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

VMware vRealize Log Insight Getting Started Guide 5

1 Before You Install vRealize Log Insight 7
   Supported Log Files and Archive Formats in vRealize Log Insight 7
   Security Requirements 7
   Product Compatibility 8
   Minimum Requirements 9
   Sizing the vRealize Log Insight Virtual Appliance 10
   Integrating vRealize Log Insight and vRealize Operations Manager 11
   Life Cycle of an Event 11
   Key Aspects of the Event Life Cycle 12

2 Installing vRealize Log Insight 15
   Deploy the vRealize Log Insight Virtual Appliance 15
   Start New Standalone Deployment 17
   Join Existing Deployment 19

3 The Customer Experience Improvement Program 21
   Trace Data that vRealize Log Insight Collects 21

Index 23
The VMware vRealize Log Insight Getting Started Guide provides information about deploying and configuring VMware® vRealize™ Log Insight™, including how to size the vRealize Log Insight virtual appliance to receive log messages from your environment.

**Intended Audience**

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

To start using vRealize Log Insight in your environment, you must deploy the vRealize Log Insight virtual appliance and apply several basic configurations.

This chapter includes the following topics:

- “Supported Log Files and Archive Formats in vRealize Log Insight,” on page 7
- “Security Requirements,” on page 7
- “Product Compatibility,” on page 8
- “Minimum Requirements,” on page 9
- “Sizing the vRealize Log Insight Virtual Appliance,” on page 10
- “Integrating vRealize Log Insight and vRealize Operations Manager,” on page 11
- “Life Cycle of an Event,” on page 11
- “Key Aspects of the Event Life Cycle,” on page 12

**Supported Log Files and Archive Formats in vRealize Log Insight**

You can use vRealize Log Insight to analyse any unstructured or structured log files.

If the source host has the capability to send log events over either the syslog protocol or HTTP, Log Insight can accept the data. To analyze historic data you can import log files that were archived by vRealize Log Insight.

See Import a Log Insight Archive into 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.

**Security Requirements**

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

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

IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of vRealize Log Insight must read the VMware vRealize Log Insight Security Guide.
The Security Guide contains concise references to the security features of vRealize Log Insight. Topics include the product external interfaces, ports, authentication mechanisms, and options for configuration and management of security features.

For information about securing your virtual environment, see the *VMware vSphere Security Guide* and the Security Center on the VMware Web site.

**Product Compatibility**

vRealize Log Insight collects data over the syslog protocol and HTTP, can connect to vCenter Server to collect events, tasks, and alarms data, and can integrate with vRealize Operations Manager to send notification events and enable launch in context. Check the *VMware vRealize Log Insight Release Notes* for latest updates on supported product versions.

**Virtual Appliance Deployment**

You must and deploy the vRealize Log Insight virtual appliance using vSphere. Always use a vSphere Client to connect to a vCenter Server. The vRealize Log Insight virtual appliance should be deployed on an ESX/ESXi host version 4.1 or later that is managed by vCenter Server version 4.1 or later.

**Syslog Feeds**

vRealize Log Insight collects and analyses syslog data over the following ports and protocols.

- 514/UDP
- 514/TCP
- 1514/TCP (SSL)

You must configure environment components such as operating systems, applications, storage, firewalls, and network devices to push their syslog feeds to vRealize Log Insight.

**API Feeds**

The vRealize Log Insight Ingestion API collects data over the following port and protocol.

- 9000/TCP
- 9543/TCP (SSL)

**vSphere Integration**

You can configure vRealize Log Insight to pull data for tasks, events, and alarms that occurred in one or more vCenter Server instances. vRealize Log Insight uses the vSphere API to connect to vCenter Server systems and collect data.

You can configure ESXi hosts to forward syslog data to vRealize Log Insight.

<table>
<thead>
<tr>
<th>Table 1-1. Supported vSphere Product Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of Integration</strong></td>
</tr>
<tr>
<td>Tasks, events, and alarms data collection</td>
</tr>
<tr>
<td>Syslog feeds</td>
</tr>
</tbody>
</table>

See *Connect Log Insight to vCenter Server 5.1.x systems*. 
vRealize Operations Manager Integration

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

- vRealize Log Insight can send notification events to vRealize Operations Manager.
  See Configure Log Insight to Send Notification Events to vRealize Operations Manager.
- The launch in context menu of vRealize Operations Manager can display actions related to vRealize Log Insight.
  See Enable Launch in Context for Log Insight in vRealize Operations Manager.

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

<table>
<thead>
<tr>
<th>Product Deliverable</th>
<th>Notification Events</th>
<th>Launch in Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Operations Manager vApp</td>
<td>vSphere UI 5.7.1 and later</td>
<td>5.7.1 and later</td>
</tr>
<tr>
<td></td>
<td>Custom UI 5.6 and later</td>
<td></td>
</tr>
<tr>
<td>vRealize Operations Manager Installable</td>
<td>5.7.0 Hot Fix 1 and later</td>
<td>5.7.1 and later</td>
</tr>
</tbody>
</table>

Minimum Requirements

VMware distributes vRealize Log Insight as a virtual appliance in OVA file format. Various resources and applications must be available for the virtual appliance to run successfully. For the most up-to-date information about requirements, check the latest release notes.

Virtual Hardware

During deployment of the vRealize Log Insight virtual appliance you can select different sizes according to the ingestion requirements for the environment. An extra small configuration is the smallest supported configuration and can support log volumes of 3GB a day for about 10 users. The extra small configuration requires the following virtual resources.

- 2 vCPUs, 2GHz each
- 4GB RAM
- Approximately 144GB storage space

For complete resources requirements based on ingestion requirements, see “Sizing the vRealize Log Insight Virtual Appliance,” on page 10

Supported Browsers

You can use one of the following browsers to connect to the vRealize Log Insight Web user interface. More recent browser versions also work with vRealize Log Insight, but have not been validated.

**IMPORTANT** Cookies must be enabled in your browser.

- Mozilla Firefox 29.0 and 38.0
- Safari 6.0 , 7.0
- Google Chrome 29.0, 34.0 and 43.0
Internet Explorer 10.x and 11.x

**Note** Internet Explorer Document mode must be set to **Standards Mode**. Other modes are not supported. **Browser Mode**: Compatibility View is not supported.

**Required Network Ports**

The following network ports must be externally accessible.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/TCP</td>
<td>HTTP</td>
</tr>
<tr>
<td>443/TCP</td>
<td>HTTPS</td>
</tr>
<tr>
<td>514/UDP, 514/TCP</td>
<td>Syslog</td>
</tr>
<tr>
<td>1514/TCP</td>
<td>Syslog</td>
</tr>
<tr>
<td>9000/TCP</td>
<td>vRealize Log Insight Ingestion API</td>
</tr>
<tr>
<td>9543/TCP</td>
<td>vRealize Log Insight Ingestion API (SSL)</td>
</tr>
</tbody>
</table>

**Sizing the vRealize Log Insight Virtual Appliance**

By default, the vRealize Log Insight virtual appliance has 4 vCPUs, 8GB of virtual memory, and 132GB of disk space provisioned. vRealize Log Insight uses 100GB of the disk space to store raw data, index, metadata, and so on.

**Standalone Deployment**

You can change the settings according to the environment for which you intend to collect logs.

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.

The sizing is based on the following assumptions.

- Each vCPU is at least 2GHz.
- Each ESXi host sends up to 10 messages per second with an average message size of 170 bytes/message. This is roughly equivalent to 150MB/day/host.

**Note** For large installations, you must upgrade the virtual hardware version of the vRealize Log Insight virtual machine. vRealize Log Insight supports virtual hardware version 7 or later. Virtual hardware version 7 can support up to 8 vCPUs. Therefore, you must upgrade to virtual hardware version 8 or later for ESXi 5.x if you plan to provision 16 vCPUs. You use the vSphere Client to upgrade the virtual hardware. If you want to upgrade virtual hardware to the latest version, read and understand the information in the VMware knowledge base article [Upgrading a virtual machine to the latest hardware version (1010675)](https://kb.vmware.com/kb/1010675).
Cluster Deployment

Use a medium configuration, or larger, for the master and worker nodes in a vRealize Log Insight cluster. The number of events per second increases linearly with the number of nodes. For example, in a cluster of 3-12 nodes (2 nodes are not supported), the net in a 12 node cluster is 180,000 events per second (EPS) or 2.7 TB of events per day.

Reducing the Memory Size

If you want to use the Extra Small version of the appliance on your laptop, but the laptop does not have enough memory, you can reduce the memory size to 2GB.

Integrating vRealize Log Insight and vRealize Operations Manager

To enable integration between vRealize Log Insight and vRealize Operations Manager, configuration must be performed in both products.

Procedure

1. Install the vRealize Log Insight Management Pack into vRealize Operations Manager.
   The vRealize Log Insight Management Pack is required for the Launch in Context functionality between the two products. The vRealize Log Insight Management Pack is available with the vRealize Operations Manager download file or on the VMware Solution Exchange website.
2. Configure vRealize Log Insight to connect to vRealize Operations Manager.
3. Configure vRealize Log Insight alerts to forward information to vRealize Operations Manager.
   See the Configure vRealize Log Insight to Send Notification Events to vRealize Operations Manager topic in the vRealize Log Insight Administration Guide.
   See the Enable Launch in Context for vRealize Log Insight in vRealize Operations Manager in the vRealize Log Insight Administration Guide.

Life Cycle of an Event

The end-to-end life cycle of a log message or event includes multiple stages as the data flows in and out of vRealize Log Insight from agent read, parse, ingestion, indexing (buckets), alerting, query, archive (bucket seal and ship), and deletion.

An event is...
- Generated on a device (outside of vRealize Log Insight)
- Picked up and sent to vRealize Log Insight (inside and/or outside Log Insight)
  - Log Insight agent using ingestion API or syslog
  - Third party agent such as rsyslog, syslog-ng or log4j using syslog
  - Custom writing to ingestion API (e.g. log4j appender)
  - Custom writing to syslog (e.g. log4j appender)
- Received by vRealize Log Insight
  - If using ILB then L4 LB directs the event to a single node which is responsible for processing it
  - Event is declined — client handles declines (UDP drops, TCP uses protocol settings, CFAPI uses disk-backed queue)
Event is accepted and client is notified

Passed through the vRealize Log Insight ingestion pipeline

Keyword index is created/updated — index is stored in proprietary format on local disk

Machine learning clusters event — clustering is stored in Cassandra

Event is stored in compressed proprietary format on the local disk in a bucket

Queried

Keyword and glob queries are matched against the keyword index

Regex is matched against compressed events

Archived

Bucket seal and marked as archived

Deleted

Buckets are deleted in a FIFO model

Key Aspects of the Event Life Cycle

As an event ages, there are key characteristics that define the life cycle.

- Each event ages as new events come in.
- Each event is stored in a single on-disk bucket.
- Buckets are not replicated across Log Insight nodes — if you lose a node then you lose the data on that node.
- A bucket can be a maximum of 1GB in size.
- When a bucket reaches 1GB, it is sealed.
- A sealed bucket is immutable — it is readable but you cannot write to it.
- Buckets are kept based on /storage/core – 3% and deleted on a FIFO model.
- Each bucket is sealed and then marked to be archived.
- Once a sealed bucket is archived it is marked as archived. This means an event may be retained locally and in the archives at the same time.
- Once an event is deleted locally it can no longer be queried unless imported from the archive using the CLI.
- Once all events for a machine learning cluster are deleted from vRealize Log Insight, the cluster is removed from Cassandra.
- vRealize Log Insight automatically rebalances all incoming events fairly across nodes in the cluster. For example, even if a node is explicitly sent an event, it may not be the node to ingest the event.
- Event metadata is stored in a proprietary format on a single vRealize Log Insight node and not in a database.
- The node an event was ingested on cannot be determined.
- Events are stored locally in buckets that can grow up to 1GB in size.
- Buckets are not replicated across nodes.
- Once a bucket gets to 1GB it is sealed.
- After a bucket is sealed it can be archived and marked as archived.
- An event can exist locally on a node as well as on the archive.
- Buckets are deleted in a FIFO model.
- All buckets are stored on the /storage/core partition.
- vRealize Log Insight deletes old buckets when less than 3% of available space is available.

**NOTE**  A near-full /storage/core partition is usual and expected. That partition should never reach 100% because vRealize Log Insight manages that partition. However, you should not attempt to store data on that partition as it may interfere with the old bucket delete process.

**IMPORTANT**  vRealize Log Insight

- Does not move data to the archive location right before deleting.
- Does not consume disk space.
- Does not require an Administrator to delete data.
- Does not store received log data replicated in Cassandra.
vRealize Log Insight is delivered as a virtual appliance that you must deploy in your environment. To deploy the vRealize Log Insight virtual appliance, follow the standard OVF deployment procedure.

This chapter includes the following topics:
- “Deploy the vRealize Log Insight Virtual Appliance,” on page 15
- “Start New Standalone Deployment,” on page 17
- “Join Existing Deployment,” on page 19

### 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>
</tbody>
</table>
## Log Ingest Rate

<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>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.
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 Edit Settings.</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.

Start New Standalone Deployment

When you access the vRealize Log Insight Web interface for the first time after the virtual appliance deployment or after removing a worker node from a cluster, you must complete the initial configuration steps.

All settings that you modify during the initial configuration are also available in the Administration Web user interface.

For information about the trace data that vRealize Log Insight might collect and send to VMware if you choose to participate in the Customer Experience Improvement Program, see Chapter 3, “The Customer Experience Improvement Program,” on page 21.

Prerequisites

- In the vSphere Client, note the IP address of the vRealize Log Insight virtual appliance. For more information, see the VMware vSphere Documentation Center.
- Verify that you are using a supported browser, see the VMware vSphere Documentation Center.
- Verify that you have a valid license key. You can request an evaluation or permanent license key by using your account to My VMware™ https://my.vmware.com/.
- If you want to use local, vCenter Server, or Active Directory credentials to integrate vRealize Log Insight with vRealize Operations Manager, verify that these users are imported in vRealize Operations Manager Custom user interface. For instructions about configuring LDAP, see the vRealize Operations Manager Documentation Center.

Procedure

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

   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.

   The initial configuration wizard opens.

2. Click Start New Deployment.
3 Set the password for the Admin user and click **Save and Continue**.
   Optionally, you can provide an email address for the admin user.

4 Enter the license key, click **Set Key**, and click **Continue**.

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

6 (Optional) To opt out of the Customer Experience Improvement Program, clear the **Send weekly Trace Data to VMware as part of the Customer Experience Improvement Program** checkbox. Click **Save and Continue**.

7 (Optional) Select the **Always Use English** checkbox to ensure that the user interface and content is always displayed in English.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP server (recommended)</td>
<td>By default, vRealize Log Insight is configured to synchronize time with public NTP servers. If an external NTP server is not accessible due to firewall settings, you can use the internal NTP server of your organization. Use commas to separate multiple NTP servers.</td>
</tr>
<tr>
<td>ESX/ESXi host</td>
<td>If no NTP servers are available, you can sync the time with the ESXi host where you deployed the vRealize Log Insight virtual appliance.</td>
</tr>
</tbody>
</table>

9 Click **Save and Continue**.

10 Specify the properties of an SMTP server to enable outgoing alert and system notification emails.
   To verify that the SMTP configuration is correct, type a valid email address and click **Test**.
   vRealize Log Insight sends a test email to the address that you provided.

11 Click **Save and Continue**.

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

**What to do next**

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

- Assign a permanent license to vRealize Log Insight. See **Assign a Permanent License to Log Insight**.

- Install the vRealize Log Insight adapter in vRealize Operations Manager standalone to enable the Launch in Context functionality. See **Install the Log Insight Adapter in vRealize Operations Manager Standalone**.

- Install the vRealize Log Insight Windows Agent to collect events from Windows event channels, Windows directories, and flat text log files. See **Installing the Log Insight Windows Agent as a Windows Service**.
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.
The Customer Experience Improvement Program

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

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

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

Trace Data that vRealize Log Insight Collects

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

Categories of Information in Trace Data

Trace data contains the following categories of information.

- **alert.log**: Contains information about user defined alerts that have been triggered.
- **cassandra.log**: Contains information regarding cluster configuration storage and replication in Apache Cassandra.
- **li-vsphere.log**: Contains information regarding the integration between vRealize Log Insight and vSphere.
- **loginsight_daemon_std out.log**: Contains information about the standard output of vRealize Log Insight daemon.
- **pgsql.log**: Contains information about events related to the Postgres server, prior to upgrade.
- **runtime.log**: Contains information about low-level system trace activities conducted by vRealize Log Insight, including indexing, garbage collection, and monitoring activities. If an error occurs while vRealize Log Insight is processing data or a query, information about the error appears in the runtime.log file.
- **systemalert.log**: Contains information about system alerts that vRealize Log Insight sends.
**ui.log**  
Contains information regarding interactions with user interface components and parameters, such as which buttons were pressed or which options were selected from a drop-down menu.

**ui_runtime.log**  
Contains information about events that occur during runtime of the vRealize Log Insight user interface.

**upgrade.log**  
Contains information about events that occur during vRealize Log Insight upgrade.

**usage.log**  
Contains information regarding the queries that the query engine runs. Each line has the exact query that the search engine runs, including the time it was started, the length of time it ran, and if an error occurred during its execution.

**vcenter-operations.log**  
Contains information regarding the integration between vRealize Log Insight and vRealize Operations Manager, sending query alerts to vRealize Operations Manager and registering vRealize Log Insight with vRealize Operations Manager for launch in context.

**watchdog.log**  
Contains information from the watchdog process that monitors vRealize Log Insight and restarts the application if it fails or becomes unresponsive. The watchdog.log file contains information documenting when such failures are detected.

**Personal Information in Trace Data**

Trace data can also contain personal information, including:

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

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

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

You can stop the transfer of trace data to VMware at any time. See Stop Sending 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.
Index

A
about this guide 5
appliance deployment 15
appliance sizing 10

B
before you start 7
browsers, supported 9

C
cluster mode 19
compatibility 8
customer experience 21

D
deployment 15
disk size 10

E
event life cycle 11, 12

H
hardware requirements 9
hardware version 10

I
importing logs 7
initial configuration 17
installation 15
integration with vRealize Operations Manager 11

J
join cluster 19

L
life cycle 12
log formats 7
Log Insight, installing 15

M
master node 19
memory 10

P
ports, requirements 9

Q
quick start 7

R
requirements
  hardware 9
  network ports 9
  supported browsers 9
runtime.log 21

S
security 7
setting up Log Insight 17
standalone deployment 17
start new deployment 17
supported logs 7

T
trace data 21

U
ui.log 21
usage.log 21

V
vCPU 10
virtual hardware 10
virtual appliance deployment 15
virtual appliance setup 17

W
watchdog.log 21
worker node 19