VMware vCenter Log Insight Administration Guide

vCenter Log Insight 1.5

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-001298-00

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

About vCenter Log Insight Administration Guide

The *VMware vCenter Log Insight Administration Guide* provides information about administering Log Insight, including how to manage user accounts, integrate with other VMware products and troubleshoot common problems.

Intended Audience

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

Administering Log Insight 1

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.

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

- Obtain a valid license key from My VMware™.
- 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, select **License**.

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

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

Upgrading from Previous Versions of Log Insight

The upgrade procedure to follow varies with the installed version of Log Insight that you want to upgrade.

Installed Version	Upgrade Version	Upgrade Procedure
Log Insight 1.0 GA and 1.5 TP1	Log Insight 1.5	See "Upgrade Log Insight by Using CLI," on page 9.
Log Insight 1.5 TP2 and later	Log Insight 1.5	See "Upgrade Log Insight By Using the Web Interface," on page 10.

Upgrade Log Insight by Using CLI

Because Log Insight 1.0 GA and 1.5 TP1 do not provide a user interface for upgrade, you must use a CLI to update these versions to Log Insight 1.5.

For Log Insight versions 1.5 TP2 and later, use the Administration user interface for upgrades. See "Upgrade Log Insight By Using the Web Interface," on page 10.

This procedure uses the virtual appliance console, but you can run it through SSH as well.

NOTE All active users of the Log Insight instance are logged out during the upgrade process.

Prerequisites

- Verify that you set the root user password on the Log Insight virtual appliance to enable SSH and console operations. See "Configure the Root SSH Password for the Log Insight Virtual Appliance," on page 8.
- Create a snapshot or backup copy of the Log Insight virtual appliance.
- Obtain a copy of the Log Insight upgrade bundle `.rpm` file.

Procedure

1 Download the `.rpm` file to a host that has SSH access to the Log Insight virtual appliance.

2 Use the secure copy protocol to copy the `.rpm` file to the Log Insight virtual appliance.

Operating System	Command/Tool
Linux	`scp` *`path to the RPM file`*`/loginsight-cloudvm-`*`version-log-insight-buildnumber`*`.x86_64.rpm root@<LogInsightIPorHostname>:~`
Windows	For Windows systems, download an SCP client like WinSCP.

3 Use the vSphere Client console to log in to the Log Insight virtual appliance as the root user.

4 Run the `service loginsight stop` command.

5 Run the `rpm -Uvh loginsight-cloudvm-<version>-<log-insight-build-number>.x86_64.rpm` command, and wait for the upgrade to complete.

6 Run the `service loginsight start` command.

7 Verify that you can log in to the Log Insight Web user interface.

Remember 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 see an error page, log in as the root user in the virtual appliance console, and run the `service loginsight restart` command to restart the `loginsight` service.

Upgrade Log Insight By Using the Web Interface

Admin users can upgrade Log Insight 1.5 TP2 and later by using the administration user interface.

Note All active users of the Log Insight instance are logged out during the upgrade process.

Prerequisites

- Create a snapshot or backup copy of the Log Insight virtual appliance.
- Obtain a copy of the Log Insight upgrade bundle `.rpm` file.
- 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 Management, click **Appliance**.

3 Click **Upload RPM**, and browse for the `.rpm` file.

4 Click **Upgrade**.

Log Insight uploads the `.rpm` file to the virtual appliance and displays a confirmation dialog box.

5 Click **Upgrade** to confirm.

6 Accept the new EULA to complete the upgrade procedure.

Check the Health of the Log Insight Virtual Appliance

You can check available resources and active queries on the Log Insight virtual appliance, and view current statistics about the operation of Log Insight.

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 **System Monitor**.

3 Click the buttons on the System Monitor page to view the information that you need.

Option	Description
Resources	View information about the CPU, memory, IOPS (read and write activity), and storage usage on the Log Insight virtual appliance. The charts on the right represent historical data for the last 24 hours, and are refreshed at five-minute intervals. The charts on the left display information for the last five minutes, and are refreshed every three seconds.
Active Queries	View information about the queries that are currently active in Log Insight.
Statistics	View statistics about the log ingest operations and rates. To view more detailed statistics, click **Show advanced statistics**.

What to do next

You can use the information from the System Monitor page to manage resources on 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 35.

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 39.

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.

Managing User Accounts in Log Insight

Administrators can create user accounts to provide users with access to the Log Insight Web interface.

The current version of Log Insight supports two user roles, Normal user and Admin user.

Only administrator users can create and edit all user accounts.

Normal users can modify their own accounts to change their email or account password.

Create a New User Account in Log Insight

Administrators can create user accounts to provide access to the Log Insight Web user interface.

The current version of Log Insight supports two user roles, Normal user and Admin user.

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 **Users**.

3 Click **New User**.

4 In the **Authentication Method** drop-down menu, select **Default (built-in)**.

5 Type a user name and email address.

The email address is optional.

6 From the **Role** drop-down menu, select the user role.

Option	Description
Normal User	Normal users can access the full functionality of Log Insight to view log events, run queries to search and filter logs, import content packs into their own user space, add alert queries, and manage their own user accounts to change their password or email address. Normal users do not have access to the administration options, cannot share content with other users, and cannot modify the accounts of other users, and cannot install a content pack as a content pack.
Admin	Admin users can access the full functionality of Log Insight, can administer Log Insight, and can manage the accounts of all other users.

7 Copy the password from the **Password** text box and provide it to the user.

8 Click **Save**.

Add an Active Directory User to Log Insight

You can allow active directory users (AD) to log in to Log Insight by using their domain credentials.

When you enable AD support in Log Insight, you configure a domain name and provide a binding user that belongs to the domain. Log Insight uses the binding user to verify the connection to the AD domain, and to verify the existence of AD users and groups.

The AD users that you add to Log Insight must either belong to the domain of the binding user, or to a domain that trusts the domain of the binding user.

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.
- Verify that you configured the AD support. See "Enable User Authentication Through Active Directory," on page 35.

Procedure

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

2 Under Management, click **Users**.

3 Click **New User**.

4 From the **Authentication Method** drop-down menu, select **Active Directory**.

The default domain name that you specified when you configured AD support appears in the **Domain** text box. If you are adding users from the default domain, do not modify the domain name.

5 (Optional) If you want to add a user from a domain that trusts the default domain, type the name of the trusting domain in the **Domain** text box.

6 Type the name of a domain user.

7 From the **Role** drop-down menu, select the user role.

Option	Description
Normal User	Normal users can access the full functionality of Log Insight to view log events, run queries to search and filter logs, import content packs into their own user space, add alert queries, and manage their own user accounts to change their password or email address. Normal users do not have access to the administration options, cannot share content with other users, and cannot modify the accounts of other users, and cannot install a content pack as a content pack.
Admin	Admin users can access the full functionality of Log Insight, can administer Log Insight, and can manage the accounts of all other users.

8 Click **Save**.

Log Insight verifies whether the user exists in the domain that you specified or in its trusted domains. If the user does not exist, a dialog box informs you that Log Insight cannot verify that user. You can save the user without verification or cancel and correct the user name.

AD users that you add can use their domain credentials to log in to Log Insight.

Add an Active Directory Group to Log Insight

Instead of adding individual domain users, you can add domain groups to allow users to log in to Log Insight.

When you enable AD support in Log Insight, you configure a domain name and provide a binding user that belongs to the domain. Log Insight uses the binding user to verify the connection to the AD domain, and to verify the existence of AD users and groups.

The AD groups that you add to Log Insight must either belong to the domain of the binding user, or to a domain that is trusted by the domain of the binding user.

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.
- Verify that you configured the AD support. See "Enable User Authentication Through Active Directory," on page 35.

Procedure

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

2 Under Management, click **Users**.

3 Under Active Directory Groups, click **New Group**.

The default domain name that you specified when you configured AD support appears in the **Domain** text box. If you are adding groups from the default domain, do not modify the domain name.

4 (Optional) If you want to add a group from a domain that trusts the default domain, type the name of the trusting domain in the **Domain** text box.

5 Type the name of the AD group that you want to add.

6 From the **Role** drop-down menu, select the user role.

Option	Description
Normal User	Normal users can access the full functionality of Log Insight to view log events, run queries to search and filter logs, import content packs into their own user space, add alert queries, and manage their own user accounts to change their password or email address. Normal users do not have access to the administration options, cannot share content with other users, and cannot modify the accounts of other users, and cannot install a content pack as a content pack.
Admin	Admin users can access the full functionality of Log Insight, can administer Log Insight, and can manage the accounts of all other users.

7 Click **Save**.

Log Insight verifies whether the AD group exists in the domain that you specified or in a trusting domain. If the group cannot be found, a dialog box informs you that Log Insight cannot verify that group. You can save the group without verification or cancel to correct the group name.

Users that belong to the AD group that you added can use their domain account to log in to Log Insight and have the same level of permissions as the group to which they belong.

Modify a User Account in Log Insight

A Log Insight administrator can change the user account type and reset their passwords. All users can change their email addresses and passwords.

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, select **Users**.

3 Select the user account that you want to modify and click the **Edit** icon .

4 Modify the parameters of the account and click **Save**.

NOTE The modified user permissions are applied the next time a user logs in. If a user is logged in while you apply changes to their account, your changes are not applied until the user logs out and logs in again.

Delete a User Account from Log Insight

You can delete user accounts by using the Log Insight Administration user interface.

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 **Users**.

3 Select the check box beside the user name that you want to delete.

4 Click the **Delete** icon  .

Configure Log Insight System Alerts

An administrator can configure Log Insight to send notifications related to its own health.

Log Insight generates these notifications when an important system event occurs, for example when the disk space is almost exhausted and Log Insight must start deleting or archiving old log files.

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 Configuration, click **General**.

3 Under the Alerts header, set the system notifications.

   a In the **Email System Notifications To** text box, type the email addresses to be notified.

   Use commas to separate multiple email addresses.

   b Select the **Send a notification when capacity drops below** check box and set the threshold that triggers the notifications.

   c (Optional) Verify that the **Suspend User Alerts** check box is not selected.

   You can select this check box to stop all user defined email alerts.

   NOTE System notifications can be disabled by removing the email addresses specified in the **Email System Notification To** text box (not recommended).

4 Click **Save**.

5 Click **Restart Log Insight** to apply your changes.

Email Notifications that Log Insight Sends

Log Insight sends two types of email notifications, system notifications and user defined notifications.

Administrators can configure Log Insight to send email notifications when certain events occur in the system. The from address of system notification emails is configured by the administrator user on the SMTP configuration page of the Administration UI, in the **Sender** text box. See "Configure the SMTP Server for Log Insight," on page 19.

Administrator users can also configure Log Insight to send notification emails when the storage capacity drops below a defined threshold.

Every Log Insight user can create alert queries to receive email notifications from Log Insight when certain criteria are met.

Administrator users can disable all user defined notifications.

Type	Alert Name	Description
System	Oldest Data Will Be Unsearchable Soon	This alert notifies you when Log Insight is expected to start decommissioning old data from the virtual appliance storage and what is the expected size of searchable data at the current ingest rate. Data that has been rotated out will be archived if you have configured archiving, or deleted if you have not. The alert is sent after each restart of the Log Insight service.
System	Repository Retention Time	This alert notifies you about the amount of searchable data that Log Insight can store at the current ingest rates and in the storage space that is available on the virtual appliance. Admin users can define the storage notification threshold. See "Configure Log Insight System Alerts," on page 16.
System	Dropped Events	This alert notifies you that Log Insight failed to ingest all incoming log messages. ■ In case of any TCP Message drops, as tracked by Log Insight server, a system alert is sent in both cases as follows: ■ Once a day ■ Each time the Log Insight service is restarted, manually or automatically. ■ The email contains the number of messages dropped since last alert email was sent and total message drops since the last restart of Log Insight. NOTE The time in the sent line is controlled by the email client, and is in the local time zone, while the email body displays UTC time.
System	Corrupt Index Buckets	This alert notifies you that part of the on-disk index is corrupt. A corrupt index usually indicates serious issues of the underlying storage system. The corrupt part of the index will be excluded from serving queries. A corrupt index affects the ingestion of new data. Log Insight checks the integrity of the index upon service start-up. In case of detected corruption Log Insight sends a system alert as follows: ■ Once a day ■ Each time the Log Insight service is restarted, manually or automatically.

Type	Alert Name	Description
System	Out Of Disk	This alert notifies you that Log Insight is running out of allocated disk space. This alert signals that Log Insight has most probably run into a storage related issue.
System	Archive Space Will Be Full	This alert notifies you that the disk space on the NFS server used for archiving Log Insight data will be used up soon.
System	Archive Failure	This alert notifies you that an operation of archiving Log Insight data to the NFS server has failed. This usually means that Log Insight is having trouble connecting to or writing to the NFS server.
System	Total Disk Space Change	This alert notifies you that the total size of the partition for Log Insight data storage has decreased. This usually signals a serious issue in the underlying storage system. When Log Insight detects the condition it sends this alert as follows: ■ Immeadiately ■ Once a day
System	Pending Archivings	This alert notifies you that Log Insight cannot archive data as expected. The alert usually indicates problems with the NFS storage that you configured for data archiving.
User Defined	Alert Queries	This alert notifies you that a query returned results that match the criteria that you have set for the alert. Every user can define alert queries that send email notifications when certain criteria are met. See topic Add an Alert Query in Log Insight to Send Email Notifications in the *Log Insight User's Guide*.

Synchronize the Time on the Log Insight Virtual Appliance

You must synchronize the time on the Log Insight virtual appliance with an NTP server or with the ESX/ESXi host on which you deployed the virtual appliance.

Time is critical to the core functionality of Log Insight.

By default, Log Insight synchronizes time with a pre-defined list of public NTP servers. If public NTP servers are not accessible due to a firewall, you can use the internal NTP server of your company. If no NTP servers are available, you can sync time with the ESX/ESXi host where you have deployed the Log Insight virtual appliance.

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 Configuration, click **Time**.

3 From the **Sync time with** drop-down menu, select the time source.

Option	Description
NTP server	Synchronizes the time on the Log Insight virtual appliance with one of the listed NTP servers.
ESX/ESXi host	Synchronizes the time on the Log Insight virtual appliance with the ESX/ESXi host on which you have deployed the virtual appliance.

4 (Optional) If you selected NTP server synchronisation, list the NTP server addresses, and click **Test**.

NOTE Testing the connection to NTP servers might take up to 20 seconds per server.

5 Click **Save**.

Configure the SMTP Server for Log Insight

You can configure an SMTP to allow Log Insight to send email alerts.

System alerts are generated when Log Insight detects an important system event, for example when the storage capacity on the virtual appliance reached the thresholds that you set. See "Email Notifications that Log Insight Sends," on page 16.

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 Configuration, click **SMTP**.

3 Type the SMTP server address and port number.

4 If the SMTP server users an encrypted connection, select the encryption protocol.

5 In the **Sender** text box, type an email address to use when sending system alerts.

The **Sender** address appears as the From address in system notification emails. It need not be a real address, and can be something that represents the specific instance of Log Insight. For example, `loginisght@example.com`.

6 Type a user name and password to authenticate with the SMTP server when sending system alerts.

7 Type a destination email and click **Send Test Email** to check the connection.

8 Click **Save**.

9 Click **Restart Log Insight** to apply your changes.

Integrating Log Insight with Other VMware Products

Log Insight can integrate with other VMware products to use events and log data, and provide better visibility of the events that occur in your virtual environment.

Integration with VMware vSphere

Log Insight Administrator users can set up Log Insight to connect to vCenter Server systems at two-minute intervals, and collect events, alarms, and tasks data from these vCenter Server systems. In addition, Log Insight can configure ESXi hosts via vCenter Server. See "Connect Log Insight to a vSphere Environment," on page 20.

Integration with VMware vCenter Operations Manager

You can integrate Log Insight with vCenter Operations Manager vApp and vCenter Operations Manager Installable. Integrating with the Installable version requires additional changes to the vCenter Operations Manager configuration. For information about configuring vCenter Operations Manager Installable to integrate with Log Insight, see the *Log Insight Getting Started Guide*.

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

Notification Events Log Insight administrator users can set up Log Insight to send notification events to vCenter Operations Manager based on queries that you create. These notification events are not alerts in vCenter Operations Manager, and do not affect the values of the Health, Risk, or Efficiency badge. See "Configure Log Insight to Send Notification Events to vCenter Operations Manager," on page 27.

Launch in Context Launch in context is a feature in vCenter Operations Manager that lets you launch an external application via URL in a specific context. The context is defined by the active UI element and object selection. Launch in context lets the Log Insight adapter add menu items to a number of different views within the Custom user interface and the vSphere user interface of vCenter Operations Manager. See "Enable Launch in Context for Log Insight in vCenter Operations Manager," on page 30.

NOTE Notification events do not depend on the launch in context configuration. You can send notification events from Log Insight to vCenter Operations Manager even if you do not enable the launch in context feature.

If the environment changes, Log Insight administrator users can change, add, or remove vSphere systems from Log Insight, change or remove the instance of vCenter Operations Manager to which alert notifications are sent, and change the passwords that are used to connect to vSphere systems and vCenter Operations Manager.

Connect Log Insight to a vSphere Environment

Before you configure Log Insight to collect alarms, events, and tasks data from your vSphere environment, you must connect Log Insight to one or more vCenter Server systems.

Log Insight can collect two types of data from vCenter Server instances and the ESXi hosts that they manage.

- Events, tasks, and alerts are structured data with specific meaning. If configured,Log Insight pulls events, tasks, and alerts from the registered vCenter Server instances.

- 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.

Prerequisites

- For the level of integration that you want to achieve, verify that you have user credentials with enough privileges to perform the necessary configuration on the vCenter Server system and its ESXi hosts.

Level of Integration	Required Privileges
Events, tasks, and alarms collection	■ **System.View**
Syslog configuration on ESXi hosts	■ **Host.Configuration.Change settings** ■ **Host.Configuration.Network configuration** NOTE The **Host.Configuration.Advanced Configuration** permission is required when configuring ESXi 4.1 hosts.

NOTE You must configure the permission on the top-level folder within the vCenter Server inventory, and verify that the **Propagate to children** check box is selected.

- Verify that you know the IP address or domain name of the vCenter Server system.
- Verify that you are logged in to the 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 Integration, click **vSphere**.

3 Type the IP address and credentials for a vCenter Server, and click **Test Connection**.

4 (Optional) To register another vCenter Server, click **Add vCenter Server** and repeat steps 3 through 5.

NOTE Do not register vCenter Server systems with duplicate names or IP addresses . Log Insight does not check for duplicate vCenter Server names. You must verify that the list of registered vCenter Server systems does not contain duplicate entries.

5 Click **Save**.

What to do next

- Start collecting events, tasks, and alarms data from the vCenter Server instance that you registered. See "Configure Log Insight to Pull Events, Tasks, and Alarms from vCenter Server Instance," on page 21.
- Start collecting syslog feeds from the ESXi hosts that the vCenter Server manages. See "Configure an ESXi Host to Forward Log Events to Log Insight," on page 22.

Configure Log Insight to Pull Events, Tasks, and Alarms from vCenter Server Instance

Events, tasks, and alerts are structured data with specific meaning. You can configure Log Insight to collect alarms, events, and tasks data from one or more vCenter Server systems.

You use the Administration UI to configure Log Insight to connect to vCenter Server systems. The information is pulled from the vCenter Server systems by using the Log Insight API, and appears as a vSphere content pack in the Log Insight Web user interface.

NOTE Log Insight can pull alarms, events, and tasks data only from vCenter Server 5.1 and later.

Prerequisites

Verify that you have user credentials with **System.View** privileges.

NOTE You must configure the permission on the top-level folder within the vCenter Server inventory, and verify that the **Propagate to children** check box is selected.

Procedure

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

2 Under Integration, click **vSphere**.

3 Locate the vCenter Server instance from which you want to collect data, and select the **Collect vCenter Server events, tasks, and alarms** check box.

4 Click **Save**.

Log Insight connects to the vCenter Server every two minutes and ingests all new information since the last successful poll.

What to do next

- Analyze vSphere events using the vSphere content pack or custom queries.
- Enable vSphere content pack alerts or custom alerts.

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.

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 26.

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**.

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 22 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 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 22 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.

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 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.

To configure ESXi hosts to forward their logs to Log Insight, see the topic *Connect Log Insight to vCenter Server 5.1.x Systems* in the Log Insight Administration Guide.

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.

Configure Log Insight to Send Notification Events to vCenter Operations Manager

You can configure Log Insight to send alert notifications to vCenter Operations Manager.

You can integrate Log Insight with vCenter Operations Manager vApp and vCenter Operations Manager Installable. Integrating with the Installable version requires additional changes to the vCenter Operations Manager configuration. For information about configuring vCenter Operations Manager Installable to integrate with Log Insight, see the *Log Insight Getting Started Guide*.

Integrating Log Insight alerts with vCenter Operations Manager allows you to view all information about your environment in a single user interface.

You can send notification events from multiple Log Insight instances to a single vCenter Operations Manager instance. You can enable launch in context for a single Log Insight instance per vCenter Operations Manager instance.

Prerequisites

- Verify that the version of vCenter Operations Manager supports alert notifications from Log Insight. For more information about supported product versions, see topic Product Compatibility in the *Log Insight Getting Started Guide*.

  NOTE Log Insight does not check the version of the target vCenter Operations Manager and lets you proceed with the configuration of the notifications. However, the notification events might not appear as expected in the vCenter Operations Manager user interface.

- 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.

- Verify that you know the IP address or host name of the target vCenter Operations Manager instance.
- 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 Integration, select **vCenter Operations Manager**.

3 Type the IP address or host name, and user credentials for the UI VM of the vCenter Operations Manager instance, and click **Test Connection** .

Log Insight uses the credentials to push notification events to vCenter Operations Manager.

4 In the vCenter Operations Manager pane, select **Enable alerts integration**.

5 Click **Save**.

What to do next

You can configure alert queries to send notification events to vCenter Operations Manager. See topic Add an Alert Query in Log Insight to Send Notification Events to vCenter Operations Manager in the *Log Insight User's Guide*.

Log Insight Notification Events in vCenter Operations Manager

You can configure Log Insight to send notification events to vCenter Operations Manager based on the alert queries that you create.

When you configure a notification alert in Log Insight, you select a resource in vCenter Operations Manager that is associated with the notification events. See the topic Add an Alert Query in Log Insight to Send Notification Events to vCenter Operations Manager in the *Log Insight User's Guide*.

The location of Log Insight notification events depends on the vCenter Operations Manager user interface version that you use.

Table 1-1. Sections of the vCenter Operations Manager User Interface Where Notification Events Appear

vCenter Operations Manager User Interface	Section that Displays Log Insight Notification Events
Custom user interface	■ The Alerts Overview page ■ All dashboards that display the Alerts dashboard widget
vSphere user interface	■ The **Events** tab under the **Operations** tab ■ The **Events** tab under the **Planning** tab

The alert name and description that you provided in Log Insight appear in the Alert Info column of the alert lists in vCenter Operations Manager.

In the Custom user interface, the Alert Info column is not visible by default. You can enable the Alert Info column by expanding the drop-down menu in the table header and selecting the **Alert Info** check box.

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 start 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, for 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 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 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. 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, enable launch in context from the Administration Web user interface of Log Insight.

See the topic *Enable Launch in Context for Log Insight in vCenter Operations Manager* in the *Log Insight Administration Guide*.

vCenter Operations Manager Content Pack for Log Insight

The vCenter Operations Manager content pack for Log Insight contain dashboards, extracted fields, saved queries, and alerts that are used to analyze all logs redirected from a vCenter Operations Manager instance.

The vCenter Operations Manager content pack provides a way to analyze all logs redirected from a vCenter Operations Manager instance. The content pack contains dashboards, queries and alerts to provide diagnostics and troubleshooting capabilities to the vCenter Operations Manager administrator. The dashboards are grouped according to the major components of vCenter Operations Manager like Analytics, UI, and Adapters to provide better manageability. You can enable various alerts to send notification events in vCenter Operations Manager and e-mails to administrators.

NOTE The vCenter Operations Manager content pack requires Log Insight version 1.5 and vCenter Operations Manager verison 5.8.

You can download the vCenter Operations Manager content pack from https://solutionexchange.vmware.com/store/loginsight.

See topic Working with Content Packs in *Log Insight User's Guide*.

Enable Launch in Context for Log Insight in vCenter Operations Manager

You can configure vCenter Operations Manager to display menu items related to Log Insight and launch Log Insight with an object-specific query.

You can integrate Log Insight with vCenter Operations Manager vApp and vCenter Operations Manager Installable. Integrating with the Installable version requires additional changes to the vCenter Operations Manager configuration. For information about configuring vCenter Operations Manager Installable to integrate with Log Insight, see the *Log Insight Getting Started Guide*.

IMPORTANT One instance of vCenter Operations Manager supports launch in context for only one instance of Log Insight. Because Log Insight does not check whether other instances are already registered with vCenter Operations Manager, you might override the settings of another user.

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.
- 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.

- Verify that the version of vCenter Operations Manager is 5.7.1 or later.

  NOTE Log Insight does not check the version of the target vCenter Operations Manager and allows you to proceed. However, vCenter Operations Manager 5.7.1 or later is required for the link back to Log Insight to work and open the alert that generated the notification event.

  For more information about supported product versions, see the topic Product Compatibility in the *Log Insight Getting Started Guide*.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Integration, select **vCenter Operations Manager**.
3. Type the IP address or host name, and user credentials for the UI VM of the vCenter Operations Manager vApp, and click **Test Connection** .

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

4. Select the **Enable Launch in Context** check box.
5. Click **Save**.

Log Insight configures the vCenter Operations Manager instance. This operation might take a few minutes.

Items related to Log Insight appear in the menus of vCenter Operations Manager.

What to do next

Launch a Log Insight query from the vCenter Operations Manager instance. See "Log Insight Launch in Context," on page 31

Log Insight Launch in Context

You can configure vCenter Operations Manager 5.7.1 or later to trigger actions related to Log Insight.

When you enable launch in context for Log Insight, a Log Insight resource is created under the HTTP Post adapter in vCenter Operations Manager. The resource identifier contains the IP address of the Log Insight instance, and is used by vCenter Operations Manager to open Log Insight.

Launch in Context in the vSphere User Interface of vCenter Operations Manager

The launch in context options that are related to Log Insight appear in the **Actions** drop-down menu of the vSphere user interface. You can use these menu items to open Log Insight, and search for log events from an object in vCenter Operations Manager.

The available launch in context action depends on the object that you select in vCenter Operations Manager inventory. The time range of the queries is limited to 60 minutes before you click a launch in context option.

Table 1-2. Objects in vCenter Operations Manager vSphere UI and their Corresponding Launch in Context Options and Actions

Object selected in vCenter Operations Manager	Launch in Context Option in the Actions Drop-Down Menu	Action in vCenter Operations Manager	Action in Log Insight
World	**Open vCenter Log Insight**	Opens Log Insight.	Log Insight displays the **Interactive Analytics** tab.
vCenter Server	**Open vCenter Log Insight**	Opens Log Insight.	Log Insight displays the **Interactive Analytics** tab.

Table 1-2. Objects in vCenter Operations Manager vSphere UI and their Corresponding Launch in Context Options and Actions (Continued)

Object selected in vCenter Operations Manager	Launch in Context Option in the Actions Drop-Down Menu	Action in vCenter Operations Manager	Action in Log Insight
Datacenter	**Search for logs in vCenter Log Insight**	Opens Log Insight and passes the resource names of all host systems under the selected Datacenter object.	Log Insight displays the **Interactive Analytics** tab and performs a query to find log events that contain names of hosts within the data center.
Cluster	**Search for logs in vCenter Log Insight**	Opens Log Insight and passes the resource names of all host systems under the selected Cluster object.	Log Insight displays the **Interactive Analytics** tab and performs a query to find log events that contain names of hosts within the cluster.
Host System	**Search for logs in vCenter Log Insight**	Opens Log Insight and passes the resource name of the selected Host object.	Log Insight displays the **Interactive Analytics** tab and performs a query to find log events that contain the name of the selected Host system.
Virtual Machine	**Search for logs in vCenter Log Insight**	Opens Log Insight and passes the IP address of the selected virtual machine and the resource name of the related host system.	Log Insight displays the **Interactive Analytics** tab and performs a query to find log events that contain the IP address of the virtual machine, and the name of the host where the virtual machine resides.

On the **Alerts** tab, if you select an alert and select **Search for logs in Log Insight** from the in-context menu, the time range of the query is limited to one hour before the alert is triggered. For example, if an alert was triggered at 2:00 PM, the query in Log Insight displays all log messages that occurred between 1:00 PM and 2:00 PM. This helps you identify events that might have triggered the alert.

You can open Log Insight from metric charts in vCenter Operations Manager. The time range of the query thatLog Insight runs matches the time range of the metric chart.

NOTE The time that you see in Log Insight and vCenter Operations Manager metric charts might differ if the time setting of the virtual appliances is different.

Launch in Context in the Custom User Interface of vCenter Operations Manager

The launch in context icon  appears on several pages of the Custom user interface, but you can launch Log Insight only from the pages that display Log Insight notification events:

- The Alerts Overview page.
- The Alert Summary page of a Log Insight notification alert.
- The Alerts widgets on your dashboards, when a Log Insight notification alert is selected.

When you select a Log Insight notification event in the Custom user interface, you can choose between two launch in context actions.

Table 1-3. Launch in Context Options and Actions in vCenter Operations Manager Custom UI

Launch in Context Option in vCenter Operations Manager	Action in vCenter Operations Manager	Action in Log Insight
Open vCenter Log Insight	Opens Log Insight.	Log Insight displays the **Dashboards** tab and loads the vSphere Overview dashboard.
Search for Logs in vCenter Log Insight	Opens Log Insight and passes the ID of the query that triggered the notification event.	Log Insight displays the **Interactive Analytics** tab and performs the query that triggered the notification event.

When you select an alert that has not originated from Log Insight, the launch in context menu contains the **Search for VM and Host Logs in vCenter Log Insight** menu item. If you select this menu item, vCenter Operations Manager opens Log Insight and passes the identifiers of the object that triggered the alert. Log Insight uses the resource identifiers to perform a search in the available log events.

Disable Launch in Context for Log Insight in vCenter Operations Manager

You can uninstall the Log Insight adapter from the vCenter Operations Manager instance to remove menu items related to Log Insight from the vCenter Operations Manager user interface.

You use the Administration UI of Log Insight to disable launch in context. If you do not have access to Log Insight or if the Log Insight instance is deleted before the connection with vCenter Operations Manager is disabled, you can unregister Log Insight from the Administration UI of vCenter Operations Manager. See the Help in the vCenter Operations Manager Administration portal.

CAUTION One instance of vCenter Operations Manager supports launch in context for only one instance of Log Insight. If another instance of Log Insight has been registered after you registered the instance that you want to disable, the second instance overrides the settings of the first one without notifying you.

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 Integration, select **vCenter Operations Manager**.
3. Deselect the **Enable Launch in Context** check box.
4. Click **Save**.

Log Insight configures the vCenter Operations Manager instance to remove the Log Insight adapter. This operation might take a few minutes.

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.

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 38.

What to do next

After Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in Log Insight. For troubleshooting, see topic *ESXi Logs Stop Arriving in Log Insight* in the *Log Insight Administration Guide*.

Enable User Authentication Through Active Directory

Log Insight has a built-in authentication method that you can use to authenticate users.

When you create new user accounts by using the built-in authentication method, you provide users with passwords that they must use to log in to Log Insight.

To avoid having users remember multiple passwords, you can enable the support for Active Directory authentication.

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 Configuration, click **Authentication**.

3 Select the **Enable Active Directory support** check box.

4 In the **Default Domain** text box, type a domain name.

For example, **`company-name.com`**.

NOTE You cannot list multiple domains in the default domain text box. If the default domain that you specify is trusted by other domains, Log Insight uses the default domain and the binding user to verify AD users and groups in the trusting domains .

5 Type the credentials of a binding user that belongs to the default domain.

Log Insight uses the default domain and the binding user to verify AD users and groups in the default domain, and in domains that trust the default domain.

6 Click **Save**.

What to do next

Give permissions to AD users and groups to access the current instance of Log Insight. See "Add an Active Directory User to Log Insight," on page 13.

Configure the Protocol to Use for Active Directory

By default, when Log Insight connects to Active Directory, it first tries non-SSL LDAP, and then SSL LDAP if necessary.

If you want to limit the Active Directory communication to one particular protocol, or want to change the order of protocols that are tried, you must apply additional configurations in the Log Insight virtual appliance.

Prerequisites

- Verify that you have the root user credentials to log in to the Log Insight virtual appliance. See "Configure the Root SSH Password for the Log Insight Virtual Appliance," on page 8
- To enable SSH connections, 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 Open the `/usr/lib/loginisight/application/etc/loginsight-config-base.xml` file for editing.

If you use a VI editor, the command is `vi loginsight-config-base.xml`.

3 In the `Authentication` section, add the line that corresponds to the configuration that you want to apply:

Option	Description
`<ad-protocols value="LDAP" />`	For specifically using LDAP without SSL
`<ad-protocols value="LDAPS" />`	For specifically using LDAP with SSL only
`<ad-protocols value="LDAP,LDAPS" />`	For specifically using LDAP first and then using LDAP with SSL.
`<ad-protocols value="LDAPS,LDAP" />`	For specifically using LDAPS first and then using LDAP without SSL

When you do not select a protocol, Log Insight attempts to use LDAP first, and then uses LDAP with SSL.

4 Save and close the file.

5 Run the `service loginsight restart` command.

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

After Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in Log Insight. For troubleshooting, see topic *ESXi Logs Stop Arriving in Log Insight* in the *Log Insight Administration Guide*.

Change the Default Timeout Period for Log Insight Web Sessions

By default, to keep your environment secure, Log Insight Web sessions expire in 30 minutes. You can increase or decrease the timeout duration.

You can modify the timeout period by using the vSphere Client, or by establishing a 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. See "Configure the Root SSH Password for the Log Insight Virtual Appliance," on page 8
- To enable SSH connections, 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 Run the `service loginsight stop` command.

3 Open the `/usr/lib/loginisight/application/3rd_party/apache-tomcat-*/webapps/ROOT/WEB-INF/web.xml` file for editing.

4 Locate the `<session-timeout>` parameter.

5 Specify a timeout value in minutes.

The value `-1` disables session timeouts.

6 Save and close the file.

7 Run the `service loginsight start` command.

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.

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

After Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in Log Insight. For troubleshooting, see topic *ESXi Logs Stop Arriving in Log Insight* in the *Log Insight Administration Guide*.

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.

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 li-info@vmware.com.

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 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**.

Log Insight stops sending trace data to VMware.

Troubleshooting Log Insight 2

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 2-1. 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 11.

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

2 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' and domain='';"`
```

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.

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

NOTE Do not change this password.

4 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.

5 To update the admin user record, run the following command.

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

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.

Index

R

S

T

U

V