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 Getting Started Guide

The *VMware vCenter Log Insight Getting Started Guide* provides information about deploying and configuring VMware® vCenter™ Log Insight™, including how to size the Log Insight virtual appliance to receive log messages from your environment.

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 virtual appliance that you must deploy in your environment.

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

This chapter includes the following topics:

Deploy the Log Insight Virtual Appliance

Download the Log Insight virtual appliance. VMware distributes the Log Insight virtual appliance as an `.ova` file. Deploy the Log Insight virtual appliance by using the vSphere Client.

Prerequisites

- Verify that you have a copy of the Log Insight virtual appliance `.ova` file.
- 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.
- Verify that you read and understand the virtual appliance sizing recommendations. See GUID-284FC5F4-B832-47A7-912E-D407A760CAE4#GUID-284FC5F4-B832-47A7-912E-D407A760CAE4.

Procedure

1. In the vSphere Client, select **File > Deploy OVF Template**.
2. Follow the prompts in the Deploy OVF Template wizard.
3. On the Deployment Configuration page, select the size of the Log Insight virtual appliance based on the size of the environment for which you intend to collect logs.

Option	Description
Extra Small	Up to 20 hosts
Small	Up to 100 hosts
Medium	Up to 250 hosts
Large	Up to 750 hosts

NOTE If you select **Large**, you must upgrade the virtual hardware on the Log Insight virtual machine after the deployment.

4 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.

  IMPORTANT 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.

5 (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.

Use comma to separate domain name servers.

6 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 takes several minutes to complete. At the end of the process, the virtual appliance restarts.

7 Navigate to the **Console** tab and check the IP address of the Log Insight virtual appliance.

IP Address Prefix	Description
https://	The DHCP configuration on the virtual appliance is correct.
http://	The DHCP configuration on the virtual appliance failed. a Power off the Log Insight virtual appliance. b Right-click the virtual appliance and select **Edit Settings**. c Set a static IP address for the virtual appliance.

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. See "Configure Log Insight," on page 9.

  The Log Insight 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 user 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 31.
- For information on supported browser versions, see GUID-4E3853AA-EFBF-4004-B182-DF5F6DC3826F#GUID-4E3853AA-EFBF-4004-B182-DF5F6DC3826F.
- Verify that you have a valid license key. You can request an evaluation or permanent license key by using your account to My VMware™.
- If you want to use local, vCenter Server, or Active Directory credentials to integrate Log Insight with vCenter Operations Manager, verify that these users are imported in vCenter Operations Manager Custom user interface. For instructions about configuring LDAP, see the vCenter Operations Manager Administration Guide.

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

   Optionally, you can provide an email address for the admin user.

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

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**.

Option	Description
NTP server (recommended)	By default, Log Insight is configured to synchronize time with 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. Use commas to separate multiple NTP servers.
ESX/ESXi host	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) To allow active directory users access in Log Insight, select **Enable Active Directory support** and click **Save and Continue**.

NOTE Active Directory is enabled for Log Insight only and does not affect the integration with other VMware products.

10 Specify the properties of an SMTP server to enable outgoing alert and system notification emails.

11 To verify that the SMTP configuration is correct, type a valid email address and click **Test**.

Log Insight sends a test email to the address that you provided.

12 Click **Save and Continue**.

13 (Optional) Configure the integration between Log Insight and vCenter Operations Manager.

a Type the hostname and user credentials for the UI VM of the vCenter Operations Manager vApp, and click **Test Connection** to verify the connection.

NOTE You must provide the user credentials of a vCenter Operations Manager administrator user.

b To allow Log Insight to send alert notifications triggered by Log Insight alarms, select **Enable alerts integration**.

c To allow vCenter Operations Manager to launch Log Insight with an object-specific query, click **Enable Launch in Context**.

This operation might take a few minutes.

14 Click **Save and Continue**.

15 (Optional) To archive 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.

16 Click **Save and Continue**.

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

After the Log Insight process restarts, you are redirected to the **Dashboards** tab of Log Insight.

What to do next

- Go to the **Administration** page by selecting the drop-down menu icon  in the navigation bar and use the **vSphere Integration** page to configure Log Insight to pull tasks, events, and alerts from vCenter Server instances, and to configure ESXi hosts to send syslog feeds to Log Insight.

Administering Log Insight 2

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

Some changes to the configuration of Log Insight are applied only after you restart the `loginsight` service. Changes related to time configuration, vSphere integration, and authentication do not require restart.

This chapter includes the following topics:

Configure the Root SSH Password for 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. Go to a command line by following the key combination specified on the splash screen.
3. In the console, type **`root`**, and press Enter. Leave the password empty and press Enter.

   The following message is displayed in the console: `Password change requested. Choose a new password.`
4. Leave the old password empty and press Enter.

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

The password must consist of at least eight characters, and must include at least one upper case letter, one lower case letter, one digit, and one special character. You cannot repeat the same character more than four 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.

Log Storage Policy

The Log Insight virtual appliance uses a minimum of 100GB of storage for incoming logs.

When the volume of logs imported into Log Insight reaches the 100GB limit, old log messages are automatically and periodically retired on a first-come-first-retired basis. To preserve old messages, you can enable the archiving feature of Log Insight. See "Enable or Disable Data Archiving in Log Insight," on page 13.

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

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

Log in to the vSphere Client as a user who has privileges to modify the hardware of virtual machines in the environment.

Shut down the Log Insight virtual appliance safely. See "Power Off the Log Insight Virtual Appliance," on page 21.

Procedure

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

2 On the **Hardware** tab, 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.

Option	Description
Thick Provision Lazy Zeroed	Creates a virtual disk in the default thick format. The space required for the virtual disk is allocated when the virtual disk is created. The data residing on the physical device is not erased during creation, but is zeroed out on demand at a later time, after 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. The space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data residing 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 default 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 may result in complete data loss.

Enable or Disable Data Archiving in Log Insight

Data archiving preserves old logs that might otherwise be removed from the Log Insight virtual appliance due to storage constraints. Log Insight can store archived data to NFS mounts.

NOTE Log Insight does not manage the NFS mount used for archiving purposes. If system notifications are enabled, Log Insight sends an email when the NFS mount is about to run out of space or is unavailable . If the NFS mount does not have enough free space or is unavailable for a period of time greater than the retention period of the virtual appliance, Log Insight stops ingesting new data until the NFS mount has enough free space, becomes available, or archiving is disabled.

Prerequisites

- 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.

- Verify that you are logged in to the Log Insight Web user interface as an Admin 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. Click the configuration drop-down menu icon and select **Administration**.
2. Under Configuration, click **Storage**.
3. Select the **Enable Data Archiving** check box, type the path to an NFS partition where logs will be archived, and click **Test** to verify the connection.

   If data archiving is enabled, old log files are saved to the NFS partition.
4. Click **Save**.

NOTE Data archiving preserves log events that have since been removed from the Log Insight virtual appliance due to storage constraints. Log events that have been removed from the Log Insight virtual appliance, but have been archived are no longer searchable. If you want to search archived logs, you must import them into a Log Insight instance. For more information about importing archived log files, see "Import a Log Insight Archive into Log Insight," on page 19.

What to do next

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 near real time.

Forwarding Log Files to Log Insight

Log Insight can analyze log events from any VMware vCloud Suite component that can forward syslog feeds.

Configure an ESXi Host to Forward Log Events to Log Insight

Logs contain unstructured data that can be analyzed in Log Insight. ESXi hosts or vCenter Server Appliance instances can push their logs to Log Insight through syslog.

You must configure the ESXi hosts or vCenter Server Appliance instances to push their syslog data to Log Insight.

You use the Administration user interface of Log Insight to configure ESXi hosts on a registered vCenter Server to forward syslog feeds to Log Insight.

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

For information on configuring syslog feeds from a vCenter Server Appliance, see "Configure a vCenter Server Appliance to Forward Log Events to Log Insight," on page 19.

NOTE Log Insight can receive syslog data from ESXi host versions 4.x and later.

Prerequisites

- Verify that the vCenter Server that manages the ESXi host is registered with your Log Insight instance.
- 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.

Procedure

1 Click the configuration drop-down menu icon and select **Administration**.

2 Under Integration, click **vSphere**.

3 Locate the vCenter Server instance that manages the ESXi host from which you want to receive syslog feeds.

4 Select the **Configure ESXi hosts to send logs to Log Insight** check box.

  By default, Log Insight configures all reachable ESXi hosts of version 4.x and later to send their logs via UDP . ESX hosts are not supported.

  NOTE While ESXi 5.x hosts can have multiple syslog targets, ESXi 4.x hosts can have only one target. By default, Log Insight overwrites and replaces any existingESXi 4.x syslog targets.

5 (Optional) To select which ESXi hosts forward their logs to Log Insight, which protocol is used for forwarding logs to Log Insight, and how to handle syslog configuration on ESXi 4.x hosts, click **Advanced Options**.

6 Click **Save**.

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.

You can run the `configure-esxi` script by using the virtual appliance console in the vSphere Client, or though an SSH connection.

NOTE User names and passwords in the scripts can 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 script 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 virtual appliance.
- 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 the root user credentials to log in to the Log Insight virtual appliance.

- If you plan to connect to the Log Insight virtual appliance by using SSH, verify that TCP port 22 is open.

Procedure

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

2 To configure all ESXi 4.x and 5.x hosts nondestructively to send their logs to myloginsight.mydomain.com, run the following command.

```
configure-esxi -u 'my-vc-user' -s myvc.mydomain.com -t 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.

3 To configure all ESXi 4.x and 5.x hosts to send their logs, run the following command.

```
configure-esxi -u 'my-vc-user' -s myvc.mydomain.com -t 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.

4 To reload syslog on all ESXi hosts, run the following command.

```
configure-esxi -u 'my-vc-user' -s 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.

5 To query the current remote syslog configurations on all ESXi 4.x and 5.x hosts attached to a vCenter Server, run the following command.

```
configure-esxi -u 'my-vc-user' -s myvc.mydomain.com -q
```

6 (Optional) To remove a specific syslog target from the list of remote syslog targets, run the following command.

```
configure-esxi -u 'my-vc-user' -s myvc.mydomain.com -r 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.

NOTE The configurations that you apply by using the `configure-esxi` script might not be reflected in the Log Insight user interface.

What to do next

For complete information about using the `configure-esxi` script, run `configure-esxi --help`.

Configure Syslog Manually Through Command Line

You can set up syslog by using the `esxcli` utility to forward log events to Log Insight.

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

Prerequisites

NOTE If you already configured an ESXi host to forward log events to Log Insight, following the "Configure an ESXi Host to Forward Log Events to Log Insight," on page 14 procedure (recommended), you can ignore the manual configuration procedure.

- 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 4.x, read and understand the information in the VMware knowledge base article Enabling syslog on ESXi 3.5 and 4.x (KB 1016621).
- 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.

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 current configuration options on the host, run the following command.

```
esxcli system syslog config get
```

3 To modify a host configuration, run the following command to specify the options to change.

```
esxcli system syslog config set --loghost=tcp|udp|ssl://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.

Configure Syslog Manually Through the vSphere Web Client

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.

NOTE The procedure might vary depending on the version of the ESXi host that you configure, and the vSphere Web Client that you use .

Prerequisites

NOTE If you already configured an ESXi host to forward log events to Log Insight, following the "Configure an ESXi Host to Forward Log Events to Log Insight," on page 14 procedure (recommended), you can ignore the manual configuration procedure.

- 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 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 System Settings**.
3. Locate the Syslog.global.logHost property and click the **Edit** icon  .
4. Modify the Syslog.global.logHost property to point to the Log Insight IP address or host name and click **OK**.

   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 virtual appliance.

   NOTE Use port 514 for UDP and TCP communication, and port 1514 for SSL protocol.
5. Verify that Firewall is not blocking the communication ports.
   a. On the **Settings** tab, click **Security Profile**, and verify that syslog appears in the Outgoing Connections list.
   b. If you do not see syslog in the Outgoing Connections list, click **Edit** on the upper right.
   c. On the list of services, scroll down to locate the syslog service, and select the **syslog** check box.
   d. Click **OK**.

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

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

Prerequisites

- Verify that you have the root user credentials for the vCenter Server Appliance.
- If you plan to connect to the Log Insight virtual appliance by using SSH, verify that TCP port 22 is open.

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 Insight Archive into Log Insight

You can use the command line to import 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.

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 NFS server where Log Insight logs are archived.
- Verify that the Log Insight virtual appliance has enough disk space to accommodate the imported log files.

  The minimum free space in the `/storage/core` partition on the virtual appliance must equal approximately 10 times the size of the archived log that you want to import.

Procedure

1 Establish an SSH connection to the Log Insight vApp 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 Importing archived data might take a long time, depending on the size of the imported folder.

4 Close the SSH connection.

What to do next

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

Install a Custom SSL Certificate by Using the Log Insight Web Interface

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

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 The Log Insight Web user interface and the SSL syslog protocol use the same certificate for authentication.

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.
  - The private key and all the certificates that are included in the certificate file are PEM-encoded. Log Insight does not support DER-encoded certificates and private keys.
  - The private key and all the certificates 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 you are logged in to the Log Insight Web user interface as an Admin 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.
- If you use Internet Explorer 9, verify that you have Adobe Flash Player installed on your system.

Procedure

1 Click the configuration drop-down menu icon and select **Administration**.

2 Under Configuration, click **SSL Certificate**.

3 Browse to your custom SSL certificate and click **Open**.

4 Click **Save**.

What to do next

Enable or Disable the Web Authentication

Web authentication in Log Insight is enabled by default.

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

Prerequisites

- 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 Admin 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.
- Verify that you have the root user credentials to log in to the Log Insight virtual appliance.

Procedure

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

2 Under Configuration, click **General.**

3 In the Web UI widget, use the **Enable Authentication** check box to change the Web authentication state.

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

Restart the Log Insight Service

You can restart Log Insight by using the Administration page in the Web user interface.

CAUTION Restarting Log Insight closes all active user sessions. Users of the Log Insight instance will be forced to log in again.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface as an Admin 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 Click the configuration drop-down menu icon  and select **Administration**.

2 Under Management, click **Appliance**.

3 Click **Restart Log Insight** and click **Restart**.

What to do next

Power Off the Log Insight Virtual Appliance

To avoid data loss when powering off Log Insight, you must power the virtual appliance off by following a strict 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 virtual appliance by using the **Power > Shut Down Guest** menu option in the vSphere Client, by using the virtual appliance console, or by establishing an SSH connection to the Log Insight virtual appliance and running a command.

Prerequisites

- If you plan to connect to the Log Insight virtual appliance by using SSH, verify that TCP port 22 is open.
- 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 vApp 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.

Remove the Log Insight Adapter from a vCenter Operations Manager instance

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

This instance of the adapter remains in the vCenter Operations Manager instance 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 instance.

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 host name of the target vCenter Operations Manager instance.
- Depending on the vCenter Operations Manager license that you own, verify that you have minimum user credentials.

vCenter Operations Manager License	Minimum Required Credentials
Standard	Default Admin user credentials
Advanced or Enterprise	Read Only user credentials

NOTE If you want to use Active Directory or vCenter Server accounts, verify that these accounts are added in vCenter Operations Manager Custom user interface. For information about adding active directory users in vCenter Operations Manager, see the VMware vCenter Operations Manager Administration Guide.

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 instance.

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 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 instance, and *log insight location* is the host location of the child resource of the relationship you want to remove.

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 attempt to solve common problems related to Log Insight administration 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

1 Click the configuration drop-down menu icon and select **Administration**.

2 Under Integration, click **vSphere**.

3 For each vCenter Server instance that has the **View ESXi syslog configuration details** link, click the **View ESXi syslog configuration details** link.

4 Select all hosts that previously had a configuration and click **Configure**.

NOTE The configuration process can take several minutes. You must repeat the procedure every time you restart Log Insight. For details about syslog problems and solutions, see VMware ESXi 5.x 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 percent of the storage space per minute.

Cause

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

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

If archiving is enabled, Log Insight archives the bucket before retiring it. If the free space is filled before the old bucket is archived and 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 12.

Download a Log Insight Support Bundle

If Log Insight does not operate as expected because of a problem, you can send a copy of the log and configuration files to VMware Support Services.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface as an Admin 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 Click the configuration drop-down menu icon and select **Administration**.

2 Under Management, click **Appliance**.

3 Under the Support header, click **Download Support Bundle**.

The Log Insight system collects the diagnostic information and streams the data to your browser in a compressed tarball.

4 In the File Download dialog box, click **Save**.

5 Select a location to which you want to save the tarball archive and click **Save**.

What to do next

You can review the contents of log files for error messages. When you resolve or close issues, delete the outdated support bundle to save disk space.

Use the Virtual Appliance Console to Create a Support Bundle of Log Insight

If you cannot access the Log Insight Web user interface, you can download the support bundle by using the virtual appliance console or after establishing an SSH connection to the Log Insight virtual appliance.

Prerequisites

- Verify that you have the root user credentials to log in to the Log Insight virtual appliance.
- If you plan to connect to the Log Insight virtual appliance by using SSH, verify that TCP port 22 is open.

Procedure

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

2 To generate the support bungle, run `loginsight-support`.

The support information is collected and saved in a `*.tar.gz` file that has the following naming convention: `loginsight-support-YYYY-MM-DD_HHMMSS.xxxxx.tar.gz`, where `xxxxx` is the process ID under which the `loginsight-support` process ran.

What to do next

Forward the support bundle to VMware Support Services as requested.

Reset the Admin User Password

If an administrator user forgets the password to the Web user interface, the account becomes unreachable.

Problem

If Log Insight has only one Admin user and the Admin user forgets the password, the application cannot be administered. If an Admin user is the only user of Log Insight, the whole Web user interface becomes inaccessible.

Cause

Log Insight does not provide a user interface for Admin users to reset their own passwords, if the user does not remember their current password.

NOTE Admin users who are able to log in can reset the password of other Admin users. Reset the Admin user password only when all Admin user accounts' passwords are unknown.

Solution

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

2 Change the directory to `/usr/lib/loginsight/application/lib/pgsql/bin`

3 To copy the Admin user Salt, run the following command.

```
SALT=`./psql –A –t –d logdb –U liuser –p 12543 –c "select salt from li_user where
name='admin' ;"`
```

NOTE The outer quotes are inserted by using the back quote symbol that is on the same key as tilde on your keyboard. Do not use single quotes.

---

4 Enter the required the password for liuser. The password is liuser.

NOTE Do not change this password.

5 To hash the password, run the following command.

```
PASS=`echo –n "vmware$SALT" | sha256sum | cut –d " " –f 1`
```

NOTE The outer quotes are inserted by using the back quote symbol that is on the same key as tilde on your keyboard. Do not use single quotes.

6 Update the admin user record by running the following command.

```
./psql –d logdb –U liuser –p 12543 –c "update li_user set password='$PASS' where
name='admin' ;"
```

7 Enter the required the password for liuser. The password is liuser.

NOTE Do not change this password.

What to do next

Log in to the Log Insight Web user interface with the following credentials

- Username: admin
- Password: vmware

and change the Admin user password.

Reset the Root User Password

If you forget the password of the root user, you can no longer establish SSH connections or use the console of the Log Insight virtual appliance.

Problem

If you cannot establish SSH connections or use the console of the Log Insight virtual appliance, you cannot accomplish some of the administration tasks, nor can you reset the password of the admin user.

Solution

1 In the vSphere Client, restart the guest operating system of the Log Insight virtual appliance, and open the console for the virtual machine.

2 Click in the console, wait for the GRUB menu to appear and press any letter key.

NOTE The GRUB prompt remains on the screen for 7 seconds before it starts the boot sequence.

3 On the GRUB menu, use the arrow keys to select **SUSE Linux Enterprise Server for VMware**.

4 Press the spacebar, type **`init=/bin/sh`**, and press Enter.

The kernel boots in shell mode.

5 In the shell, type **`passwd`**, press Enter, and follow the on-screen instructions to change the root password.

The password must consist of at least eight characters, and must include at least one upper case letter, one lower case letter, one digit, and one special character such as $ or &. You cannot repeat the same character more than four times.

6 In the shell, type **`reboot`**.

What to do next

Once Log Insight reboots, validate that you can log in as the root user.

Alerts Could Not Be Delivered to vCenter Operations Manager

Log Insight notifies you if an alert event cannot be sent to vCenter Operations Manager. Log Insight retries sending the alert every minute until the problem is resolved.

Problem

A red sign with an exclamation mark appears in the Log Insight toolbar when an alert could not be delivered to vCenter Operations Manager.

Cause

Connectivity problems prevent Log Insight from sending alert notifications to vCenter Operations Manager.

Solution

- Click on the red icon to open the list of error messages, and scroll down to view the latest message.

  The red sign disappears from the toolbar when you open the list of error messages, or if the problem is resolved.

- To fix the connectivity problem with vCenter Operations Manager, try the following.
  - Verify that the vCenter Operations Manager vApp is not shut down.
  - Verify that the you can connect to vCenter Operations Manager via the **Test Connection** button in the **vCenter Operations Manager** section of the **Administration** page of the Log Insight Web user interface.
  - Verify that you have the correct credentials by logging directly into vCenter Operations Manager.
  - Check Log Insight and vCenter Operations Manager logs for messages related to connectivity problems.
  - Verify that no alerts are filtered out in vCenter Operations Manager vSphere User Interface.

Unable to Log In Using Active Directory Credentials

You cannot log in to the Log Insight Web user interface when you use Active Directory credentials.

Problem

You cannot log in to Log Insight by using your Active Directory domain user credentials, despite that an administrator has added your Active Directory account to Log Insight.

Cause

The most common causes are expired passwords, incorrect credentials, connectivity problems, or lack of synch between the Log Insight virtual appliance and Active Directory clocks.

Solution

- Verify that your credentials are valid, your password has not expired, and your Active Directory account is not locked.
- If you have not specified a domain to use with Active Directory authentication, verify that you have an account on the default domain stored in Log Insight configuration at `/usr/lib/loginsight/application/etc/loginsight-config-base.xml`

- Verify Log Insight has connectivity to the Active Directory server.
  - Go to the **Authentication** section of the **Administration** page of the Log Insight Web user interface, fill in your user credentials, and click the **Test Connection** button.
  - Check the Log Insight `/storage/var/loginsight/runtime.log` for messages related to DNS problems.
- Verify that the Log Insight and Active Directory clocks are in synch.
  - Check the Log Insight `/storage/var/loginsight/runtime.log` for messages related to clock skew.
  - Use an NTP server to synchronize the Log Insight and Active Directory clocks.

The Customer Experience Improvement Program 4

You can configure Log Insight to collect data to 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 the VMware 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 li-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`.

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

Index

W