMware.

If you have any questions or concerns regarding the Customer Experience Improvement Program for Log Insight, contact loginsight-info@vmware.com.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface as an administrator user. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 From the configuration drop-down menu, select **Administration**.

2 Under Configuration, click **General**.

3 In the Customer Experience Improvement Program pane, deselect the **Send weekly Trace Data to VMware as part of the Customer Experience Improvement Program** check box.

4 Click **Save** and restart Log Insight to apply your settings.

Log Insight stops sending trace data to VMware.

Index