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
Contents

About vRealize Log Insight Administration Guide  5

1 Upgrading vRealize Log Insight  7
   vRealize Log Insight Upgrade Path  7
   Upgrading to vRealize Log Insight 3.0  7
   Upgrading to vRealize Log Insight 2.5 and Earlier Releases  8

2 Configuring vRealize Log Insight  13
   vRealize Log Insight 3.0 Configuration Limits  13
   Configure the Root SSH Password for the Log Insight Virtual Appliance  14
   Change the Network Settings of the vRealize Log Insight vApp  15
   Assign a Permanent License to vRealize Log Insight  15
   Log Storage Policy  16
   Increase the Storage Capacity of the vRealize Log Insight Virtual Appliance  16
   Enable or Disable Data Archiving in vRealize Log Insight  17
   Configure vRealize Log Insight System Alerts  18
   Synchronize the Time on the vRealize Log Insight Virtual Appliance  24
   Configure the SMTP Server for vRealize Log Insight  25
   Install a Custom SSL Certificate by Using the vRealize Log Insight Web Interface  26
   Change the Default Timeout Period for vRealize Log Insight Web Sessions  33
   Format of the vRealize Log Insight Archive Files  33
   Import a vRealize Log Insight Archive into vRealize Log Insight  33
   Export a Log Insight Archive to a Raw Text File or JSON  34
   Add vRealize Log Insight Event Forwarding Destination  35
   Configure vRealize Log Insight Event Forwarding with SSL  36
   Restart the vRealize Log Insight Service  37
   Power Off the vRealize Log Insight Virtual Appliance  37
   Add Memory and CPU to the vRealize Log Insight Virtual Appliance  38
   Stop Sending Trace Data to VMware  38

3 Configuring vRealize Log Insight Clusters  39
   Add a Worker Node to a vRealize Log Insight Cluster  39
   Remove a Worker Node from a vRealize Log Insight Cluster  42
   Enable Integrated Load Balancer  43

4 Configuring vRealize Log Insight Agents  45
   Monitor the Status of the vRealize Log Insight Windows and Linux Agents  45
   Working with Agent Groups  45

5 Managing vRealize Log Insight User Accounts  49
   User Management Overview  49
About vRealize Log Insight Administration Guide

The vRealize Log Insight Administration Guide provides information about administering VMware® vRealize™ Log Insight™, including how to manage user accounts and how to integrate Log Insight Agents with other VMware products. It also includes information used to troubleshoot Log Insight Agents.

Intended Audience

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

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.
Upgrading vRealize Log Insight

Depending on the current version of vRealize Log Insight, you can upgrade to a newer version.

This chapter includes the following topics:

- “vRealize Log Insight Upgrade Path,” on page 7
- “Upgrading to vRealize Log Insight 3.0,” on page 7
- “Upgrading to vRealize Log Insight 2.5 and Earlier Releases,” on page 8

vRealize Log Insight Upgrade Path

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

<table>
<thead>
<tr>
<th>Installed Version</th>
<th>Upgrade Version</th>
<th>Upgrade Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Log Insight 2.5</td>
<td>vRealize Log Insight 3.0</td>
<td>See “Upgrading to vRealize Log Insight 3.0,” on page 7</td>
</tr>
<tr>
<td>vRealize Log Insight 2.0</td>
<td>vRealize Log Insight 2.5</td>
<td>See “Upgrade a Worker Node in a vRealize Log Insight Cluster,” on page 8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Upgrade vRealize Log Insight 1.5 GA and later by Using the Web Interface,” on page 10</td>
</tr>
<tr>
<td>vRealize Log Insight 1.5</td>
<td>vRealize Log Insight 2.0</td>
<td>See “Upgrade a Worker Node in a vRealize Log Insight Cluster,” on page 8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Upgrade vRealize Log Insight 1.5 GA and later by Using the Web Interface,” on page 10</td>
</tr>
</tbody>
</table>

Upgrading to vRealize Log Insight 3.0

You can automatically upgrade a cluster to vRealize Log Insight 3.0.

If using the integrated load balancer, navigate to the load balancer address, otherwise navigate to the master node address.

**Prerequisites**

- Verify you are upgrading from vRealize Log Insight 2.5 GA.
- Create a snapshot or backup copy of the Log Insight virtual appliance.
- Obtain a copy of the vRealize Log Insight 3.0 upgrade bundle .pok file.
Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select Administration.
2. Under Management, click Appliance.
3. Click Upgrade from PAK to upload the .pak file.
4. Accept the new EULA to complete the upgrade procedure.

What to do next

After the master node upgrade process is complete, you can view the remaining upgrade process which is automatic.

Check for the email sent to the Admin to confirm the upgrade completed successfully.

Upgrading to vRealize Log Insight 2.5 and Earlier Releases

You can upgrade to vRealize Log Insight 2.5 and earlier releases.

Depending on the current version, you can upgrade to vRealize Log Insight 2.x using the CLI or the web interface.

Upgrade a Worker Node in a vRealize Log Insight Cluster

You can upgrade one or more worker nodes in a vRealize Log Insight cluster.

The vRealize Log Insight master node updates worker nodes centrally through the Web user interface.

IMPORTANT Always add or upgrade vRealize Log Insight cluster nodes sequentially. Do not add or upgrade worker nodes in parallel because it might cause consistency problems.

Prerequisites

- Create a snapshot or backup copy of the Log Insight virtual appliance.
- Obtain a copy of the vRealize Log Insight upgrade bundle .pak file.
- Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.
- Upgrade the master node of the vRealize Log Insight cluster. See “Upgrade vRealize Log Insight 1.5 GA and later by Using the Web Interface,” on page 10.
- If you use an external load balancer, take the node off the balancer before you put it in maintenance mode.

Procedure

1. Click the configuration drop-down menu icon and select Administration.
2. Under Management, click Cluster.
3 In the Workers table, find the node you want, click , and click Continue.

The node is now in maintenance mode.

**Note** A node in maintenance mode continues to receive logs.

4 Click and then click Upgrade worker to confirm.

**Note** The icon is only available for workers that run earlier versions than the master. The icon is not visible after the worker successfully upgrades to the version of the master.

When the upgrade completes, the worker restarts and reconnects to the cluster.

**What to do next**
Upgrade the remaining worker nodes in your vRealize Log Insight cluster.

### Upgrade vRealize Log Insight by Using CLI

Because vRealize 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 vRealize Log Insight versions 1.5 TP2 and later, use the Administration user interface for upgrades. See “Upgrade vRealize Log Insight 1.5 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 vRealize 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 14.
- Create a snapshot or backup copy of the Log Insight virtual appliance.
- Obtain a copy of the vRealize Log Insight upgrade bundle .rpm file.

**Procedure**

1 Download the .rpm file to a host that has SSH access to the vRealize Log Insight virtual appliance.
2 Use the secure copy protocol to copy the .rpm file to the vRealize Log Insight virtual appliance.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Command/Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>scp path to the RPM file/loginsight-cloudvm-version-log-insight-buildnumber.x86_64.rpm root@&lt;LogInsightIPorHostname&gt;:/~</td>
</tr>
<tr>
<td>Windows</td>
<td>For Windows systems, download an SCP client like WinSCP.</td>
</tr>
</tbody>
</table>

3 Use the vSphere Client console to log in to the vRealize 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 vRealize 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 vRealize Log Insight 1.5 by Using the Web Interface**

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

**Note** All active users of the vRealize 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 vRealize Log Insight upgrade bundle `.rpm` file.
- Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the `Edit` Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

**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.
   vRealize 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.

**Upgrade vRealize Log Insight 1.5 GA and later by Using the Web Interface**

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

**Note** All active users of the vRealize 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 vRealize Log Insight upgrade bundle `.pak` file.
- Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the `Edit` Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

**Procedure**
1. Click the configuration drop-down menu icon and select Administration.
2. Under Management, click Appliance.
3 Click **Upload PAK**, and browse to the .pak file.

4 Click **Upgrade**.

   vRealize Log Insight uploads the .pak 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.

**What to do next**

You can deploy a new instance of the vRealize Log Insight virtual appliance and add it to the existing vRealize Log Insight node to form a cluster. The existing node becomes a master node and the newly deployed vRealize Log Insight instance becomes a worker node. See “Add a Worker Node to a vRealize Log Insight Cluster,” on page 39.
Configuring vRealize Log Insight

You can configure and customize vRealize Log Insight to change default settings, network settings, and modify storage resources. You can also configure system alerts.

This chapter includes the following topics:

- “vRealize Log Insight 3.0 Configuration Limits,” on page 13
- “Configure the Root SSH Password for the Log Insight Virtual Appliance,” on page 14
- “Change the Network Settings of the vRealize Log Insight vApp,” on page 15
- “Assign a Permanent License to vRealize Log Insight,” on page 15
- “Log Storage Policy,” on page 16
- “Increase the Storage Capacity of the vRealize Log Insight Virtual Appliance,” on page 16
- “Enable or Disable Data Archiving in vRealize Log Insight,” on page 17
- “Configure vRealize Log Insight System Alerts,” on page 18
- “Synchronize the Time on the vRealize Log Insight Virtual Appliance,” on page 24
- “Configure the SMTP Server for vRealize Log Insight,” on page 25
- “Install a Custom SSL Certificate by Using the vRealize Log Insight Web Interface,” on page 26
- “Change the Default Timeout Period for vRealize Log Insight Web Sessions,” on page 33
- “Format of the vRealize Log Insight Archive Files,” on page 33
- “Import a vRealize Log Insight Archive into vRealize Log Insight,” on page 33
- “Export a Log Insight Archive to a Raw Text File or JSON,” on page 34
- “Add vRealize Log Insight Event Forwarding Destination,” on page 35
- “Configure vRealize Log Insight Event Forwarding with SSL,” on page 36
- “Restart the vRealize Log Insight Service,” on page 37
- “Power Off the vRealize Log Insight Virtual Appliance,” on page 37
- “Add Memory and CPU to the vRealize Log Insight Virtual Appliance,” on page 38
- “Stop Sending Trace Data to VMware,” on page 38

vRealize Log Insight 3.0 Configuration Limits

When you configure vRealize Log Insight, you must stay at or below the supported maximums.

These configuration limits apply to vRealize Log Insight 3.0.
### Table 2-1. vRealize Log Insight 3.0 Configuration Maximums

<table>
<thead>
<tr>
<th>Item</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>16 vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>32 GB</td>
</tr>
<tr>
<td>Storage device (vmdk)</td>
<td>2 TB - 512 bytes</td>
</tr>
<tr>
<td>Total addressable storage</td>
<td>4 TB (+ OS drive)</td>
</tr>
<tr>
<td>Syslog connections</td>
<td>750</td>
</tr>
<tr>
<td><strong>Cluster Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Nodes</td>
<td>12 (Master + 11 Workers)</td>
</tr>
<tr>
<td><strong>Ingestion per Node</strong></td>
<td></td>
</tr>
<tr>
<td>Events per second</td>
<td>15,000 eps</td>
</tr>
<tr>
<td>Syslog message length</td>
<td>10 KB (text field)</td>
</tr>
<tr>
<td>Ingestion API HTTP POST request</td>
<td>16 KB (text field); 4 MB per HTTP POST request</td>
</tr>
<tr>
<td>Windows event log channels</td>
<td>60</td>
</tr>
<tr>
<td><strong>Integrations</strong></td>
<td></td>
</tr>
<tr>
<td>vRealize Operations Manager</td>
<td>1</td>
</tr>
<tr>
<td>vSphere vCenter Server</td>
<td>10</td>
</tr>
<tr>
<td>Active Directory domains</td>
<td>1</td>
</tr>
<tr>
<td>Email servers</td>
<td>1</td>
</tr>
<tr>
<td>DNS servers</td>
<td>2</td>
</tr>
<tr>
<td>NTP servers</td>
<td>4</td>
</tr>
<tr>
<td>Forwarders</td>
<td>10</td>
</tr>
</tbody>
</table>

---

**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 vRealize Log Insight virtual appliance is deployed and running.

**Procedure**

1. In the vSphere Client inventory, click the vRealize 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 vRealize Log Insight virtual appliance.

### Change the Network Settings of the vRealize Log Insight vApp

You can change the network settings of the vRealize Log Insight virtual appliance by editing the vApp properties in the vSphere Client.

**Prerequisites**

Verify that you have permissions to edit vApp properties.

**Procedure**

1. Power off the vRealize Log Insight vApp.
2. Right-click the vRealize Log Insight vApp in the inventory and click **Edit Settings**.
3. Click the Options tab and select vApp Options > IP Allocation Policy.
4. Select an IP allocation option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed</td>
<td>IP addresses are manually configured. No automatic allocation is performed.</td>
</tr>
<tr>
<td>Transient</td>
<td>IP addresses are automatically allocated using IP pools from a specified range when the vApp is powered on. The IP addresses are released when the appliance is powered off.</td>
</tr>
<tr>
<td>DHCP</td>
<td>A DHCP server is used to allocate the IP addresses. The addresses assigned by the DHCP server are visible in the OVF environments of virtual machines started in the vApp.</td>
</tr>
</tbody>
</table>

5. (Optional) If you select Fixed, click vApp Options > Properties and assign an IP address, netmask, gateway, DNS and host name for the vRealize Log Insight vApp.

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


### Assign a Permanent License to vRealize Log Insight

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

You obtain an evaluation license when you download vRealize 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 vRealize Log Insight.

You use the Administration section of the vRealize Log Insight Web user interface to check the vRealize 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 vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is https://log-insight-host, where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

**Procedure**

1. Click the configuration drop-down menu icon \( \equiv \) 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.

**Log Storage Policy**

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

When the volume of logs imported into vRealize 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 vRealize Log Insight. See “Enable or Disable Data Archiving in vRealize Log Insight,” on page 17.

Data stored by vRealize 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 vRealize Log Insight Virtual Appliance**

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

You increase the storage space by adding a new virtual disk to the vRealize 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 vRealize Log Insight virtual appliance safely. See “Power Off the vRealize Log Insight Virtual Appliance,” on page 37.

**Procedure**

1. In the vSphere Client inventory, right-click the vRealize 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.
   vRealize Log Insight supports virtual hard disks of up to 2 TB. If you need more capacity, add more than one virtual hard disk.
   b Select a disk format.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Thick Provision Lazy Zeroed</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Thick Provision Eager Zeroed</strong></td>
<td>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 vRealize Log Insight virtual appliance.</td>
</tr>
<tr>
<td><strong>Thin Provision</strong></td>
<td>Creates a disk in thin format. Use this format to save storage space.</td>
</tr>
</tbody>
</table>

c 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 vRealize 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 vRealize Log Insight virtual appliance may result in complete data loss.

---

### Enable or Disable Data Archiving in vRealize Log Insight

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

vRealize Log Insight collects and stores logs on disk in a series of 1 GB buckets. A bucket consists of compressed log files and an index. A bucket contains everything necessary to perform queries for a specific time range. When the size of the bucket exceeds 1 GB in size, vRealize Log Insight stops writing, closes all files in the bucket and seals the bucket.

When data archiving is enabled, vRealize Log Insight copies the raw compressed log files from the bucket to an NFS mount when the bucket is sealed. Buckets that have been sealed prior to enabling data archiving are not retroactively archived.

**Note** vRealize Log Insight does not manage the NFS mount used for archiving purposes. If system notifications are enabled, vRealize 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, vRealize 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.
  - If using a Windows NFS server, allow unmapped user Unix access (by UID/GID).
- Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Configuration, click **Archiving**.
3. Select the **Enable Data Archiving** check box, enter the path to an NFS partition where logs will be archived in the form nfs://servername/sharename.
4. Click **Test** to verify the connection.
5. Click **Save**.

**Note** Data archiving preserves log events that have since been removed from the vRealize Log Insight virtual appliance due to storage constraints. Log events that have been removed from the vRealize 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 vRealize Log Insight instance. For more information about importing archived log files, see “Import a vRealize Log Insight Archive into vRealize Log Insight,” on page 33.

What to do next

After vRealize Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in vRealize Log Insight. For troubleshooting, see ESXi Logs Stop Arriving in Log Insight.

Configure vRealize Log Insight System Alerts

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

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

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize 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.

**About vRealize Log Insight Email Notifications and Alerts**

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

Administrators can configure vRealize 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 vRealize Log Insight,” on page 25.

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

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

Administrator users can disable all user defined notifications.

<table>
<thead>
<tr>
<th>Type</th>
<th>Alert Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Oldest Data Will Be Unsearchable Soon</td>
<td>This alert notifies you when vRealize 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 vRealize Log Insight service.</td>
</tr>
<tr>
<td>System</td>
<td>Repository Retention Time</td>
<td>This alert notifies you about the amount of searchable data that vRealize Log Insight can store at the current ingest rate and in the storage space that is available on the virtual appliance. Admin users can define the storage notification threshold. See “Configure vRealize Log Insight System Alerts,” on page 18.</td>
</tr>
<tr>
<td>Type</td>
<td>Alert Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| System   | Dropped Events          | This alert notifies you that vRealize Log Insight failed to ingest all incoming log messages.  
- In case of any TCP Message drops, as tracked by vRealize Log Insight server, a system alert is sent in both cases as follows:  
  - Once a day  
  - Each time the vRealize 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 vRealize 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. vRealize Log Insight checks the integrity of the index upon service start-up. In case of detected corruption vRealize Log Insight sends a system alert as follows:  
  - Once a day  
  - Each time the vRealize Log Insight service is restarted, manually or automatically. |
<p>| System   | Out Of Disk             | This alert notifies you that vRealize Log Insight is running out of allocated disk space. This alert signals that vRealize 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 vRealize Log Insight data will be used up soon.                                                                                                                                                                                                                                                                                                           |
| System   | Archive Failure         | This alert notifies you that an operation of archiving vRealize Log Insight data to the NFS server has failed. This usually means that vRealize Log Insight is having trouble connecting to or writing to the NFS server.                                                                                                                                                                                                                                           |</p>
<table>
<thead>
<tr>
<th>Type</th>
<th>Alert Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| System      | Total Disk Space Change                        | This alert notifies you that the total size of the partition for vRealize Log Insight data storage has decreased. This usually signals a serious issue in the underlying storage system. When vRealize Log Insight detects the condition it sends this alert as follows:  
  - Immediately  
  - Once a day |
<p>| System      | Pending Archivings                              | This alert notifies you that vRealize Log Insight cannot archive data as expected. The alert usually indicates problems with the NFS storage that you configured for data archiving. |
| System      | License is about to be expired                  | This alert notifies you that the vRealize Log Insight is about to expire.                                                                                                                                      |
| System      | License is expired                              | This alert notifies you that the vRealize Log Insight is to expired.                                                                                                                                               |
| System      | Unable to connect to AD server                  | This alert notifies you that vRealize Log Insight is unable to connect to the configured Active Directory server.                                                                                               |
| System      | Cannot take over High Availability IP address [IP Address] as it is already held by another machine | This alert notifies you that the Log Insight cluster was unable to take over the configured IP Address for the Integrated Load Balancer (ILB). The most common reason for this notification is that another host within the same network holds the IP address, and therefore the IP address is not available to be taken over by the Log Insight cluster. You can resolve this conflict by either releasing the IP address from the host that currently holds it, or configuring Log Insight Integrated Load Balancer with a Static IP address that is available in the network. When changing the ILB IP address, remember to reconfigure all clients to send logs to the new IP address, or to a FQDN/URL that resolves to this IP address. You must also unconfigure and reconfigure every vCenter Server integrated with Log Insight from the vSphere integration page. |</p>
<table>
<thead>
<tr>
<th>Type</th>
<th>Alert Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>High Availability IP address [IP Address] is unavailable due to too many node failures</td>
<td>This alert notifies you that the IP Address configured for the Integrated Load Balancer (ILB) is unavailable. This means that clients trying to send logs to Log Insight cluster via the ILB IP address or a FQDN/URL that resolves to this IP address will see it as unavailable. The most common reason for this notification is that a majority of the nodes in the Log Insight cluster are unhealthy, unavailable, or unreachable from the master node. Another common reason is that NTP time synchronization has not been enabled, or the configured NTP servers have significant time drift between each other. You can confirm that the problem is still ongoing by trying to ping (if allowed) the IP address and checking if it not reachable. You can resolve this problem by ensuring a majority of your cluster nodes are healthy and reachable, and enabling NTP time synchronization to accurate NTP servers.</td>
</tr>
<tr>
<td>System</td>
<td>Too many migrations of High Availability IP address [IP Address] between Log Insight nodes</td>
<td>This alert notifies you that the IP Address configured for the Integrated Load Balancer (ILB) has migrated too many times within the last 10 minutes. Under normal operation, the IP Address rarely moves between Log Insight cluster nodes. However, the IP Address might move if the current owner node is restarted or put in maintenance. The other reason can be lack of time synchronization between Log Insight cluster nodes, which is essential for proper cluster functioning. In case of latter, you can fix the problem by enabling NTP time synchronization to accurate NTP servers.</td>
</tr>
<tr>
<td>User Defined</td>
<td>Alert Queries</td>
<td>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 Add an Alert Query in Log Insight to Send Email Notifications. See topic Add an Alert Query in Log Insight to Send Email Notifications in the Log Insight User’s Guide.</td>
</tr>
</tbody>
</table>
## Scale Out System Alerts

vRealize Log Insight sends specific system alerts to notify you of scale-out events such as node joining and membership status changes.

<table>
<thead>
<tr>
<th>Sent by</th>
<th>Alert Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master node</td>
<td>Approval needed for new worker node</td>
<td>This alert notifies you of a membership request from a worker node. An Admin user needs to approve or deny the request.</td>
</tr>
<tr>
<td>Master node</td>
<td>New worker node approved</td>
<td>This alert notifies you that an Admin user approved a membership request from a worker node to join a vRealize Log Insight cluster.</td>
</tr>
<tr>
<td>Master node</td>
<td>New worker node denied</td>
<td>This alert notifies you that an Admin user denied a membership request from a worker node to join a vRealize Log Insight cluster. If the request was denied by mistake, an Admin user can place the request again from the worker and then approve it at the master node.</td>
</tr>
<tr>
<td>Master node</td>
<td>Maximum supported nodes exceeded due to worker node</td>
<td>This alert notifies you that the number of worker nodes in the Log Insight cluster has exceeded the maximum supported count due to a new worker node.</td>
</tr>
<tr>
<td>Master node</td>
<td>Allowed nodes exceeded, new worker node denied</td>
<td>This alert notifies you that an Admin user attempted to add more nodes to the cluster than the maximum allowed node count and the node has been denied.</td>
</tr>
<tr>
<td>Master node</td>
<td>Worker node disconnected</td>
<td>This alert notifies you that a previously connected worker node disconnected from the vRealize Log Insight cluster.</td>
</tr>
<tr>
<td>Master node</td>
<td>Worker node reconnected</td>
<td>This alert notifies you that a worker node reconnected to the vRealize Log Insight cluster.</td>
</tr>
<tr>
<td>Master node</td>
<td>Worker node revoked by admin</td>
<td>This alert notifies you that an Admin user revoked a worker node membership and the node is no longer a part of the vRealize Log Insight cluster.</td>
</tr>
<tr>
<td>Master node</td>
<td>Unknown worker node rejected</td>
<td>This alert notifies you that the vRealize Log Insight master node rejected a request by a worker node because the worker node is unknown to the master. If the worker is a valid node and it should be added to the cluster, log in to the worker node, remove its token file and user configuration at <code>/storage/core/loginsight/config/</code>, and run restart <code>loginsight</code> service on the worker node.</td>
</tr>
<tr>
<td>Sent by</td>
<td>Alert Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Master node</td>
<td>Worker node has entered into maintenance mode</td>
<td>This alert notifies you that a worker node entered into maintenance mode and an Admin user has to remove the worker node from maintenance mode before it can receive configuration changes and serve queries.</td>
</tr>
<tr>
<td>Master node</td>
<td>Worker node has returned to service</td>
<td>This alert notifies you that a worker node exited maintenance mode and returned to service.</td>
</tr>
<tr>
<td>Worker node</td>
<td>Master failed or disconnected from worker node</td>
<td>This alert notifies you that a worker node that sends the alert is unable to contact the vRealize Log Insight master node. This might indicate that the master node failed, and might need to be restarted. If the master node failed, the cluster cannot be configured and queries cannot be submitted until it is back online. Worker nodes continue to ingest messages. <strong>Note</strong>: You might receive many such alerts because many workers might detect the master node failure independently and raise notifications.</td>
</tr>
<tr>
<td>Worker node</td>
<td>Master connected to worker node</td>
<td>This alert notifies you that a worker node that sends the alert is reconnected to the vRealize Log Insight master node.</td>
</tr>
</tbody>
</table>

**Synchronize the Time on the vRealize Log Insight Virtual Appliance**

You must synchronize the time on the vRealize 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 vRealize Log Insight.

By default, vRealize 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 vRealize Log Insight virtual appliance.

**Prerequisites**

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP server</td>
<td>Synchronizes the time on the vRealize Log Insight virtual appliance with one of the listed NTP servers.</td>
</tr>
<tr>
<td>ESX/ESXi host</td>
<td>Synchronizes the time on the vRealize Log Insight virtual appliance with the ESX/ESXi host on which you have deployed the virtual appliance.</td>
</tr>
</tbody>
</table>

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 vRealize Log Insight

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

System alerts are generated when vRealize Log Insight detects an important system event, for example when the storage capacity on the virtual appliance reached the thresholds that you set. See “About vRealize Log Insight Email Notifications and Alerts,” on page 19.

**Prerequisites**
Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize 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 uses 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 vRealize 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**.
Install a Custom SSL Certificate by Using the vRealize Log Insight Web Interface

By default, vRealize Log Insight installs a self-signed SSL certificate on the virtual appliance. The self-signed certificate generates security warnings when you connect to the vRealize 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 only feature requiring a custom SSL certificate is Event Forwarding through SSL. If you have a Cluster setup with ILB enabled, see “Enable Integrated Load Balancer,” on page 43 for the specific requirements of a custom SSL certificate.

**Note**  The vRealize Log Insight Web user interface and the Log Insight Ingestion protocol cfapi 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. vRealize 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. vRealize Log Insight does not support certificates in the PFX, PKCS12, PKCS7, or other formats.
- Verify that you concatenate the entire body of each certificate into a single text file in the following order.
  - a  The Private Key - your_domain_name.key
  - b  The Primary Certificate - your_domain_name.crt
  - c  The Intermediate Certificate - DigiCertCA.crt
  - d  The Root Certificate - TrustedRoot.crt
- Verify that you include the beginning and ending tags of each certificate in the following format.

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```
- Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.
**Procedure**

1. **Generate a Self-Signed Certificate** on page 27
   You can generate a self-signed certificate for Windows or Linux by using the OpenSSL tool.

2. **Generate a Certificate Signing Request** on page 28
   Generate a certificate signing request by using the OpenSSL tool for Windows.

3. **Request a Signature from a Certificate Authority** on page 29
   Send your certificate signing request to a Certificate Authority of your choice and request a signature.

4. **Concatenate Certificate Files** on page 29
   Combine your key and certificate files into a PEM file.

5. **Upload Signed Certificate** on page 29
   You can upload a signed SSL certificate.

6. **Configure SSL Connection Between the vRealize Log Insight Server and the Log Insight Agents** on page 30
   SSL function allows you to provide SSL only connections between the Log Insight Agents and the vRealize Log Insight Server through the secure flow of Ingestion API. You can also configure various SSL parameters of the Log Insight Agents.

**Generate a Self-Signed Certificate**

You can generate a self-signed certificate for Windows or Linux by using the OpenSSL tool.

**Prerequisites**

- Download the appropriate installer for OpenSSL from [http://www.openssl.org/related/binaries.html](http://www.openssl.org/related/binaries.html). Use the downloaded OpenSSL installer to install it on Windows.
- Edit the `openssl.cfg` file to add additional required parameters. Make sure the `[req]` section has the `req_extensions` parameter defined.

```plaintext
[req]

. 

req_extensions=v3_req #
```

- Add an appropriate Subject Alternative Name entry for the hostname or IP address of your server, for example `server-01.loginsight.domain`. You cannot specify a pattern for the hostname.

```plaintext
[v3_req]

. 

subjectAltName=DNS:server-01.loginsight.domain
subjectAltName=IP:10.27.74.215
```

**Procedure**

1. Create a folder to save your certificate files, for example `C:\Certs\LI-2.6`.

2. Open a command prompt and run the following command.

   ```bash
   C:\Certs\LI-2.6>openssl req -x509 -nodes -newkey 2048 -keyout server.key -out server.crt -days 3650
   ```

   OpenSSL prompts you to supply certificate properties, including country, organization, and so on.
Enter the exact IP address or hostname of your vRealize Log Insight server, or the vRealize Log Insight cluster address if load balancing is enabled. This property is the only one for which it is mandatory to specify a value.

Two files are created, key.pm and cert.pm.
- key.pm is the PEM encoded private key.
- cert.pm is the self-signed certificate, which is signed by key.pm.

What to do next
- Concatenate the certificate files. See “Concatenate Certificate Files,” on page 29.

Generate a Certificate Signing Request

Generate a certificate signing request by using the OpenSSL tool for Windows.

Prerequisites
- Download the appropriate installer for OpenSSL from http://www.openssl.org/related/binaries.html. Use the downloaded OpenSSL installer to install it on Windows.
- Edit the openssl.cfg file to add additional required parameters. Make sure the [req] section has the req_extensions parameter defined.

```plaintext
[req]
  .
  .
  req_extensions=v3_req #
```
- Add an appropriate Subject Alternative Name entry for the hostname or IP address of your server, for example server-01.loginsight.domain. You cannot specify a pattern for the hostname.

```plaintext
[v3_req]
  .
  .
  subjectAltName=DNS:server-01.loginsight.domain
  #subjectAltName=IP:10.27.74.215
```

Procedure
1. Create a folder to save your certificate files, for example C:\Certs\LogInsight.
2. Open a Command Prompt and run the following command to generate your private key.
   ```plaintext
   C:\Certs\LogInsight>openssl genrsa -out server.key 2048
   ```
3. Create a certificate signing request by running the following command.
   ```plaintext
   C:\Certs\LogInsight>openssl req -new -key server.key -out server.csr
   ```
   **NOTE** This command runs interactively and asks you a number of questions. Your certificate authority will cross check your answers. Your answers must match the legal documents regarding the registration of your company.
4. Follow the onscreen instructions and enter the information that will be incorporated into your certificate request.
   **IMPORTANT** In the Common Name field, enter the hostname or IP address of your server, for example mail.your.domain. If you want to include all subdomains, enter *your.domain.
Your certificate signing request file server.csr is generated and saved.

**Request a Signature from a Certificate Authority**

Send your certificate signing request to a Certificate Authority of your choice and request a signature.

**Procedure**

- Submit your server.csr file to a Certificate Authority.

**NOTE** Request that the Certificate Authority encode your file in the PEM format.

The Certificate Authority processes your request and sends you back a server.crt file encoded in the PEM format.

**Concatenate Certificate Files**

Combine your key and certificate files into a PEM file.

**Procedure**

1. Create a new server.pem file and open it in a text editor.
2. Copy the contents of your server.key file and paste it in server.pem using the following format.

   
   
   
   
   -----BEGIN RSA PRIVATE KEY-----
   (Your Private Key: server.key)
   -----END RSA PRIVATE KEY-----

3. Copy the contents of your server.crt file and paste it in server.pem using the following format.

   
   
   
   
   -----BEGIN CERTIFICATE-----
   (Your Primary SSL certificate: server.crt)
   -----END CERTIFICATE-----

4. If the Certificate Authorities provided you with an intermediate or chained certificate, append the intermediate or chained certificates to the end of the public certificate file in the following format.

   
   
   
   
   -----BEGIN RSA PRIVATE KEY-----
   (Your Private Key: server.key)
   -----END RSA PRIVATE KEY-----
   -----BEGIN CERTIFICATE-----
   (Your Primary SSL certificate: server.crt)
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   (Your Intermediate certificate: DigiCertCA.crt)
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   (Your Root certificate: TrustedRoot.crt)
   -----END CERTIFICATE-----

5. Save your server.pem file.

**Upload Signed Certificate**

You can upload a signed SSL certificate.

**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**.
5. Restart vRealize Log Insight.

**What to do next**

After vRealize Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in vRealize Log Insight. For troubleshooting, see ESXi Logs Stop Arriving in Log Insight.

After vRealize Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in vRealize Log Insight. For troubleshooting, see the topic related to ESXi logs in the Log Insight Administration Guide.

**Configure SSL Connection Between the vRealize Log Insight Server and the Log Insight Agents**

SSL function allows you to provide SSL only connections between the Log Insight Agents and the vRealize Log Insight Server through the secure flow of Ingestion API. You can also configure various SSL parameters of the Log Insight Agents.

**Main SSL Functions**

Understanding of the main SSL functions can help you configure the Log Insight Agents properly.

The vRealize Log Insight Agent stores certificates and uses them to verify the identity of the server during all but the first connection to a particular server. If the server identity cannot be confirmed, the vRealize Log Insight Agent rejects connection with server and writes an appropriate error message to the log. Certificates received by the Agent are stored in `cert` folder.

- For Windows go to `C:\ProgramData\VMware\Log Insight Agent\cert`.
- For Linux go to `/var/lib/loginsight-agent/cert`.

When the vRealize Log Insight Agent establishes secure connection with the vRealize Log Insight Server, the Agent checks the certificate received from the vRealize Log Insight Server for validity. The vRealize Log Insight Agent uses system-trusted root certificates.

- The Log Insight Linux Agent loads trusted certificates from `/etc/pki/tls/certs/ca-bundle.crt` or `/etc/ssl/certs/ca-certificates.crt`.
- The Log Insight Windows Agent uses system root certificates.

If the vRealize Log Insight Agent has a locally stored self-signed certificate and receives a different valid self-signed certificate with the same public key, then the agent accepts the new certificate. This can happen when a self-signed certificate is regenerated using the same private key but with different details like new expiration date. Otherwise, connection is rejected.

If the vRealize Log Insight Agent has a locally stored self-signed certificate and receives valid CA-signed certificate, the vRealize Log Insight Agent silently replaces new accepted certificate.

If the vRealize Log Insight Agent receives self-signed certificate after having a CA-signed certificate, the Log Insight Agent rejects it. The vRealize Log Insight Agent accepts self-signed certificate received from vRealize Log Insight Server only when it connects to the server for the first time.

If the vRealize Log Insight Agent has a locally stored CA-signed certificate and receives a valid certificate signed by another trusted CA, the Agent rejects it. You can modify the configuration options of the vRealize Log Insight Agent to accept the new certificate. See “Configure the vRealize Log Insight Agent SSL Parameters,” on page 31.
Enforce SSL Only Connections

You can use the vRealize Log Insight Web UI to configure the Log Insight Agents and the Ingestion API to allow only SSL connections to the server.

**Note** The current version of vRealize Log Insight doesn't support syslog SSL connections and works only for vRealize Log Insight Ingestion API.

**Prerequisites**

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

**Procedure**

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Configuration, click **SSL**.
3. Under the API Server SSL, select the **Require SSL Connection** check box.
4. Click **Save**.

vRealize Log Insight API allows only SSL connections to the server. Non-SSL connections are refused.

**Configure the vRealize Log Insight Agent SSL Parameters**

You can edit the vRealize Log Insight agent configuration file to change the SSL configuration, add a path to the trusted root certificates, and define whether certificates are accepted by the agent.

This procedure applies to the vRealize Log Insight agents for Windows and Linux.

**Prerequisites**

For the vRealize Log Insight Linux agent:

- Log in as root or use sudo to run console commands.
- Log in to the Linux machine on which you installed the vRealize Log Insight Linux agent, open a console and run `pgrep liagent` to verify that the vRealize Log Insight Linux agent is installed and running.

For the vRealize Log Insight Windows agent:

- Log in to the Windows machine on which you installed the vRealize Log Insight Windows agent and start the Services manager to verify that the VMware vRealize Log Insight agent service is installed.

**Procedure**

1. Navigate to the folder containing the `liagent.ini` file.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>/var/lib/loginsight-agent/</td>
</tr>
<tr>
<td>Windows</td>
<td>%ProgramData%\VMware\Log Insight Agent</td>
</tr>
</tbody>
</table>

2. Open the `liagent.ini` file in any text editor.
Add the following keys to the [server] section of the liagent.ini file.

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssl_ca_path</td>
<td>The path to the trusted root certificates bundle file. If not specified, the vRealize Log Insight Windows agent uses system root certificates. The vRealize Log Insight Linux agent attempts to load trusted certificates from /etc/pki/tls/certs/ca-bundle.crt or /etc/ssl/certs/ca-certificates.crt.</td>
</tr>
<tr>
<td>ssl_accept_any</td>
<td>Defines whether any certificates are accepted by the vRealize Log Insight agent. The possible values are yes, 1, no, or 0. When the value is set to yes or 1, the vRealize Log Insight Agent accepts any certificate from the server and establish secure connection for sending data. The default value is no. If the ssl_accept_any is set to yes or 1, the Log Insight Agent accepts certificates that do not have matching Common Name.</td>
</tr>
<tr>
<td>ssl_accept_any_trusted</td>
<td>The possible values are yes, 1, no, or 0. If the vRealize Log Insight Agent has a locally stored trusted Certificate Authority-signed certificate and receives a different valid certificate signed by a different trusted Certificate Authority it checks the configuration option. If the value is set to yes or 1, the Agent accepts the new valid certificate. If the value is set to no or 0, it rejects the certificate and terminates the connection. The default value is no.</td>
</tr>
<tr>
<td>ssl_cn</td>
<td>The self-signed certificate Common Name. The default value is VMware vCenter Log Insight. You can define a custom Common Name to be checked against the certificate Common Name field. The vRealize Log Insight Agent checks the Common Name field of the received certificate against the host name configured to connect by hostname key in the [server] section. If it does not match, the Agent checks the Common Name field against the ssl_cn key in the liagent.ini file. If the values match, the vRealize Log Insight Agent accepts the certificate.</td>
</tr>
</tbody>
</table>

**Note** The keys are used only if the protocol in the [server] section is set to cfapi and SSL is enabled.

Save and close the liagent.ini file.

**Example: Configuration**

The following is an example of the SSL configuration.

```ini
proto=cfapi
port=9543
ssl=yes
ssl_ca_path=/etc/pki/tls/certs/ca-bundle.crt
ssl_accept_any=no
ssl_accept_any_trusted=yes
ssl_cn=LOGINSIGHT
```
Change the Default Timeout Period for vRealize Log Insight Web Sessions

By default, to keep your environment secure, vRealize 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 Web UI.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select Administration.
2. Under Configuration, click General.
3. In the Browser Session pane, specify a timeout value in minutes.
   - The value -1 disables session timeouts.
4. Click Save.

Format of the vRealize Log Insight Archive Files

vRealize Log Insight archives data in a specific format.

vRealize Log Insight stores archive files on an NFS server and organizes them in hierarchical directories based on archiving time. For example,

```
/backup/2014/08/07/16/bd234b2d-df98-44ae-991a-e0562f10a49/data.blob
```

where /backup is the NFS location, 2014/08/07/16 is the archiving time, bd234b2d-df98-44ae-991a-e0562f10a49 is the bucket ID, and data.blob is the archived data for the bucket.

The archive data data.blob is a compressed file that uses vRealize Log Insight internal encoding. It contains the original content for all of the messages stored in the bucket, together with the static fields such as timestamp, host name, source, and appname.

You can import archived data to vRealize Log Insight, export archive data to a raw text file, and extract message content from archive data. See “Export a Log Insight Archive to a Raw Text File or JSON,” on page 34 and “Import a vRealize Log Insight Archive into vRealize Log Insight,” on page 33.

Import a vRealize Log Insight Archive into vRealize Log Insight

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

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

Prerequisites

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- Verify that you have access to the NFS server where vRealize Log Insight logs are archived.
Verify that the vRealize 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 vRealize 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 vRealize Log Insight logs, run the following command.

   ```bash
   /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.

---

**Export a Log Insight Archive to a Raw Text File or JSON**

You can use the command line to export a vRealize Log Insight archive to a regular raw text file or in JSON format.

**Note**: This is an advanced procedure. Command syntax and output formats might change in later releases of vRealize Log Insight without backward compatibility.

**Prerequisites**

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance.
- Verify that the vRealize Log Insight virtual appliance has enough disk space to accommodate the exported files.

**Procedure**

1. Establish an SSH connection to the vRealize Log Insight vApp and log in as the root user.
2. Create an archive directory on the vRealize Log Insight vApp.

   ```bash
   mkdir /archive
   ```

3. Mount the shared folder on the NFS server where the archived data resides by running the following command.

   ```bash
   mount -t nfs archive-fileshare:archive directory path /archive
   ```

4. Check the available storage space on the vRealize Log Insight vApp.

   ```bash
   df -h
   ```

5. Export a vRealize Log Insight archive to a raw text file.

   ```bash
   /usr/lib/loginsight/application/sbin/repo-exporter -d archive-file-directory output-file
   ```

   For example,

   ```bash
   /usr/lib/loginsight/application/sbin/repo-exporter -d /archive/2014/08/07/16/bd234b2d-df98-44ae-991a-e8562f10a49 /tmp/output.txt
   ```
6 Export a vRealize Log Insight archive message content in JSON format.


   For example,

   /usr/lib/loginsight/application/sbin/repo-exporter -F -d /archive/2014/08/07/16/bd234b2d-
   df98-44ae-991a-e0562f10a49 /tmp/output.json

7 Close the SSH connection.

Add vRealize Log Insight Event Forwarding Destination

You can configure a vRealize Log Insight server to forward incoming events to a syslog or Ingestion API target in addition to storing and indexing events.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

Verify that the destination can handle the number of events that are forwarded. If the destination cluster is much smaller than the forwarding instance, some events might be dropped.

Procedure

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

2 Under Management, click Event Forwarding.

3 Click New Destination and provide the required information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for the new destination.</td>
</tr>
<tr>
<td>Host</td>
<td>The IP address or fully qualified domain name. CAUTION: Entering master, node, and Integrated Load Balancer (ILB) IP addresses and hostnames are restricted when configuring forwarding destinations. Be sure to avoid creating network loops that may cause functionality issues such as reporting duplicate events.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Ingestion API or syslog. The default value is Ingestion API. When events are forwarded using Ingestion API, the event’s original source is preserved in the source field. When events are forwarded using syslog, the event’s original source is lost and the receiver may record the message’s source as the vRealize Log Insight forwarder’s IP address or hostname.</td>
</tr>
</tbody>
</table>

4 (Optional) Add tags.

Tags let you add fields with predefined values to events for easier querying. You can add multiple comma-separated tags.

   NOTE Tags are only available when using the Ingestion API.

5 (Optional) To restrict which events are forwarded, click Add Filter.

   If you do not select a filter, all events are forwarded.
6  (Optional) Click **Show Advanced Settings** to modify the following forwarding options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port</strong></td>
<td>The port to which events are sent on the remote destination. The default value is set based on the protocol specified. Do not change unless the remote destination listens on a different port.</td>
</tr>
<tr>
<td><strong>Disk Cache</strong></td>
<td>The amount of local disk space to reserve for buffering events that you configure to be forwarded. Buffering is used when the remote destination is unavailable or unable to process the events being sent to it. If the local buffer becomes full and the remote destination is still unavailable, then the oldest local events are dropped and not forwarded to the remote destination even when the remote destination is back online. The default value is 200 MB.</td>
</tr>
<tr>
<td><strong>Worker Count</strong></td>
<td>The number of simultaneous outgoing connections to use. Set a higher worker count for higher network latency to the forwarded destination and for higher number of forwarded events per second. The default value is 2.</td>
</tr>
</tbody>
</table>

7  To verify your configuration, click **Test**.

8  Click **Save**.

**What to do next**

- “Configure vRealize Log Insight Event Forwarding with SSL,” on page 36.
- You can edit or clone an event forwarding destination.

**Configure vRealize Log Insight Event Forwarding with SSL**

You can configure a vRealize Log Insight server to forward incoming events to a syslog or Ingestion API target with SSL.

**Prerequisites**

Event Forwarding with SSL does not work with the self-signed certificate installed on destination servers by default. A custom SSL certificate must be created using the steps in “Generate a Certificate Signing Request,” on page 28 and then uploaded. See “Install a Custom SSL Certificate by Using the vRealize Log Insight Web Interface,” on page 26

**Procedure**

1  Copy the trusted root certificate into a temporary directory on the forwarder instance. For example /home.

2  SSH to the forwarder instance and run the following commands.

```bash
localhost:~ # cd /usr/java/jre1.7.0_51/lib/security/
localhost:/usr/java/jre1.7.0_51/lib/security # ../../bin/keytool
-import -alias loginsight -file /home/cacert.crt -keystore cacerts
```

The default keystore password is **changeit**.

**NOTE**  Java versions might vary with time.

3  Restart the vRealize Log Insight instance.

**What to do next**

Restart the vRealize Log Insight Service

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

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

**Prerequisites**

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

**Procedure**

1. Click the configuration drop-down menu icon and select Administration.
2. Under Management, click Appliance.
3. Click Restart Master and click Restart.

**What to do next**

After vRealize Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in vRealize Log Insight. For troubleshooting, see ESXi Logs Stop Arriving in Log Insight.

After vRealize Log Insight restarts, verify that syslog feeds from ESXi continue to arrive in vRealize Log Insight. For troubleshooting, see the topic related to ESXi logs in the Log Insight Administration Guide.

Power Off the vRealize Log Insight Virtual Appliance

To avoid data loss when powering off a vRealize Log Insight master or worker node, you must power the node off by following a strict sequence of steps.

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

You can power off the vRealize 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 vRealize Log Insight virtual appliance and running a command.

**Prerequisites**

- If you plan to connect to the vRealize 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 vRealize Log Insight virtual appliance.

**Procedure**

1. Establish an SSH connection to the vRealize Log Insight vApp and log in as the root user.
2. To power off the vRealize Log Insight virtual appliance, run shutdown -h now.

**What to do next**

You can safely modify the virtual hardware of the vRealize Log Insight virtual appliance.
Add Memory and CPU to the vRealize Log Insight Virtual Appliance

You can change the amount of memory and CPUs allocated to a vRealize Log Insight virtual appliance after deployment.

You might need to adjust resource allocation if, for example, the number of events in your environment increases.

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 vRealize Log Insight virtual appliance safely. See “Power Off the vRealize Log Insight Virtual Appliance,” on page 37

Procedure
1. In the vSphere Client inventory, right-click the vRealize Log Insight virtual machine and select Edit Settings.
2. On the Hardware tab, click Add.
3. Adjust the amount of CPU and memory as needed.
4. Review the information and click Finish.
5. Click OK to save your changes and close the dialog box.

When you power on the vRealize Log Insight virtual appliance, the virtual machine begins to utilize the new resources.

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 vRealize Log Insight, contact li-info@vmware.com.

Prerequisites
Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize 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.

vRealize Log Insight stops sending trace data to VMware.
Configuring vRealize Log Insight Clusters

You can add, remove, and upgrade the nodes of a vRealize Log Insight cluster.

**NOTE**  WAN clustering is not supported by vRealize Log Insight. Current versions of vRealize Log Insight do not support WAN clustering (also called geoclustering, high-availability clustering or remote clustering). All nodes in the cluster should be deployed in the same Layer 2 LAN. In addition, the ports described in Ports and External Interfaces must be opened between nodes for proper communication.

This chapter includes the following topics:

- “Add a Worker Node to a vRealize Log Insight Cluster,” on page 39
- “Remove a Worker Node from a vRealize Log Insight Cluster,” on page 42
- “Enable Integrated Load Balancer,” on page 43

**Add a Worker Node to a vRealize Log Insight Cluster**

Deploy a new instance of the Log Insight virtual appliance and add it to an existing Log Insight master node.

**Procedure**

1. **Deploy the vRealize Log Insight Virtual Appliance** on page 39
   - Download the vRealize Log Insight virtual appliance. VMware distributes the vRealize Log Insight virtual appliance as an `.ova` file. Deploy the vRealize Log Insight virtual appliance by using the vSphere Client.

2. **Join Existing Deployment** on page 41
   - After you deploy and set up a standalone vRealize Log Insight node, you can deploy a new vRealize Log Insight instance and add it to the existing node to form a vRealize Log Insight cluster.

**Deploy the vRealize Log Insight Virtual Appliance**

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

**Prerequisites**

- Verify that you have a copy of the vRealize Log Insight virtual appliance `.ova` file.
- Verify that you have permissions to deploy OVF templates to the inventory.
- Verify that your environment has enough resources to accommodate the minimum requirements of the vRealize Log Insight virtual appliance. See Minimum Requirements.
Verify that you read and understand the virtual appliance sizing recommendations. See Sizing the Log Insight Virtual Appliance.

Procedure

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

2. Follow the prompts in the Deploy OVF Template wizard.

3. On the Deployment Configuration page, select the size of the vRealize Log Insight virtual appliance based on the size of the environment for which you intend to collect logs.

   **Small** is the minimum requirement for production environments.

   During the virtual appliance deployment, you can select the size of the appliance as follows.

<table>
<thead>
<tr>
<th>Option</th>
<th>Log Ingest Rate</th>
<th>vCPUs</th>
<th>Memory</th>
<th>IOPS</th>
<th>Syslog Connections</th>
<th>Events per Second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extra Small</td>
<td>6GB/day</td>
<td>2</td>
<td>4GB</td>
<td>75</td>
<td>20</td>
<td>400</td>
</tr>
<tr>
<td>Small</td>
<td>30GB/day</td>
<td>4</td>
<td>8GB</td>
<td>500</td>
<td>100</td>
<td>2000</td>
</tr>
<tr>
<td>Medium</td>
<td>75GB/day</td>
<td>8</td>
<td>16GB</td>
<td>1000</td>
<td>250</td>
<td>5000</td>
</tr>
<tr>
<td>Large</td>
<td>225GB/day</td>
<td>16</td>
<td>32GB</td>
<td>1500</td>
<td>750</td>
<td>15,000</td>
</tr>
</tbody>
</table>

   **Note** You can use a syslog aggregator to increase the number of syslog connections that send events to vRealize Log Insight. However, the maximum number of events per second is fixed and does not depend on the use of a syslog aggregator. A vRealize Log Insight instance cannot be used as a syslog aggregator.

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

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

   - **Thick Provision Lazy Zeroed** creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. The data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time, on first write from the virtual appliance.

   - **Thick Provision Eager Zeroed** creates a type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks.

   **Important** Deploy the vRealize Log Insight virtual appliance with thick provisioned eager zeroed disks whenever possible for better performance and operation of the virtual appliance.

   - **Thin Provision** creates a disk in thin format. The disk grows as the data saved on it grows. If your storage device does not support thick provisioning disks or you want to conserve unused disk space on the vRealize Log Insight virtual appliance, deploy the virtual appliance with thin provisioned disks.

   **Note** Shrinking disks on the vRealize Log Insight virtual appliance is not supported and might result in data corruption or data loss.
5 (Optional) On the Properties page, set the networking parameters for the vRealize Log Insight virtual appliance.

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

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

Use comma to separate domain name servers.

6 (Optional) On the Properties page, set the root password for the vRealize Log Insight virtual appliance.

7 Follow the prompts to complete the deployment.

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

After you power on the virtual appliance, an initialization process begins. The initialization process takes several minutes to complete. At the end of the process, the virtual appliance restarts.

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

<table>
<thead>
<tr>
<th>IP Address Prefix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>https://</td>
<td>The DHCP configuration on the virtual appliance is correct.</td>
</tr>
<tr>
<td>http://</td>
<td>The DHCP configuration on the virtual appliance failed.</td>
</tr>
<tr>
<td></td>
<td>a Power off the vRealize Log Insight virtual appliance.</td>
</tr>
<tr>
<td></td>
<td>b Right-click the virtual appliance and select <strong>Edit Settings</strong>.</td>
</tr>
<tr>
<td></td>
<td>c Set a static IP address for the virtual appliance.</td>
</tr>
</tbody>
</table>

**What to do next**

- To enable SSH connections to the vRealize Log Insight virtual appliance, configure the root password in the virtual appliance console. See *Configure the Root SSH Password for the Log Insight Virtual Appliance*.

- If you want to configure a standalone vRealize Log Insight deployment, see *Configure New Log Insight Deployment*.

The vRealize Log Insight Web interface is available at https://log-insight-host where *log-insight-host* is the IP address or host name of the vRealize Log Insight virtual appliance.

**Join Existing Deployment**

After you deploy and set up a standalone vRealize Log Insight node, you can deploy a new vRealize Log Insight instance and add it to the existing node to form a vRealize Log Insight cluster.

vRealize Log Insight can scale out by using multiple virtual appliance instances. This enables linear scaling of the ingestion throughput, increases query performance and allows for ingestion high availability. In cluster mode, vRealize Log Insight provides master and worker nodes. Both master and worker nodes are responsible for a subset of data. Master nodes can query all subsets of data and aggregate the results.

**IMPORTANT** It is highly recommended that you configure a minimum of three nodes in a vRealize Log Insight cluster to provide ingestion, configuration, and user space High Availability.

**Prerequisites**

- In the vSphere Client, note the IP address of the worker vRealize Log Insight virtual appliance.

- Verify that you have the IP address or host name of the master vRealize Log Insight virtual appliance.
- Verify that you have an administrator account on the master vRealize Log Insight virtual appliance.
- Verify that the versions of the vRealize Log Insight master and worker nodes are in sync. Do not add an older version vRealize Log Insight worker to a newer version vRealize Log Insight master node.
- You must synchronize the time on the vRealize Log Insight virtual appliance with an NTP server. See Synchronize the Time on the Log Insight Virtual Appliance.
- For information on supported browser versions, see the vRealize Log Insight Release Notes.

Procedure

1. Use a supported browser to navigate to the Web user interface of the vRealize Log Insight worker. The URL format is https://log_insight-host/, where log_insight-host is the IP address or host name of the vRealize Log Insight worker virtual appliance. The initial configuration wizard opens.
2. Click Join Existing Deployment.
3. Enter the IP address or host name of the vRealize Log Insight master and click Go.
   The worker sends a request to the vRealize Log Insight master to join the existing deployment.
4. Click the Click here to access the Cluster Management page link.
5. Log in as an administrator.
   The Cluster page loads.
6. Click Allow.
   The worker joins the existing deployment and vRealize Log Insight begins to operate in a cluster.

What to do next

- To add another worker, deploy a new vRealize Log Insight instance and add it to the cluster using the startup wizard.
- Repeat the procedure to add a minimum of two vRealize Log Insight worker nodes.

Remove a Worker Node from a vRealize Log Insight Cluster

You can remove a worker node that is no longer working correctly from a vRealize Log Insight cluster and add it to a different cluster or start a standalone deployment. Do not remove worker nodes that are operating correctly from a cluster.

Removing a node will result in data loss. If a node must be removed, ensure that it has been backed up first. Avoid removing nodes within 30 minutes of adding new nodes.

Prerequisites

- Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.
- If you use an external load balancer, take the node off the balancer before you put it in maintenance mode.

Procedure

1. Click the configuration drop-down menu icon and select Administration.
2. Under Management, click Cluster.
3 In the Workers table, find the the node you want, click , and click Continue. The node is now in maintenance mode.

**NOTE** A node in maintenance mode continues to receive logs.

4 Click to remove the node.

vRealize Log Insight removes the node from the cluster and sends out an email notification.

**Example:**

**What to do next**

Navigate to the Web user interface of the removed node to configure it. You can add the node to different existing vRealize Log Insight cluster or start a new standalone deployment.

**Enable Integrated Load Balancer**

You can enable the integrated load balancer on a vRealize Log Insight cluster to ensure that incoming Ingestion traffic is accepted by vRealize Log Insight even if some vRealize Log Insight nodes become unavailable.

It is highly recommended that you enable the Integrated Load Balancer (ILB) in a vRealize Log Insight cluster environment.

The ILB ensures that incoming Ingestion traffic is accepted by vRealize Log Insight even if some vRealize Log Insight nodes become unavailable. The ILB also balances incoming traffic fairly among available vRealize Log Insight nodes. vRealize Log Insight clients, using both the Web user interface and ingestion (through Syslog or the Ingestion API), should connect to vRealize Log Insight via the ILB address.

ILB requires that all vRealize Log Insight nodes be on the same Layer 2 network, such as behind the same switch or otherwise able to receive ARP requests from and send ARP requests to each other. The ILB IP address should be set up so that any vRealize Log Insight node can own it and receive traffic for it. Typically, this means that the ILB IP address will be in the same subnet as the physical address of the vRealize Log Insight nodes. After you configure the ILB IP address, try to ping it from a different network to ensure that it is reachable.

To simplify future changes and upgrades, you can have clients point to a FQDN that resolves to the ILB IP address, instead of pointing directly to the ILB IP address.

**Prerequisites**

- Configure a minimum of three nodes in a vRealize Log Insight cluster.
- Verify that all vRealize Log Insight nodes and the specified Integrated Load Balancer IP address are on the same network.
- The vRealize Log Insight master and worker nodes must have the same certificates. Otherwise the vRealize Log Insight Agents configured to connect through SSL will reject the connection. When uploading a CA-signed certificate to vRealize Log Insight master and worker nodes, set the Common Name to ILB IP address during certificate generation request. See “Generate a Certificate Signing Request,” on page 28.
- You must synchronize the time on the vRealize Log Insight virtual appliance with an NTP server. See Synchronize the Time on the Log Insight Virtual Appliance.

**Procedure**

1 Click the configuration drop-down menu icon and select Administration.
2 Under Management, click Cluster.

3 Under Configuration, select Enable Integrated Load Balancer and enter the virtual IP address to use for integrated load balancing.

4 (Optional) To enable vRealize Log Insight users to access the cluster via FQDN, point the clients to the FQDN instead of directly to the configured ILB IP address.

5 Click Save.
Configuring vRealize Log Insight Agents

You can monitor the status of vRealize Log Insight agents and you can create agent groups to enable configuration changes to be applied to multiple agents.

This chapter includes the following topics:

- “Monitor the Status of the vRealize Log Insight Windows and Linux Agents,” on page 45
- “Working with Agent Groups,” on page 45

Monitor the Status of the vRealize Log Insight Windows and Linux Agents

You can monitor the status of the vRealize Log Insight Windows and Linux agents and view current statistics about their operation.

Only those agents that are configured to send data via CFAPI appear on the Agents page. Agents that are configured to send data via the syslog appear on the Hosts page, as with other syslog sources.

Prerequisites

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure

1. Click the configuration drop-down menu icon and select Administration.
2. Under Management, click Agents.

What to do next

You can use the information from the Agents page to monitor the operation of the installed vRealize Log Insight Windows and Linux agents.

Working with Agent Groups

Using vRealize Log Insight server, you can configure agents from within the application's user interface. Agents poll the vRealize Log Insight server on a regular basis to determine if new configurations are available.

You can group agents that require the same configuration. For example, you might group all vRealize Log Insight Windows agents separately from the vRealize Log Insight Linux agents.
In the All Agents menu, existing agent groups from content packs are listed automatically. The agents listed relate to content packs that you have already installed, for example the vSphere content pack) that use agent groups.

Content pack groups are read-only.

Only configuration sections beginning with [winlog], [filelog], and [parser] are used in content packs. Additional sections are not exported as part of a content pack. Only single-line comments (lines beginning with ;) under the [winlog], [filelog], and [parser] sections, are preserved in a content pack.

See the vRealize Log Insight Agent Administration Guide for information about configuring agents including information on merging configurations between local and server-side configurations.

- **Agent Group Configuration Merging** on page 46
  
  With agent groups, agents can be part of multiple groups and they can belong to the default group All Agents—enabling centralized configuration.

- **Create an Agent Group** on page 46
  
  You can create a group of agents that are configured with the same parameters.

- **Edit an Agent Group** on page 47
  
  You can edit the name and description of an agent group, change the filters, and edit the configuration.

- **Add a Content Pack Agent Group as an Agent Group** on page 47
  
  You can add an agent group that was defined as part of a content pack to your active groups and apply an agent configuration to the group.

- **Delete an Agent Group** on page 48
  
  You can delete an agent group to remove it from the active groups list.

### Agent Group Configuration Merging

With agent groups, agents can be part of multiple groups and they can belong to the default group All Agents—enabling centralized configuration.

Merging occurs server-side—and the resulting configuration is merged with the agent-side configuration. The merged configuration is a result of the following rules.

- The individual group configurations have a higher priority and overrides the All Agents group settings.
- The All Agents group configuration overrides the local configuration.
- You cannot configure sections with the same name in different groups except with the All Agents groups. However, the sections in individual groups have a higher priority.

The merged configuration is stored in the agent-side liagent-effective.ini file.

### Create an Agent Group

You can create a group of agents that are configured with the same parameters.

**Prerequisites**

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

**Procedure**

1. Click the configuration drop-down menu icon and select Administration.
2. Under Management, click **Agents**.

3. In the **All Agents** menu, click **New Group**.

4. Provide a unique name and a description for the agent group and click **New Group**.
   
   The agent group is created and appears in the **All Agents** list, but is not saved.

5. Specify one or more of the following filters to the agent group.
   - IP address
   - hostname
   - version
   - OS
   
   For example, you can select the OS filter contains and specify the value `windows` to identify all your Windows agents for configuration.

   Until you specify a filter, all agents are listed.

6. Specify the agent configuration values in the Agent Configuration area and click **Save New Group**.

   The agent configuration is applied after the next polling interval.

### Edit an Agent Group

You can edit the name and description of an agent group, change the filters, and edit the configuration.

**Prerequisites**

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

**Procedure**

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

2. Under Management, click **Agents**.

3. In the **All Agents** menu, select the name of the appropriate agent group and click the pencil icon to edit it.

4. Make your changes.

<table>
<thead>
<tr>
<th>Item to Edit</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name or Description</td>
<td>Make the necessary changes and click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Filters or Configuration</td>
<td>Make the necessary changes and click <strong>Save Group</strong>.</td>
</tr>
</tbody>
</table>

### Add a Content Pack Agent Group as an Agent Group

You can add an agent group that was defined as part of a content pack to your active groups and apply an agent configuration to the group.

**Prerequisites**

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.
Procedure

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Agents**.
3. In the **All Agents** menu, select an agent template for the Available Templates list.
4. Click **Copy Template** to copy the content pack agent group to your active groups.
5. Click **Copy**.
6. Select the required filters and click **Save new group**.

The content pack agent group is added to the active groups and the agents are configured according to the filters that you specified.

Delete an Agent Group

You can delete an agent group to remove it from the active groups list.

**Prerequisites**

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

**Procedure**

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Agents**.
3. In the **All Agents** menu, select the name of the agent group to delete, by clicking the X icon next to its name.
4. Click **Delete**.

The agent group is removed from the active groups.
Managing vRealize Log Insight User Accounts

Administrators can create user accounts and roles to provide access to the vRealize Log Insight web interface. Only users with the Edit Admin permission can create and edit user accounts. However, users can change their own email and account password without having Edit Admin permission.

This chapter includes the following topics:

- “User Management Overview,” on page 49
- “Role-Based Access Control,” on page 50
- “Create a New User Account in vRealize Log Insight,” on page 50
- “Add an Active Directory User to vRealize Log Insight,” on page 51
- “Add an Active Directory Group to vRealize Log Insight,” on page 52
- “Define a Data Set,” on page 53
- “Create and Modify Roles,” on page 54
- “Delete a User Account from vRealize Log Insight,” on page 55
- “Enable User Authentication Through Active Directory,” on page 55

User Management Overview

System administrators use a combination of user logins, role-based access control, permissions, and data sets to manage vRealize Log Insight users. Role-based access control lets administrators manage users and the tasks that they can perform.

Roles are sets of permissions required to perform particular tasks. System administrators define roles as part of defining security policies, and grant the roles to users. To change the permissions and tasks associated with a particular task, the system administrator updates the role settings. The updated settings take effect for all users associated with the role.

- To allow a user to perform a task, the system administrator grants the role to the user.
- To prevent a user from performing a task, the system administrator revokes the role from the user.

Managing access, roles, and permissions for each user is based on their user login account. Each user can be granted multiple roles and permissions.

Users who cannot view or access certain objects or cannot perform certain operations were not granted the permissions to do so.
Role-Based Access Control

Role-based access control lets system administrators control user access to vRealize Log Insight and control tasks that users can perform after they log in. To implement role-based access control, system administrators associate or revoke permissions and roles with or from user login accounts.

**Users**
System administrators can control the access and actions of each user by granting or revoking permissions and roles to or from the login account of the user.

**Permissions**
Permissions control the allowed actions in vRealize Log Insight. Permissions apply to particular administrative or user tasks in vRealize Log Insight. For example, you can grant the View Admin permission to allow a user to view the vRealize Log Insight administrative settings.

**Data Sets**
Data sets consist of a set of filters. You can use data sets to provide users with access to specific content by associating a data set with a role.

**Roles**
Roles are collections of permissions and data sets that can be associated with users. Roles provide a convenient way to package all the permissions required to perform a task. One user can be assigned multiple roles.

Create a New User Account in vRealize Log Insight

Users that are given the Super Admin role can create user accounts to provide access to the vRealize Log Insight Web user interface.

**Prerequisites**
Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

**Procedure**
1. Click the configuration drop-down menu icon and select Administration.
2. Under Management, click Access Control.
3. Click Users and Groups.
4. Click New User.
5. In the Authentication drop-down menu, select Default (built-in).
6. Type a user name and email address.
   - The email address is optional.
7 From the **Roles** list on the right, select one or more predefined or custom user roles.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Users can access the full functionality of vRealize 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. Users do not have access to the administration options, cannot share content with other users, cannot modify the accounts of other users, and cannot install a content pack as a content pack.</td>
</tr>
<tr>
<td>Dashboard User</td>
<td>Dashboard users can only use the Dashboards page of vRealize Log Insight.</td>
</tr>
<tr>
<td>View Only Admin</td>
<td>View Admin users can view Admin information, have full User access and can edit Shared content.</td>
</tr>
<tr>
<td>Super Admin</td>
<td>Super Admin users can access the full functionality of vRealize Log Insight, can administer vRealize Log Insight, and can manage the accounts of all other users.</td>
</tr>
</tbody>
</table>

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

9 Click **Save**.

**Add an Active Directory User to vRealize Log Insight**

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

When you enable AD support in vRealize Log Insight, you configure a domain name and provide a binding user that belongs to the domain. vRealize 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 vRealize 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 vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.
- Verify that you configured AD support. See “**Enable User Authentication Through Active Directory,**” on page 55

**Procedure**

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

2 Under Management, click **Access Control**.

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.
From the **Roles** list on the right, select one or more predefined or custom user roles.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User</strong></td>
<td>Users can access the full functionality of vRealize 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. Users do not have access to the administration options, cannot share content with other users, cannot modify the accounts of other users, and cannot install a content pack as a content pack.</td>
</tr>
<tr>
<td><strong>Dashboard User</strong></td>
<td>Dashboard users can only use the Dashboards page of vRealize Log Insight.</td>
</tr>
<tr>
<td><strong>View Only Admin</strong></td>
<td>View Admin users can view Admin information, have full User access and can edit Shared content.</td>
</tr>
<tr>
<td><strong>Super Admin</strong></td>
<td>Super Admin users can access the full functionality of vRealize Log Insight, can administer vRealize Log Insight, and can manage the accounts of all other users.</td>
</tr>
</tbody>
</table>

Click **Save**.

vRealize 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 vRealize 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 vRealize Log Insight.

**Add an Active Directory Group to vRealize Log Insight**

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

When you enable AD support in vRealize Log Insight, you configure a domain name and provide a binding user that belongs to the domain. vRealize 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 vRealize 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 vRealize Log Insight web user interface as a user with the **Edit Admin** permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.
- Verify that you configured AD support. See “**Enable User Authentication Through Active Directory,**” on page 55

**Procedure**

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Access Control**.
3. Click **Users and Groups**.
4. 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.
5  (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.

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

7  From the **Roles** list on the right, select one or more predefined or custom user roles.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User</strong></td>
<td>Users can access the full functionality of vRealize 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. Users do not have access to the administration options, cannot share content with other users, cannot modify the accounts of other users, and cannot install a content pack as a content pack.</td>
</tr>
<tr>
<td><strong>Dashboard User</strong></td>
<td>Dashboard users can only use the Dashboards page of vRealize Log Insight.</td>
</tr>
<tr>
<td><strong>View Only Admin</strong></td>
<td>View Admin users can view Admin information, have full User access and can edit Shared content.</td>
</tr>
<tr>
<td><strong>Super Admin</strong></td>
<td>Super Admin users can access the full functionality of vRealize Log Insight, can administer vRealize Log Insight, and can manage the accounts of all other users.</td>
</tr>
</tbody>
</table>

8  Click **Save**.

vRealize 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 vRealize 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 vRealize Log Insight and have the same level of permissions as the group to which they belong.

### Define a Data Set

You can define a data set to provide users access to specific content.

**Prerequisites**

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

**Procedure**

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

2  Under Management, click **Access Control**.

3  Click **Data Sets**.

4  Click **New Data Set**.

5  Click **Add Filter**.
6 Use the first drop-down menu to select any field defined within vRealize Log Insight. For example, **hostname**. The list contains all defined fields that are available statically, in content packs, and in custom content.

**NOTE** Numeric fields contain the additional operators =, >, <, >=, and <=, which string fields do not. These operators perform numeric comparisons. Using them yields different results than using string operators. For example, the filter `response_time = 02` will match an event that contains a `response_time` field with a value 2. The filter `response_time contains 02` will not have the same match.

7 Use the second drop-down menu to select the operation to apply to the field selected in the first drop-down menu. For example, select **contains**. The **contains** filter matches full tokens: searching for the string `err` will not result in `error` as a match.

8 In the text box to the right of the filter drop-down menu, enter the value that you want to use as a filter. You can use multiple values. The operator between these values is OR.

**NOTE** The text box is not available if you select the **exists** operator in the second drop-down menu.

9 (Optional) To add more filters, click **Add Filter**.

10 Click **Save**.

**What to do next**

Associate a data set with a user role. See “Create and Modify Roles,” on page 54.

---

### Create and Modify Roles

You can create custom roles or modify predefined roles to allow users to perform certain tasks and access specific content.

**Prerequisites**

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

**Procedure**

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Access Control**.
3. Click **Roles**.
4. Click **New Role** or **to edit an existing role**.

   You must clone Super Admin and User roles first before you can edit them.

5. Modify the **Name** and **Description** text boxes.
6. Select one or more permissions from the Permissions list.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit Admin</strong></td>
<td>Can edit Admin information and settings</td>
</tr>
<tr>
<td><strong>View Admin</strong></td>
<td>Can view Admin information and settings</td>
</tr>
<tr>
<td><strong>Edit Shared</strong></td>
<td>Can edit shared content</td>
</tr>
</tbody>
</table>
### Delete a User Account from vRealize Log Insight

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

**Prerequisites**

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is https://log-insight-host, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

**Procedure**

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **Access Control**.
3. Click **Users and Groups**.
4. Select the check box beside the user name that you want to delete.
5. Click the **Delete** icon.

### Enable User Authentication Through Active Directory

vRealize 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 vRealize 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 vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is https://log-insight-host, where `log-insight-host` is the IP address or host name of the vRealize 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, vRealize Log Insight uses the default domain and the binding user to verify AD users and groups in the trusting domains.

In addition, you cannot switch to a different domain on an instance that already includes users and groups.

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

vRealize 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 vRealize Log Insight. See “Add an Active Directory User to vRealize Log Insight,” on page 51.

### Configure the Protocol to Use for Active Directory

You can configure the protocol to use when connecting to Active Directory. By default, when vRealize 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 vRealize Log Insight virtual appliance.

**Prerequisites**

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance. See “Configure the Root SSH Password for the Log Insight Virtual Appliance,” on page 14
- To enable SSH connections, verify that TCP port 22 is open.

**Procedure**

1 Establish an SSH connection to the vRealize Log Insight virtual appliance and log in as the root user.
2 Navigate to the following location: `/storage/var/loginsight/config`
3 Locate the latest configuration file where `[number]` is the largest: `/storage/core/loginsight/config/loginsight-config.xml#[number]`
4 Copy the latest configuration file: `/storage/core/loginsight/config/loginsight-config.xml#[number]`
5 Increase the `[number]` and save to the following location: `/storage/core/loginsight/config/loginsight-config.xml#[number + 1]`
6 Open the file for editing.
7 In the **Authentication** section, add the line that corresponds to the configuration that you want to apply:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ad-protocols value=&quot;LDAP&quot; /&gt;</code></td>
<td>For specifically using LDAP without SSL</td>
</tr>
<tr>
<td><code>&lt;ad-protocols value=&quot;LDAPS&quot; /&gt;</code></td>
<td>For specifically using LDAP with SSL only</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>&lt;ad-protocols value=&quot;LDAP,LDAPS&quot; /&gt;</code></td>
<td>For specifically using LDAP first and then using LDAP with SSL.</td>
</tr>
<tr>
<td><code>&lt;ad-protocols value=&quot;LDAPS,LDAP&quot; /&gt;</code></td>
<td>For specifically using LDAPS first and then using LDAP without SSL.</td>
</tr>
</tbody>
</table>

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

8. Save and close the file.

9. Run the `service loginsight restart` command.
You can monitor the vRealize Log Insight virtual appliance and the hosts and devices that send log events to vRealize Log Insight.

This chapter includes the following topics:

- “Check the Health of the vRealize Log Insight Virtual Appliance,” on page 59
- “Monitor Hosts That Send Log Events,” on page 60

### Check the Health of the vRealize Log Insight Virtual Appliance

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

**Prerequisites**

Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is `https://log-insight-host`, where `log-insight-host` is the IP address or host name of the vRealize Log Insight virtual appliance.

**Procedure**

1. Click the configuration drop-down menu icon and select **Administration**.
2. Under Management, click **System Monitor**.
3. If vRealize Log Insight is running as a cluster, click **Show resources for** and choose the node you want to monitor.
4. Click the buttons on the System Monitor page to view the information that you need.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resources</strong></td>
<td>View information about the CPU, memory, IOPS (read and write activity), and storage usage on the vRealize 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.</td>
</tr>
<tr>
<td><strong>Active Queries</strong></td>
<td>View information about the queries that are currently active in vRealize Log Insight.</td>
</tr>
<tr>
<td><strong>Statistics</strong></td>
<td>View statistics about the log ingest operations and rates. To view more detailed statistics, click <strong>Show advanced statistics</strong>.</td>
</tr>
</tbody>
</table>
What to do next
You can use the information from the System Monitor page to manage resources on the vRealize Log Insight virtual appliance.

Monitor Hosts That Send Log Events
You can view a list of all hosts and devices that send log events to vRealize Log Insight and monitor them.

Prerequisites
Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

Procedure
1. Click the configuration drop-down menu icon and select Administration.
2. Under Management, click Hosts.

Note: If you have configured a vCenter Server to send events and alarms, but have not configured the individual ESXi hosts to send logs, the Hostname column lists both the vCenter Server and the individual ESXi hosts as the source instead of listing just the vCenter Server.
Integrating vRealize Log Insight with VMware Products

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

Integration with VMware vSphere

vRealize Log Insight Administrator users can set up vRealize 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, vRealize Log Insight can configure ESXi hosts via vCenter Server. See “Connect vRealize Log Insight to a vSphere Environment,” on page 62.

Integration with VMware vRealize Operations Manager

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

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

Notification Events

vRealize Log Insight Administrator users can set up vRealize Log Insight to send notification events to vRealize Operations Manager based on queries that you create. These notification events are not alerts in vRealize Operations Manager, and do not affect the values of the Health, Risk, or Efficiency badge. See “Configure vRealize Log Insight to Send Notification Events to vRealize Operations Manager,” on page 68.

Launch in Context

Launch in context is a feature in vRealize 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 vRealize Log Insight adapter add menu items to a number of different views within the Custom user interface and the vSphere user interface of vRealize Operations Manager. See “Enable Launch in Context for vRealize Log Insight in vRealize Operations Manager,” on page 72.

Note Notification events do not depend on the launch in context configuration. You can send notification events from vRealize Log Insight to vRealize Operations Manager even if you do not enable the launch in context feature.
If the environment changes, vRealize Log Insight administrator users can change, add, or remove vSphere systems from vRealize Log Insight, change or remove the instance of vRealize Operations Manager to which alert notifications are sent, and change the passwords that are used to connect to vSphere systems and vRealize Operations Manager.

This chapter includes the following topics:

- “Connect vRealize Log Insight to a vSphere Environment,” on page 62
- “Configure vRealize Log Insight to Send Notification Events to vRealize Operations Manager,” on page 68
- “Enable vRealize Log Insight and vRealize Operations Manager Active Directory Integration,” on page 70
- “Add a Search Domain,” on page 70
- “Install the vRealize Log Insight Adapter in vRealize Operations Manager Standalone,” on page 71
- “vRealize Operations Manager Content Pack for vRealize Log Insight,” on page 72
- “Enable Launch in Context for vRealize Log Insight in vRealize Operations Manager,” on page 72
- “Disable Launch in Context for vRealize Log Insight in vRealize Operations Manager,” on page 75
- “Remove the vRealize Log Insight Adapter from a vRealize Operations Manager instance,” on page 76

Connect vRealize Log Insight to a vSphere Environment

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

vRealize 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, vRealize Log Insight pulls events, tasks, and alerts from the registered vCenter Server instances.
- Logs contain unstructured data that can be analyzed in vRealize Log Insight. ESXi hosts or vCenter Server Appliance instances can push their logs to vRealize 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.

<table>
<thead>
<tr>
<th>Level of Integration</th>
<th>Required Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events, tasks, and alarms collection</td>
<td>System.View</td>
</tr>
<tr>
<td><strong>Note</strong> System.View is a system-defined privilege. When you add a custom role and do not assign any privileges to it, the role is created as a Read Only role with three system-defined privileges: System.Anonymous, System.View, and System.Read.</td>
<td></td>
</tr>
<tr>
<td>Syslog configuration on ESXi hosts</td>
<td>Host.Configuration.Change settings</td>
</tr>
<tr>
<td></td>
<td>Host.Configuration.Network configuration</td>
</tr>
</tbody>
</table>

**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 vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize 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.
   - It is recommended that you use service account credentials.
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. vRealize 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 vRealize Log Insight to Pull Events, Tasks, and Alarms from vCenter Server Instance,” on page 63.
- Start collecting syslog feeds from the ESXi hosts that the vCenter Server manages. See “Configure an ESXi Host to Forward Log Events to vRealize Log Insight,” on page 64.

**Configure vRealize 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 vRealize Log Insight to collect alarms, events, and tasks data from one or more vCenter Server systems.

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

- **Note** vRealize 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.
vRealize 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.

**vRealize Log Insight as a Syslog Server**

vRealize Log Insight includes a built-in syslog server that is constantly active when the vRealize 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 vRealize Log Insight Web user interface near real time. The maximum syslog message length that vRealize Log Insight accepts is 10 KB.

**Configure an ESXi Host to Forward Log Events to vRealize Log Insight**

ESXi hosts or vCenter Server Appliance instances generate unstructured log data that can be analyzed in vRealize Log Insight.

You use the vRealize Log Insight Administration interface to configure ESXi hosts on a registered vCenter Server to push syslog data to vRealize Log Insight.

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

A vRealize Log Insight cluster can utilize a load balancer to distribute ESXi and vCenter Server Appliance syslog feeds between the individual nodes of the cluster.

For information on filtering syslog messages on ESXi hosts before messages are sent to vRealize Log Insight, see the *Configure Log Filtering on ESXi Hosts* topic in the Setting Up ESXi section, of the *vSphere Installation and Setup* guide.

For information on configuring syslog feeds from a vCenter Server Appliance, see “Configure a vCenter Server Appliance to Forward Log Events to vRealize Log Insight,” on page 67.

**NOTE** vRealize Log Insight can receive syslog data from ESXi hosts version 5.0 and later.

For vSphere Web Client versions 5.0 and 5.1, logging is interrupted following a vRealize Log Insight restart, or loss in connectivity. Rerun the configuration process in these instances, to restart the logging process.

**Prerequisites**
- Verify that the vCenter Server that manages the ESXi host is registered with your vRealize 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, vRealize Log Insight configures all reachable ESXi hosts of version 5.0 and later to send their logs through UDP.
5. (Optional) Enter the hostname or IP address of a load balancer you want to use to distribute syslog feeds.
6. (Optional) To select which ESXi hosts forward their logs to vRealize Log Insight, or to select which protocol is used, click Advanced Options.
7. 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 vRealize Log Insight.

To forward log messages from multiple ESXi hosts within the vCenter Server to vRealize 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** This procedure doesn't apply if you already configured an ESXi host to forward log events to vRealize Log Insight by following the “Configure an ESXi Host to Forward Log Events to vRealize Log Insight,” on page 64 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.

Chapter 7 Integrating vRealize Log Insight with VMware Products

VMware, Inc. 65
4 Modify the Syslog.global.logHost property to point to the vRealize 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 vRealize 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 vRealize 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** This procedure doesn't apply if you already configured an ESXi host to forward log events to vRealize Log Insight by following the “Configure an ESXi Host to Forward Log Events to vRealize Log Insight,” on page 64 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.

```
```

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

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

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

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

---

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

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

To configure ESXi hosts to forward their logs to vRealize Log Insight, see [Connect Log Insight to vCenter Server Systems](#).

To configure ESXi hosts to forward their logs to vRealize Log Insight, see the topic *Connect vRealize Log Insight to vCenter Server 5.1.x Systems* in the vRealize 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 vRealize 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));
   }
   ```
Configure vRealize Log Insight to Send Notification Events to vRealize Operations Manager

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

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

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

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

vRealize Log Insight uses the VMware vRealize Operations Manager Suite 6.0 REST API to create resources and relationships in vRealize Operations Manager for configuring the launch in context adapter. You can use the older HTTP POST adapter to create the launch in context adapter, but currently this requires you to set the method to POST, rather than REST. See the logininsight-config-base.xml file for more details.

Prerequisites

- Verify that the version of vRealize Operations Manager supports alert notifications from vRealize Log Insight. For more information about supported product versions, see Product Compatibility.

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

- Depending on the vRealize Operations Manager license that you own, verify that you have minimum user credentials.

<table>
<thead>
<tr>
<th>vRealize Operations Manager License</th>
<th>Minimum Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>Default Admin user credentials</td>
</tr>
<tr>
<td>Advanced or Enterprise</td>
<td>Read Only user credentials</td>
</tr>
</tbody>
</table>

  **NOTE** vRealize Log Insight does not support Active Directory integration with vRealize Operations Manager.

- Verify that you know the IP address or host name of the target vRealize Operations Manager instance.
Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

**NOTE** In an environment running a vRealize Operations Manager 6.1 cluster with a configured load balancer, you can use the load balancer IP address if one is available.

**Procedure**

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

   vRealize Log Insight uses the credentials to push notification events to vRealize Operations Manager. It is recommended that you use service account credentials.

4. In the vRealize Operations Manager pane, select Enable alerts integration.
5. Click Save.

**What to do next**

- Notification events that vRealize Log Insight sends are not visible by default in the vRealize Operations Manager vSphere UI. Go to Planning > Events and click Show notification events.
- You can configure alert queries to send notification events to vRealize Operations Manager. See Add an Alert Query in Log Insight to Send Notification Events to vRealize Operations Manager.
- You can configure alert queries to send notification events to vRealize Operations Manager. See topic Add an Alert Query in Log Insight to Send Notification Events to vRealize Operations Manager in the Log Insight User’s Guide.

**vRealize Log Insight Notification Events in vRealize Operations Manager**

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

When you configure a notification alert in vRealize Log Insight, you select a resource in vRealize Operations Manager that is associated with the notification events. See Add an Alert Query in Log Insight to Send Notification Events to vRealize Operations Manager.

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

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

**Table 7-1. Sections of the vRealize Operations Manager User Interface Where Notification Events Appear**

<table>
<thead>
<tr>
<th>vRealize Operations Manager User Interface</th>
<th>Section that Displays vRealize Log Insight Notification Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom user interface</td>
<td>■ The Alerts Overview page</td>
</tr>
<tr>
<td></td>
<td>■ All dashboards that display the Alerts dashboard widget</td>
</tr>
<tr>
<td>vSphere user interface</td>
<td>■ The Events tab under the Operations tab</td>
</tr>
<tr>
<td></td>
<td>■ The Events tab under the Planning tab</td>
</tr>
</tbody>
</table>
The alert name and description that you provided in vRealize Log Insight appear in the Alert Info column of the alert lists in vRealize 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.

**Enable vRealize Log Insight and vRealize Operations Manager Active Directory Integration**

To integrate vRealize Log Insight with vRealize Operations Manager using an LDAP source, you need the name of the LDAP source in vRealize Operations Manager; in vRealize Log Insight you need to integrate it with user@domain@source, and make sure that the user you created in vRealize Operations Manager has permissions to manipulate objects in vRealize Operations Manager.

To perform the integration, you need administration access to both vRealize Log Insight and vRealize Operations Manager.

**Procedure**

1. In vRealize Operations Manager, obtain the name of the LDAP source (SOURCE) that will have access to vRealize Operations Manager.
2. Confirm that the user has Resource Creation. Relationship Creation, and Resource Deletion permissions.
3. (Optional) To confirm access, have the user log into vRealize Operations Manager.
4. In vRealize Log Insight, the user should be specified as USER@SOURCE. If the user is a UPN (identified by NAME@DOMAIN), then the user would be specified in vRealize Log Insight as USER@DOMAIN@SOURCE.

**Add a Search Domain**

You can add a search domain to improve the vRealize Operations Manager inventory matching.

Adding a search domain improves matching when a virtual machine label and search domain resolve to the IP address of the host that sends log messages to vRealize Log Insight. For example, if you have a virtual machine named linux_01 in vRealize Operations Manager and the host name linux_01.company.com resolves to 192.168.10.10, then adding a search domain allows vRealize Log Insight to recognize and match that resource.

**Prerequisites**

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance. See “Configure the Root SSH Password for the Log Insight Virtual Appliance,” on page 14
- To enable SSH connections, verify that TCP port 22 is open

**Procedure**

1. Establish an SSH connection to the vRealize Log Insight virtual appliance and log in as the root user.
2. Open /etc/resolv.conf.
3. Add your search domain. For example, search company.com.
4. Save and close the file.
Install the vRealize Log Insight Adapter in vRealize Operations Manager Standalone

You install the vRealize Log Insight adapter in vRealize Operations Manager standalone to enable the Launch in Context functionality.

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

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

The vRealize Log Insight adapter is installed as part of vRealize Operations Manager 5.7.2 and 5.8.

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

Prerequisites

- Download the management pack installation file from [https://solutionexchange.vmware.com/store/category_groups/cloud-management](https://solutionexchange.vmware.com/store/category_groups/cloud-management). You can download the TGZ file from the Resources tab of the management pack page.
- Make a note of the build number in the TGZ file name. The build number appears after the management pack name, for example, `managementpack_name-buildnumber.tgz`.
- Verify that you have access to the server where vRealize Operations Manager runs, and that you have permissions to install software on the server.
- Verify that the version of vRealize Operations Manager is 5.7.1 or later.
- Verify that you know the IP address or host name of the target vRealize Operations Manager instance.
- Depending on the vRealize Operations Manager license that you own, verify that you have minimum user credentials.

<table>
<thead>
<tr>
<th>vRealize Operations Manager License</th>
<th>Minimum Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>Default Admin user credentials</td>
</tr>
<tr>
<td>Advanced or Enterprise</td>
<td>Read Only user credentials</td>
</tr>
</tbody>
</table>

**NOTE** vRealize Log Insight does not support Active Directory integration with vRealize Operations Manager.

Procedure

1. Open the TGZ file and extract the TAR file to a temporary location on your vRealize 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 vRealize Operations Manager 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.
Verify that the build number in the Adapter Version column for the management pack 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 vRealize Log Insight.


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

**vRealize Operations Manager Content Pack for vRealize Log Insight**

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

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

---

**NOTE** The vRealize Operations Manager content pack requires vRealize Log Insight version 1.5 and vRealize Operations Manager version 5.8.

You can download the vRealize Operations Manager content pack from https://solutionexchange.vmware.com/store/loginsight?src=Product_Product_LogInsight_YES_US.

See Working with Content Packs.

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

**Enable Launch in Context for vRealize Log Insight in vRealize Operations Manager**

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

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

---

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

**Prerequisites**

- Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the **Edit Admin** permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

- Verify that you know the IP address or host name of the target vRealize Operations Manager instance.
Depending on the vRealize Operations Manager license that you own, verify that you have minimum user credentials.

<table>
<thead>
<tr>
<th>vRealize Operations Manager License</th>
<th>Minimum Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>Default Admin user credentials</td>
</tr>
<tr>
<td>Advanced or Enterprise</td>
<td>Read Only user credentials</td>
</tr>
</tbody>
</table>

**NOTE** vRealize Log Insight does not support Active Directory integration with vRealize Operations Manager.

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

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

For more information about supported product versions, see Product Compatibility.

**Procedure**

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

   **NOTE** You must provide the user credentials of a vRealize Operations Manager administrator user.
4. Click Save.

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

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

**What to do next**

Launch a vRealize Log Insight query from the vRealize Operations Manager instance. See “vRealize Log Insight Launch in Context,” on page 73

**vRealize Log Insight Launch in Context**

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

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

**Launch in Context in the vSphere User Interface of vRealize Operations Manager**

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

The available launch in context action depends on the object that you select in vRealize Operations Manager inventory. The time range of the queries is limited to 60 minutes before you click a launch in context option.
### Table 7-2. Objects in vRealize Operations Manager vSphere UI and their Corresponding Launch in Context Options and Actions

<table>
<thead>
<tr>
<th>Object selected in vRealize Operations Manager</th>
<th>Launch in Context Option in the Actions Drop-Down Menu</th>
<th>Action in vRealize Operations Manager</th>
<th>Action in vRealize Log Insight</th>
</tr>
</thead>
<tbody>
<tr>
<td>World</td>
<td>Open vRealize Log Insight</td>
<td>Opens vRealize Log Insight.</td>
<td>vRealize Log Insight displays the Interactive Analytics tab.</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>Open vRealize Log Insight</td>
<td>Opens vRealize Log Insight.</td>
<td>vRealize Log Insight displays the Interactive Analytics tab.</td>
</tr>
<tr>
<td>Datacenter</td>
<td>Search for logs in vRealize Log Insight</td>
<td>Opens vRealize Log Insight and passes the resource names of all host systems under the selected Datacenter object.</td>
<td>vRealize Log Insight displays the Interactive Analytics tab and performs a query to find log events that contain names of hosts within the data center.</td>
</tr>
<tr>
<td>Cluster</td>
<td>Search for logs in vRealize Log Insight</td>
<td>Opens vRealize Log Insight and passes the resource names of all host systems under the selected Cluster object.</td>
<td>vRealize Log Insight displays the Interactive Analytics tab and performs a query to find log events that contain names of hosts within the cluster.</td>
</tr>
<tr>
<td>Host System</td>
<td>Search for logs in vRealize Log Insight</td>
<td>Opens vRealize Log Insight and passes the resource name of the selected Host object.</td>
<td>vRealize Log Insight displays the Interactive Analytics tab and performs a query to find log events that contain the name of the selected Host system.</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Search for logs in vRealize Log Insight</td>
<td>Opens vRealize Log Insight and passes the IP address of the selected virtual machine and the resource name of the related host system.</td>
<td>vRealize 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.</td>
</tr>
</tbody>
</table>

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 vRealize 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 vRealize Log Insight from metric charts in vRealize Operations Manager. The time range of the query that vRealize Log Insight runs matches the time range of the metric chart.

**Note**: The time that you see in vRealize Log Insight and vRealize 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 vRealize Operations Manager

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

- The Alerts Overview page.
- The Alert Summary page of a vRealize Log Insight notification alert.
- The Alerts widgets on your dashboards, when a vRealize Log Insight notification alert is selected.
When you select a vRealize Log Insight notification event in the Custom user interface, you can choose between two launch in context actions.

<table>
<thead>
<tr>
<th>Launch in Context Option in vRealize Operations Manager</th>
<th>Action in vRealize Operations Manager</th>
<th>Action in vRealize Log Insight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open vRealize Log Insight</td>
<td>Opens vRealize Log Insight.</td>
<td>vRealize Log Insight displays the Dashboards tab and loads the vSphere Overview dashboard.</td>
</tr>
<tr>
<td>Search for Logs in vRealize Log Insight</td>
<td>Opens vRealize Log Insight and passes the ID of the query that triggered the notification event.</td>
<td>vRealize Log Insight displays the Interactive Analytics tab and performs the query that triggered the notification event.</td>
</tr>
</tbody>
</table>

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

### Disable Launch in Context for vRealize Log Insight in vRealize Operations Manager

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

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

---

**Prerequisites**

- Verify that you are logged in to the vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize Log Insight virtual appliance.

**Procedure**

1. Click the configuration drop-down menu icon and select Administration.
2. Under Integration, select vRealize Operations Manager.
3. Deselect the Enable Launch in Context check box.
4. Click Save.

vRealize Log Insight configures the vRealize Operations Manager instance to remove the vRealize Log Insight adapter. This operation might take a few minutes.
Remove the vRealize Log Insight Adapter from a vRealize Operations Manager instance

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

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

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

You can use the command line utility cURL to send REST calls to vRealize Operations Manager.

Prerequisites
- Verify that cURL is installed on your system.
- Verify that you know the IP address or host name of the target vRealize Operations Manager instance.
- Depending on the vRealize Operations Manager license that you own, verify that you have minimum user credentials.

<table>
<thead>
<tr>
<th>vRealize Operations Manager License</th>
<th>Minimum Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>Default Admin user credentials</td>
</tr>
<tr>
<td>Advanced or Enterprise</td>
<td>Read Only user credentials</td>
</tr>
</tbody>
</table>

Note: vRealize Log Insight does not support Active Directory integration with vRealize Operations Manager.

Procedure

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

```bash
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 vRealize Operations Manager instance.

The query returns a result in the following format.

```
resourceName=Log Insight Server&adapterKindKey=LogInsight&resourceKindKey=LogInsightLogServer&
Parents:  
Children:
```

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

```bash
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 Server,Log Insight,LogInsightLogServerHost,HOST::log insight location"
```

Where `admin username` and `passwd` are the administrator user credentials, `URL` is the IP address of the vRealize Operations Manager instance, and `log insight location` is the host location of the child resource of the relationship you want to remove.

vRealize Log Insight launch in context items are removed from the menus in vRealize Operations Manager. For more information about launch in context, see the topic `vRealize Log Insight Launch in Context` of the vRealize Log Insight in-product help.
To guard against expensive datacenter downtime, best practices can be followed to perform backup, restore, and disaster recovery operations.

This chapter includes the following topics:

- “Backup Restore and Disaster Recovery Best Practices,” on page 79
- “General Guidelines,” on page 80
- “General Recommendations,” on page 81
- “Backup and Replication Guidelines,” on page 81
- “Restore and Disaster Recovery Guidelines,” on page 82
- “Post-Recovery Configuration Change Guidelines,” on page 83

### Backup Restore and Disaster Recovery Best Practices

To guard against expensive datacenter downtime, best practices can be followed to perform backup, restore, and disaster recovery operations.

The information in this chapter describes guidelines for backup, restore, and disaster recovery best practices for the following vRealize Log Insight versions and components.

<table>
<thead>
<tr>
<th>vRealize Log Insight Version</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0 GA</td>
<td>Master node, worker node, agent, forwarder</td>
</tr>
<tr>
<td>2.5 GA</td>
<td>Master node, worker node, agent, forwarder</td>
</tr>
</tbody>
</table>

The information in this chapter does not describe the following tools and products.

- This chapter does not include tool-specific backup, restore, and disaster recovery steps. Tool or product-specific information can be found in original product documentation.
- For information on VDP, SRM, and NetBackup best practices, see the VMware vCloud Suite best practices whitepaper on these specific tools.
- This chapter does not include guidelines for backup, restore, and disaster recovery for the following products that integrate with vRealize Log Insight.
  - vRealize Operations Manager
  - VMware vSphere server
  - ESXi hosts
  - Other products that integrate with vRealize Log Insight
General Guidelines

Follow these guidelines for backup operations and for an easier restoration of vRealize Log Insight 3.0 GA and 2.5 GA clusters in a new environment.

vRealize Log Insight 3.0 GA and 2.5 GA support the following best practices and guidelines.

- Use static IP addresses for all nodes in a vRealize Log Insight cluster.
  - Using static IP addresses eliminates the need to update the IP addresses of vRealize Log Insight cluster nodes each time the IP address of a vRealize Log Insight node changes.
  - vRealize Log Insight includes all node IP addresses in each cluster node configuration file at `/storage/core/loginsight/config/loginsight-config.xml#<n>`; where `<n>` is the largest number.
  - All products that integrate with vRealize Log Insight to feed their logs (for example: ESXi, vSphere, vRealize Operations) use the cluster master (or the load balancer if configured) nodes Fully Qualified Domain Name (FQDN) or IP address as the syslog target. Static IP addresses reduce the risk of constantly updating the syslog target IP address in multiple locations.

- Use a FQDN for all nodes in the vRealize Log Insight cluster.
  - For the master node (load balancer when used), a fully resolvable FQDN is required. Otherwise, the ESXi hosts will fail to feed the syslog messages to vRealize Log Insight or to any remote target.
  - Using an FQDN saves time on post-restore and recovery configuration changes assuming the same FQDN can be resolved on the recovery site.
  - For system alerts, vRealize Log Insight uses FQDN host names if available instead of IP addresses.
  - Assuming only underlying IP addresses change post-backup/recovery or disaster recovery operations, using FQDN eliminates the need to change the syslog target address (master node FQDN or Internal Load Balancer (ILB) FQDN) on all the external devices feeding logs to the vRealize Log Insight cluster.

- With vRealize Log Insight 2.5 GA, you must update the configuration file (located at `/storage/core/loginsight/config/loginsight-config.xml#<n>` where `<n>` is the largest number) to replace the worker node IP address with the new IP address used for the restored nodes as the FQDN is not used for worker node addresses in the configuration file. You need to make this change only on the master node and the changes are synchronized to all worker nodes.

- Join requests from a vRealize Log Insight worker node should use the FQDN of the vRealize Log Insight master node.
  - Beginning in vRealize Log Insight 2.5, the master node host value in the configuration file on each of the nodes (located at `/storage/core/loginsight/config/loginsight-config.xml#<n>`) is based on the value used by the first worker node sending a join request. Using the FQDN of the master node for the join request prevents making any manual changes to the master node host value post-disaster recovery. Otherwise, the worker nodes cannot rejoin the master node until the master node host name is updated in the configuration files on all restored cluster nodes.

- Provide static IP addresses as well as optional virtual IP addresses for the load balancer.
  - When configuring an integrated Load Balancer, provide the (optional) FQDN for the virtual IP address. This enables vRealize Log Insight to revert to the FQDN when an IP address is not reachable for any reason.
General Recommendations

Follow these recommendations for backup operations.

The following recommendations help to prepare for backup and restoration operations.

- Perform a test run of the backup, restore, and disaster recovery operations in a test or staging environment before performing these operations on a live production setup.
- Forwarders—Based on the customer requirements, there could be a single or multiple vRealize Log Insight forwarders. In addition, the forwarders can be installed as a standalone node or as a cluster. For the purpose of backup, restore, and disaster recovery operations, vRealize Log Insight forwarders are identical to the primary vRealize Log Insight cluster nodes and therefore the same backup, restore, and disaster recovery steps recommended for the main vRealize Log Insight cluster should be applied to the forwarders as well.
- Perform a full backup of the entire vRealize Log Insight cluster; do not rely on automatic procedures to backup individual files and configurations.
- Confirm that the recommended amount of resources are allocated for the vRealize Log Insight cluster, backup, restore, and disaster recovery tools as recommended by the documentation for individual backup, restore, and disaster recovery tools.
- Confirm that tool-specific best practices are followed as recommended by the documentation for individual backup, restore, and disaster recovery tools.
- Use additional tools that can provide special features and configurations to support backup, restore, and disaster recovery of virtual machines deployed using VMware products.
- Confirm that fixes are implemented and warnings and errors are addressed before performing backup, restore, and disaster recovery operations. Backup, restore, and disaster recovery tools usually provide visual validations and steps to ensure that backup, restore, and disaster recovery configurations are successfully created.

Backup and Replication Guidelines

Specific backup and replication guidelines provide additional best practices.

- Existing Issues—Confirm there are no configuration issues on source and target sites before performing the backup and restore operations.
- vRealize Log Insight Cluster Resource Allocation—In vRealize Log Insight configurations with reasonable ingestion and query loads, it’s possible that the memory and swap usage may reach almost 100% capacity during backup and replication operations. Because this occurs in a live environment, part of the memory spike is due to the vRealize Log Insight cluster usage itself. It is also possible that the scheduled backup and replication operations may contribute significantly to the memory spike.
  - In some cases worker nodes got disconnected momentarily for one to three minutes before rejoining master nodes. And we suspect that this is because of high memory usage.
  - To reduce the memory throttling on Log Insight nodes:
    - Allocate additional memory over the vRealize Log Insight recommended configurations and/or,
    - Schedule the recurring backups during off-peak hours.
  - Although CPU spikes may occur, Memory is often the main issue.
- Quiesced Snapshots—vRealize Log Insight does not support quiesced snapshots. If you are using any backup, restore, or disaster recovery tools that support quiesced snapshots, make sure to disable quiescing before enabling backup.
Forwarders—Enable regular backup and/or replication of vRealize Log Insight forwarders using the same procedures as that of the vRealize Log Insight server(s).

Agent Support—vRealize Log Insight server support Linux and Windows agents
- If the agent configuration is created on the server side, a separate backup of the agent node is not required.
- If you use the agent nodes for more than installing the agent software and if these nodes need a full backup, follow the same backup procedure as any other virtual machine.
- If the agent configuration is done on the client side (on the agents) and if the agent nodes are used only to install vRealize Log Insight agent software on them, making a backup of the agent configuration file is sufficient. Backup the `liagent.ini` file and replace the file on the recovered agent or Linux or Windows machine with the backup file.

Backup Frequency—Confirm that the backup frequency and backup types are appropriately selected based on the available resources and customer-specific requirements.

Backup Schedules—Consider the following guidelines when scheduling recurring backups.
- In most tools that perform backup or replication operations, for a reasonable loaded cluster setup, the first time a backup is triggered it may take a while for the first backup operation to finish irrespective of the tool of choice.
- However, the first backup is usually a full backup. The successive backups, which can be incremental or full backups, finish relatively faster compared to the first backup operation.

Replication Type—The choice of replication type is also critical while configuring any virtual machine for disaster recovery. Consider (Recovery Point Objective (RPO), Recovery Time Objective (RTO), and Cost and Scalability while deciding on the replication type you plan to use.

Concurrent Backup Jobs—If the resources are not an issue and if it is supported by the tool, it is recommended to enable concurrent cluster node backups to speed up the backup process. Backup all the nodes at the same time.

Monitoring—As the backup is in progress, make sure to check any environment or performance issues in the vRealize Log Insight setup. Most backup, restore, and disaster recovery tools provide monitoring capabilities.

During the backup process, check all the relevant logs on the production system as the user interface may not display all issues.

**Restore and Disaster Recovery Guidelines**

Specific restoration and disaster recovery guidelines provide additional best practices.

- Restore State—Make sure the restored nodes are in powered Off state. As a best practice, restore the nodes in a specific order as well as apply manual configuration changes in some restore scenarios as described below.
- Restore Order—Ensure that the vRealize Log Insight master node is restored first before restoring worker nodes. Worker nodes themselves can be restored in any order. Once the vRealize Log Insight server (the master node and all the worker nodes if it’s a cluster setup) is restored, restore the forwarders if configured, followed by the restoration of any recovered agents.
- Restore Target—Depending on the tool used for restoring, it is possible to restore the virtual machines to the same host, to a different host on the same data center, or to a different host on a target remote data center.

In a disaster recovery scenario, sometimes you cannot restore to the same site if the primary site is fully down but based on the option you choose, there are some manual steps required to fully restore and bring the vRealize Log Insight cluster to an up and running state.
Unless the vRealize Log Insight cluster is fully down and not accessible, make sure the cluster instances are powered off before restoring the cluster to a new site.

Confirm there is no split-brain behavior when the same IP addresses and/or FQDNs are used on the recovery site. Confirm that no one is accidentally using a partially working cluster on the primary site.

IP Customization—When restoring a vRealize Log Insight cluster, if the same IP addresses are used, confirm that all restored nodes IP addresses and FQDNs are associated with their original counterparts. For example, the following scenario would fail: In a three node cluster with nodes A, B and C; node A is restored with IP address B, and/or node B is restored with IP address C and/or C with IP address A.

If the same IP addresses are used for only a sub-set of restored nodes, you should confirm for these nodes that all restored images are associated with their original IP addresses.

Restore Schedule—During an outage or disaster, it is recommended to recover vRealize Log Insight cluster as soon as possible. Having a well documented and tested recovery plan in place is very essential to quickly bring the cluster back live.

Monitoring—Most of the backup restore and disaster recovery tools provide some kind of monitoring view to keep a watch on the live progress of the restore operations to catch any failures or warnings during a restoration operation. Make sure to take appropriate actions on any identified issues.

Post Restore Configuration Changes—If any manual configuration changes are required before the site can be fully restored, follow the guidelines in the “Post-Recovery Configuration Change Guidelines,” on page 83.

Validation—When a successful restoration is complete, perform a quick spot check of the cluster that was restored.

Post-Recovery Configuration Change Guidelines

Depending on the recovery target and IP customizations applied during the backup configuration, manual configuration changes are required to one or more vRealize Log Insight nodes before the restored site can become fully functional.

Recovering to the Same Host

The procedure for recovering a vRealize Log Insight cluster to the same host should be straight-forward and can be performed by any tool.

If possible all network, IP, and FQDN settings that are used for the production environment should be preserved in the restored and recovered site.

During the restoration process, the original copy of the cluster is overwritten with the restored version unless a new name is provided to the virtual machine.

If the same IP addresses and FQDNs are used for the restored cluster nodes, which is true in the default settings, power down the existing cluster before beginning the restore operation.

After a successful restoration and a sanity check passes, delete the old copy to conserve resources and to prevent potential accidental split-brain situations when a user may power on the old copy.

Recovering to a Different Host

Recovering to a different host requires manual configuration changes on the vRealize Log Insight cluster. See “Recovering to a Different Host,” on page 84 for information about changes that are specific to vRealize Log Insight 3.0 GA and 2.5 GA builds and which can be used with any backup recovery tool. It is assumed that the restored vRealize Log Insight nodes have been assigned different IP addresses and FQDNs than their source counterparts from which a backup was taken.
Recovering vRealize Log Insight Forwarders

The manual instructions for recovering vRealize Log Insight forwarders are the same as that of the vRealize Log Insight server as described above.

Recovering vRealize Log Insight Agents

If the complete agent OS is backed up, follow the tool-specific workflow to recover the agent OS.

- If agent configuration is made on the client side (agent OS), replace the agent.ini using the backup copy.
- If configuration changes are made on the server side only (vRealize Log Insight master node), no backup and recovery is required for the agent virtual machines.

Confirming the Restoration

You must confirm that all restored vRealize Log Insight clusters are fully functional.

- Verify that you can access the vRealize Log Insight user interface using the Internal Load Balancer (ILB) IP address or FQDN (if configured) as well as access all individual cluster nodes using respective IP addresses or FQDNs.
- From the vRealize Log Insight Administration page:
  - Verify the status of cluster nodes from the cluster page and make sure the ILB (if configured) is also in an active state.
  - Verify the vSphere integration. If required, reconfigure the integration. This occurs when the ILB and/or the master node IP address or FQDN is changed post-recovery.
  - Verify the vRealize Operations Manager integration and reconfigure again if needed.
  - Verify that all content packs and UI features are functioning properly.
  - If configured, also verify that vRealize Log Insight forwarders and agents are functioning properly.
- Verify that other key features of vRealize Log Insight are functioning as expected.

Recovering to a Different Host

When you perform a restoration to a different host, there are configuration changes that must be made on the vRealize Log Insight cluster.

This task describes configuration changes that are specific to vRealize Log Insight 3.0 GA and 2.5 GA builds that can be used with any backup recovery tool. It is assumed that the restored vRealize Log Insight nodes have been assigned different IP addresses and FQDNs than their source counterparts from which a backup was taken.

Prerequisites
Read the guidelines and recommendations described in Chapter 8, “Backup, Restore, and Disaster Recovery,” on page 79.

Procedure

1. List all new IP addresses and FQDNs that were assigned to each vRealize Log Insight node.
2 Make the following configuration changes on the master node:

a Power on the master node if it is not ON already.

Note Steps b through e are applicable for vRealize Log Insight 2.5 GA build. Making changes to the configuration files directly from the appliance console is not officially supported beginning in vRealize Log Insight 3.0 GA. Please see this KnowledgeBase article to make these changes using the web UI interface in vRealize Log Insight 3.0 GA.

b Use SSH to connect as a root user to the node's virtual appliance.

c If the vRealize Log Insight service is running, stop the service first by running this command

```
    service loginsight stop
```

d Run

```
    cd /storage/core/loginsight/config
```

e Run

```
    cp loginsight-config.xml#<n> backup-loginsight-config.xml
```

where `<n>` represents the largest number that is automatically suffixed to `loginsight-config.xml` during configuration changes.

f Open the copied version of the configuration file in your favorite editor (or in the vRealize Log Insight 3.0 GA web UI as recommended above) and look for lines that resemble the following lines. This configuration change is applicable to both vRealize Log Insight 3.0 GA and 2.5 GA.

```
<distributed overwrite-children="true">
    <daemon host="prod-es-vrli1.domain.com" port="16520" token="c4c4c6a7-f85c-4f28-a48f-43ae27cd0e">
        <service-group name="standalone" />
    </daemon>
    <daemon host="192.168.1.73" port="16520" token="a5c65b52-aff5-43ea-8a6d-38807ebc6167">
        <service-group name="workernode" />
    </daemon>
    <daemon host="192.168.1.74" port="16520" token="a2b57cb5-a6ac-48ee-8e10-17134e1e462e">
        <service-group name="workernode" />
    </daemon>
</distributed>
```

g In the above code snippet, there are three nodes: the first one is the master node which shows `</service-group name="standalone">` and the remaining two nodes are worker nodes and show `</service-group name="workernode">`.

h For the master node, in the newly recovered environment, check to see if the DNS entry that was used in the pre-recovery environment can be reused.

- If the DNS entry can be reused, you only need to update the DNS entry to point to the new IP address of the master node.
- If the DNS entry cannot be reused, replace the master node entry with new DNS name (pointing to the new IP address).
- If the DNS name cannot be assigned, as a last option, update the configuration entry with the new IP address.

i Update the worker node IP addresses as well to reflect the new IP addresses.
In the same configuration file, look for entries that represent NTP, SMTP and database and appenders sections.

This applies to vRealize Log Insight 3.0 GA and 2.5 GA.

**NOTE** The `<logging><appenders>...</appenders></logging>` section is applicable only to the vRealize Log Insight 2.5 GA build and is not available in vRealize Log Insight 3.0 GA.

```xml
<ntp>
  <ntp-servers value="ntp1.domain.com, ntp2.domain.com" />
</ntp>

<smtp>
  <server value="smtp.domain.com" />
  <default-sender value="source.domain.com@domain.com" />
</smtp>

<database>
  <password value="xserrttt" />
  <host value="vrli-node1.domain.com" />
  <port value="12543" />
</database>

<logging>
  <appenders>
    <appender name="REMOTE"
      class="com.vmware.loginsight.commons.logging.ThriftSocketAppender">
      <param name="RemoteHost" value="vdli-node1.domain.com" />
    </appender>
  </appenders>
</logging>
```

- If the configured NTP server values are not valid any longer in the new environment, update these in the `<ntp>...</ntp>` section.
- If the configured SMTP server values are not valid any longer in the new environment, update these in the `<smtp>...</smtp>` section.
- Optionally, change the `default-sender` value in the SMTP section. The value can be any value but as a good practice, you should represent the source from where the email is being sent.
- In the `<database>...</database>` section, change the host value to point to the master node FQDN or IP address.
- In the `<logging><appenders>...</appenders></logging>` section, change the parameter value for `RemoteHost` to reflect the new master node FQDN or IP address.
In the same configuration file, update the vRealize Log Insight ILB configuration section:

For a vRealize Log Insight 3.0 GA appliance,

```xml
<load-balancer>
  <leadership-lease-renewal-secs value="5" />
  <high-availability-enabled value="true" />
  <high-availability-ip value="10.158.128.165" />
  <high-availability-fqdn value="LB-FQDN.eng.vmware.com" />
  <layer4-enabled value="true" />
  <ui-balancing-enabled value="true" />
</load-balancer>
```

For a vRealize Log Insight 2.5 GA appliance,

```xml
<load-balancer>
  <leadership-lease-renewal-secs value="5" />
  <high-availability-enabled value="true" />
  <high-availability-ip value="192.168.1.75" />
  <layer4-enabled value="true" />
</load-balancer>
```

Under the `<load-balancer>` section, update the `high-availability-ip` value if it's different from the current setting.

In vRealize Log Insight 3.0 GA, make sure to also update the FQDN of the load balancer.

Rename the updated configuration file to finish the changes.

**Note** This step is applicable for vRealize Log Insight 2.5 GA only. In vRealize Log Insight 3.0 GA the changes are made through web UI.

Run: `mv backup-loginsight-config.xml loginsight-config.xml#<n+1>` where `n` represents the current maximum number suffixed to the `loginsight-config.xml` files.

For vRealize Log Insight 2.5 GA, restart the vRealize Log Insight service; run: `service loginsight start`.

**Note** For vRealize Log Insight 3.0 GA, this can be achieved from the web UI by going to the Cluster tab on the Administration page. For each node listed, select its hostname or IP address to open the details panel and click Restart Log Insight. The configuration changes are automatically applied to all cluster nodes.

Wait two minutes after the vRealize Log Insight service starts in order to give enough time for Cassandra services to come up before bringing other worker nodes online.

**Note** Skip Step 3 through Step 9 for vRealize Log Insight 3.0 GA. These steps are only applicable for vRealize Log Insight 2.5 GA. For for vRealize Log Insight 3.0 GA, follow the instructions in Step 2.

3 SSH onto the first worker node using root credentials.

4 Stop the vRealize Log Insight service; run: `service loginsight stop`.

5 Copy the latest `loginsight-config.xml` file from the master node to the worker node.

6 On the worker node, run: `scp root@[master-node-ip]:/storage/core/loginsight/config/loginsight-config.xml#<n> /storage/core/loginsight/config/`

7 Run: `service loginsight start`. 
8 Wait two minutes after the vRealize Log Insight service starts in order to give enough time for Cassandra service to start completely.

9 Repeat Step 3 through Step 6 for each worker node.
Troubleshooting vRealize Log Insight

You can solve common problems related to vRealize Log Insight administration before calling VMware Support Services.

This chapter includes the following topics:

- “ESXi Logs Stop Arriving in vRealize Log Insight,” on page 89
- “vRealize Log Insight Runs Out of Disk Space,” on page 90
- “Download a vRealize Log Insight Support Bundle,” on page 91
- “Use the Virtual Appliance Console to Create a Support Bundle of vRealize Log Insight,” on page 91
- “Reset the Admin User Password,” on page 92
- “Reset the Root User Password,” on page 92
- “Alerts Could Not Be Delivered to vRealize Operations Manager,” on page 93
- “Unable to Log In Using Active Directory Credentials,” on page 93
- “SMTP does not work with STARTTLS option enabled,” on page 94
- “Upgrade Fails Because the Signature of the .pak file Cannot Be Validated,” on page 95
- “Upgrade Fails with an Internal Server Error,” on page 95

ESXi Logs Stop Arriving in vRealize Log Insight

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

Problem

Configuration changes in vRealize Log Insight require that you restart the vRealize 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 9-1. ESXi Versions That Stop Sending Syslog Messages

<table>
<thead>
<tr>
<th>Communication Protocol</th>
<th>Affected ESXi Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>• ESXi 5.0.x</td>
</tr>
<tr>
<td></td>
<td>• ESXi 5.1.x</td>
</tr>
<tr>
<td>UDP</td>
<td>ESXi 5.0 and 5.0 Update 1</td>
</tr>
</tbody>
</table>

**IMPORTANT** The issue is fixed in ESXi 5.1 Update 2 and ESXi 5.0, Patch ESXi500-201401401-BG. VMware recommends that you apply the update or patch to be sure that your ESXi hosts do not stop sending syslog messages to their remote destinations. For more information see https://www.vmware.com/support/vsphere5/doc/vsphere-esxi-51u2-release-notes.html and VMware ESXi 5.0, Patch ESXi500-201401401-BG: Updates esx-base (2065691). If you do not wish to apply the update or patch, use the following solution.

**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 vRealize Log Insight. For details about syslog problems and solutions, see VMware ESXi 5.x host stops sending syslogs to remote server (2003127).

vRealize Log Insight Runs Out of Disk Space

A vRealize Log Insight master or worker node might run out of disk space if you are using a small virtual disk, and archiving is not enabled.

**Problem**

vRealize 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, vRealize 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 vRealize 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, vRealize Log Insight runs out of disk.

If archiving is enabled, vRealize Log Insight archives the bucket before retiring it. If the free space is filled before the old bucket is archived and retired, vRealize Log Insight runs out of disk.

**Solution**

- Increase the storage capacity of the vRealize Log Insight virtual appliance. See “Increase the Storage Capacity of the vRealize Log Insight Virtual Appliance,” on page 16.
Download a vRealize Log Insight Support Bundle

If vRealize 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 vRealize Log Insight Web user interface as a user with the Edit Admin permission. The URL format is https://log-insight-host, where log-insight-host is the IP address or host name of the vRealize 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 vRealize 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 vRealize Log Insight

If you cannot access the vRealize 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 vRealize Log Insight virtual appliance.

Prerequisites

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

Procedure

1. Establish an SSH connection to the vRealize Log Insight vApp and log in as the root user.
2. To generate the support bundle, 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 xxxx 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 Admin user forgets the password to the Web user interface, the account becomes unreachable.

Problem

If vRealize 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 vRealize Log Insight, the whole Web user interface becomes inaccessible.

Cause

vRealize 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

Prerequisites

- Verify that you have the root user credentials to log in to the vRealize Log Insight virtual appliance. See “Configure the Root SSH Password for the Log Insight Virtual Appliance,” on page 14
- To enable SSH connections, verify that TCP port 22 is open.

Procedure

1. Establish an SSH connection to the vRealize Log Insight virtual appliance and log in as the root user.
2. Type `li-reset-admin-pw.sh` and press Enter.
   The script resets the Admin user password, generates a new password and displays it on the screen.

What to do next

Log in to the vRealize Log Insight Web user interface with the new password 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 vRealize Log Insight virtual appliance.

Problem

If you cannot establish SSH connections or use the console of the vRealize 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 vRealize 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 vRealize Operations Manager**

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

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

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

**Unable to Log In Using Active Directory Credentials**
You cannot log in to the vRealize Log Insight Web user interface when you use Active Directory credentials.

**Problem**
You cannot log in to vRealize Log Insight by using your Active Directory domain user credentials, despite that an administrator has added your Active Directory account to vRealize Log Insight.
Cause
The most common causes are expired passwords, incorrect credentials, connectivity problems, or lack of synch between the vRealize 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 the latest vRealize Log Insight configuration at `/storage/core/loginsight/config/loginsight-config.xml#{number}` where `[number]` is the largest.
- Find the latest configuration file: `/storage/core/loginsight/config/loginsight-config.xml#{number}` where `[number]` is the largest.
- Verify vRealize Log Insight has connectivity to the Active Directory server.
- Go to the Authentication section of the Administration page of the vRealize Log Insight Web user interface, fill in your user credentials, and click the Test Connection button.
- Check the vRealize Log Insight `/storage/var/loginsight/runtime.log` for messages related to DNS problems.
- Verify that the vRealize Log Insight and Active Directory clocks are in synch.
- Check the vRealize Log Insight `/storage/var/loginsight/runtime.log` for messages related to clock skew.
- Use an NTP server to synchronize the vRealize Log Insight and Active Directory clocks.

SMTP does not work with STARTTLS option enabled

When you configure the SMTP server with the STARTTLS option enabled, test emails fail. Add your SSL certificate for the SMTP server to the Java truststore to resolve the problem.

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

Procedure
1. Establish an SSH connection to the vRealize Log Insight vApp and log in as the root user.
2. Copy the SSL certificate for the SMTP server to the vRealize Log Insight vApp.
3. Run the following command.
   ```bash
   /usr/java/latest/bin/keytool -import -alias certificate_name -file path_to_certificate -keystore /usr/java/latest/lib/security/cacerts
   ```
   **Note:** The outer quotes are inserted by using the back quote symbol that is on the same key as tilde on your keyboard. Do not use single quotes.
4. Enter the default the password `changeit`.
5. Run the service loginsight restart command.

What to do next
Navigate to Administration > Smtp and use Send Test Email to test your settings. See “Configure the SMTP Server for vRealize Log Insight,” on page 25.
Upgrade Fails Because the Signature of the .pak file Cannot Be Validated

vRealize Log Insight upgrade fails because of a corrupted .pak file, expired license or insufficient disk space.

**Problem**

Upgrading vRealize Log Insight fails and you see an error message Upgrade Failed. Failed to upgrade: Signature of the PAK file cannot be validated.

**Cause**

The error might occur for the following reasons:

- The uploaded file is not a .pak file.
- The uploaded .pak file is not complete.
- The license of vRealize Log Insight has expired.
- The vRealize Log Insight virtual appliance root file system does not have enough disk space.

**Solution**

- Verify that you are uploading a .pak file.
- Verify the md5sum of the .pak file against the VMware download site.
- Verify that at least one valid license is configured on vRealize Log Insight.
- Log in to the vRealize Log Insight virtual appliance and run `df -h` to check the available disk space.

**NOTE** Do not put files on the vRealize Log Insight virtual appliance root file system.

Upgrade Fails with an Internal Server Error

vRealize Log Insight upgrade fails with an Internal Server Error because of a connection problem.

**Problem**

Upgrading vRealize Log Insight fails and you see an error message Upgrade Failed. Internal Server Error.

**Cause**

A connection problem occurred between the client and the server. For example, when you attempt to upgrade from a client that is on a WAN.

**Solution**

- Upgrade LI from a client on the same LAN as the server.
Index

A
active directory
  groups 52
  users 51
Active Directory credentials 93
Active Directory integration with vROPs 70
AD
  authentication 55
  groups 52
  SSL 55, 56
  TCL 55
  users 51
adapter 71
add a search domain 70
add cpu 38
add memory 38
adding disks 16
admin password 92
agent groups
  add content pack group 47
  create 46
  delete 48
  edit 47
  working with 45
agents
  content pack agent group 47
  create group 46
  delete group 48
  edit group 47
  groups 45
alarms 63
API 31
appliance deployment 39
archive export, archive export to JSON, archive export to text file 34

B
backup recommendations 81
backup and replication guidelines 81
backup and restoration guidelines 80
backup best practices 79

certificate file, combine 29
certificate authority signing request 29
certificate signing request, generate 28
CLI upgrade 9
cluster mode 41
configuration limits 13
configure ESXi 64
configure SSL connection 30
content pack 72
create a user role 54
create agent group 46
custom certificates 26
custom SSL certificate, upload 29

D
data archiving 17
data set 53
default timeout 33
delete agent group 48
deployment 39
disable timeout 33
disabling launch in context 76
disabling trace data 38
domain account 51
domain groups 52

e
disable timeout 33
disabling launch in context 76
disabling trace data 38
domain account 51
domain groups 52

e
disable timeout 33
disabling launch in context 76
disabling trace data 38
domain account 51
domain groups 52
EEE
edit agent group 47
e-mail system alerts 25
enforce SSL connection 31
ESXi configuration 64
event forwarding, configure event forwarding, forward events 35, 36
events 63

F
forced logout 37

G
glossary 5

H
health 59
hosts monitoring 60
hosts list 60
hosts overview 60
importing logs 33
ingestion load balancer 43
installation 39
integrated load balancer 43
integrating Log Insight 61
integration
vCenter Server 62
vRealize Operations Manager 68
vSphere 62
intended audience 5
internal server error 95
IP address
change 15
configuration 15
IP address settings 15

join cluster 41

launch in context
disabling 75
enable 72
LDAP SSL 56
licensing 15
Linux Agent 31
load balancer 64
log forwarding
ESXi 64
ESXi syslog 65
syslog 66
vCenter Server Appliance 67
Log Insight cluster, adding worker nodes 39
Log Insight notifications 69
log files 91
Log Insight, upgrading through UI, upgrading to cluster 10
log insight adapter 76
Log Insight Agents 31
Log Insight adapter 71
Log Insight archive format 33
Log Insight Linux Agent 30
Log Insight Windows Agent 30
log policies 16
logging all users out 37
Loginsight, running as syslog server 64
logs import 33

monitor agents 45

N
NFS 17
notification events 61, 69
notifications, Log Insight 69

out of disk 90

P
PAK file error 95
password
admin 92
root 92
password SSH 14
PEM file, create 29
permissions 50
post-recovery configuration change guidelines 83
powering off 37
recoverying to a different host 84
red sign in toolbar 93
remove node 42
remove worker 42
restaring 37
restoration and disaster recovery guidelines 82
role-based access control 49, 50, 53
roles 50
root password 14, 92
root SSH 14
running out of disk 90

scale out alerts 23
secure connection 30
security policy 49
security model 49
service, restarting 37
session timeout 33
signed certificate, upload 29
SMTP 25
SMTP troubleshooting 94
SSH root 14
SSL 36, 56
ssl certificates 26
SSL configuration 31
SSL certificate for STARTTLS 94
SSL functionality 30
SSL parameters 31
STARTTLS troubleshooting 94
storage increasing 16
support bundle 91
supported upgrades 7
syslog 64
syslog configuration 64
system notification 18
system notifications 19, 23
system alerts 25
system health 59
system logs 91

T
tasks 63
time synchronization 24
timeout, modifying 33
timeout, disabling 33
trace data, stop sending 38
troubleshooting, ESXi logs 89

U
UI upgrade 10
unable to log in 93
unable to send alerts 93
upgrade paths 7
upgrade worker 8
upgrade cluster 7, 8
upgrade fails 95
upgrade node 8
upgrading
  CLI 9
  through UI 10
user accounts
deleting 55
  new 50
user logins 50
user access to specific data 53
user roles 54

V
vCenter Server
  alarms 63
  events 63
  tasks 63
vCenter Server Appliance 67
vC Ops integration 70
virtual appliance deployment 39
virtual appliance health 59
vRealize Operations Manager 61, 72
vRealize Operations Manager content pack 72
vSphere integration 62

W
Windows Agent 31
worker node 41
worker node, adding to a cluster 39