

Getting Started with vRealize Log Insight

May 24, 2022

vRealize Log Insight 8.0

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

<https://docs.vmware.com/>

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

Copyright © 2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

Getting Started for vRealize Log Insight 4

1 Before You Install vRealize Log Insight 5

Supported Log Files and Archive Formats in vRealize Log Insight 5

Security Requirements 6

Product Compatibility 6

Minimum Requirements 7

Planning Your vRealize Log Insight Deployment 9

Sizing the vRealize Log Insight Virtual Appliance 11

Integrating vRealize Log Insight and vRealize Operations Manager 13

2 Life Cycle of an Event 14

Key Aspects of the Event Life Cycle 15

3 Installing vRealize Log Insight 17

Deploy the vRealize Log Insight Virtual Appliance 17

Start a New vRealize Log Insight Deployment 20

Join an Existing Deployment 22

4 The Customer Experience Improvement Program 24

Getting Started for vRealize Log Insight

Getting Started for vRealize Log Insight provides information about deploying and configuring VMware[®] vRealize[™] Log Insight[™], including how to size the vRealize Log Insight virtual appliance to receive log messages.

Use this information when you want to plan or install your deployment. This information is written for experienced Linux and Windows system administrators who are familiar with virtual machine technology and data center operations.

Before You Install vRealize Log Insight

1

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](#)
- [Security Requirements](#)
- [Product Compatibility](#)
- [Minimum Requirements](#)
- [Planning Your vRealize Log Insight Deployment](#)
- [Sizing the vRealize Log Insight Virtual Appliance](#)
- [Integrating vRealize Log Insight and vRealize Operations Manager](#)

Supported Log Files and Archive Formats in vRealize Log Insight

You can use vRealize Log Insight to analyze unstructured or structured log data.

vRealize Log Insight accepts data from the following sources:

- Sources that support sending log streams with the syslog protocol.
- Sources that write log files and can run the vRealize Log Insight agent.
- Sources that can post log data with HTTP or HTTPS through the REST API. API documentation is available from vRealize Log Insight interface at https://<vRLI_host>/rest-api.
- Historic data that was archived by vRealize Log Insight.

The vSphere log parser allows you to import vSphere log bundles 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.

See [Import a Log Insight Archive into vRealize Log Insight](#) in *Administering vRealize Log Insight*.

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 security topics in *Administering vRealize Log Insight*.

These topics provide 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 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 is deployed on an ESX/ESXi host version 5.0 or later that is managed by vCenter Server version 5.0 or later.

Syslog Feeds

vRealize Log Insight collects and analyzes 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 ports and protocols.

- 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.

For compatibility information with specific versions of vCenter Server and ESXi, see the [VMware Product Interoperability Matrixes](#).

For information about connecting to a vSphere environment, see [Connect vRealize Log Insight to a vSphere Environment](#).

vRealize Operations Manager Integration

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

All supported versions of vCenter Operations Manager support notifications as well as Launch in Context.

- vRealize Log Insight can send notification events to vRealize Operations Manager.
See [Configure vRealize 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 vRealize Log Insight in vRealize Operations Manager](#).

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 from preset configuration sizes according to the ingestion requirements for your environment. The presets are certified size combinations of compute and disk resources, though you can add extra resources afterward. A small configuration, described in the following table, consumes the fewest resources while remaining supported. An extra-small configuration is also available, but it is suitable only for demos.

For complete resource requirements based on ingestion requirements, see [Sizing the vRealize Log Insight Virtual Appliance](#)

Table 1-1. Preset Values for Small Configurations

| Resources | Minimum Requirement |
|---------------|---------------------|
| Memory | 8 GB |
| vCPU | 4 |
| Storage Space | 530 GB |

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 45.0 and above
- Google Chrome 51.0 and above
- Safari 9.1 and above
- Internet Explorer 11.0 and above

Note

- Internet Explorer Document mode must be set to **Standards Mode**. Other modes are not supported.
- **Browser Mode:** Compatibility View is not supported.
- To use Internet Explorer with the vRealize Log Insight web client, Windows local storage integrity level must be configured as low.

Account Passwords

| Type | Requirements |
|--------------|--|
| Root | <p>Unless you specify a root password or use guest customization during the deployment of the OVA, the default credentials for the root user on the vRealize Log Insight virtual appliance are root/blank. You are prompted to change the root account password when you first access the vRealize Log Insight virtual appliance console.</p> <p>Note SSH is disabled until you set the root password.</p> |
| User Account | <p>User accounts that you create in vRealize Log Insight 3.3 and later require a strong password. The password must be at least 8 characters long and contain one uppercase character, one lowercase character, one number, and one special character.</p> |

Integration Requirements

| Product | Requirement |
|-----------------------------|---|
| vCenter Server | To pull events, tasks, and alarms data from a vCenter Server, you must provide a set of user credentials for that vCenter Server. The minimum role required to register and unregister vRealize Log Insight with a vCenter Server is Read-only . The role must be set at the vCenter Server level and propagated to child objects. To configure ESXi hosts that a vCenter Server manages, vRealize Log Insight requires additional privileges. |
| vSphere ESXi | vSphere ESXi 6.0 update 1 or later is required to establish SSL connections to vRealize Log Insight. |
| vRealize Operations Manager | To enable notification events and the launch-in-context functionality in a vRealize Operations Manager instance, you must provide user credentials for that vRealize Operations Manager instance. |

Network Port Requirements

The following network ports must be externally accessible.

| Port | Protocol |
|------------------|--|
| 22/TCP | SSH |
| 80/TCP | HTTP |
| 443/TCP | HTTPS |
| 514/UDP, 514/TCP | Syslog |
| 1514/TCP | Syslog ingestion via SSL only |
| 9000/TCP | vRealize Log Insight Ingestion API |
| 9543/TCP | vRealize Log Insight Ingestion API (SSL) |

Planning Your vRealize Log Insight Deployment

You can deploy vRealize Log Insight with a single node, single cluster, or cluster with forwarders.

Note External load balancers are not supported for use with vRealize Log Insight, including vRealize Log Insight clusters.

Installation Through vRealize Suite Lifecycle Manager

The vRealize Suite Lifecycle Manager automates installation, configuration, upgrade, patch, configuration management, drift remediation, and health for Suites products. As an alternative to installation with vRealize Log Insight, you can install vRealize Log Insight through the vRealize Suite Lifecycle Manager. You must be using vRealize Suite Lifecycle Manager 1.2 or later and vRealize Log Insight 4.5.1 or later. See [vRealize Suite Lifecycle Manager documentation](#) for more information.

Single Nodes

A basic vRealize Log Insight configuration includes a single node. Log sources can be applications, OS logs, virtual machine logs, hosts, the vCenter Server, virtual or physical switches and routers, storage hardware, and so on. Log streams are transported to the vRealize Log Insight node using syslog (UDP, TCP, TCP+SSL) or CFAPI (the vRealize Log Insight native ingestion protocol over HTTP or HTTPS), either directly by an application, syslog concentrator, or the vRealize Log Insight agent installed on the source.

As a best practice for single-node deployments to use the vRealize Log Insight Integrated Load Balancer (ILB) and to send queries and ingestion traffic to the ILB. This does not incur overhead and simplifies configuration if you want to add nodes to create a cluster for your deployment in the future.

As a best practice, do not use single nodes for production environments.

Clusters

Production environments generally require the use of clusters. Clusters must meet the following requirements:

- Nodes in clusters are all be of the same size and in the same data center.
- The ILB used with clusters requires that nodes be in the same L2 network.
- vRealize Log Insight virtual machines must be excluded from VMware NSX Distributed Firewall Protection.

This is because virtual IPs for clusters use a Linux Virtual Server in Direct Server Return Mode (LVS-DR) for load balancing. Direct Server Return is more efficient than routing all response traffic through a single cluster member. However, it also resembles spoofed traffic, which NSX Distributed Firewall blocks.

Sizing Clusters

A vRealize Log Insight single cluster configuration can include from three to 12 nodes and uses the ILB. A cluster requires a minimum of healthy three nodes to operate correctly.

Production environments require that nodes be at least of medium size. If you anticipate working with a large number of concurrent queries, including alerts, consider using large-sized nodes. For information about sizing, see [Sizing the vRealize Log Insight Virtual Appliance](#).

Although the minimum number of nodes in a vRealize Log Insight cluster is three, if there is failure of the nodes, a cluster with fewer than three healthy nodes will not be fully functional. Also, the number of healthy nodes in cluster must be greater than half of the total number of cluster nodes. For example, if you have a six-node cluster and three of the nodes become unavailable, the cluster is not fully functional until you remove the non-functional nodes from the cluster. Removal and reintroduction of a cluster node is not supported.

Clusters with Forwarders

A vRealize Log Insight cluster with forwarders configuration includes main indexing, storage, and a query cluster of three to 12 nodes using the ILB. A single log message is present in only one location within the main cluster, as for the single cluster.

The design is extended through the addition of multiple forwarder clusters at remote sites or clusters. Each forwarder cluster is configured to forward all its log messages to the main cluster and users connect to the main cluster, taking advantage of CFAPI for compression and resilience on the forwarding path. Forwarder clusters configured as top-of-rack can be configured with a larger local retention.

Cross-Forwarding for Redundancy

This vRealize Log Insight deployment scenario includes a cluster with forwarder that is extended and mirrored. Two main clusters are used for indexing, storage, and query. One main cluster is in each data center. Each is front-ended with a pair of dedicated forwarder clusters. All log sources from all top-of-rack aggregations concentrate at the forwarder clusters. You can independently query the same logs on both retention clusters.

vRealize Log Insight Integrated Load Balancer

To properly balance traffic across nodes in a cluster and to minimize administrative overhead, use the Integrated Load Balancer (ILB) for all deployments. This ensures that incoming ingestion traffic is accepted even if some vRealize Log Insight nodes are unavailable.

Sizing the vRealize Log Insight Virtual Appliance

By default, the vRealize Log Insight virtual appliance uses the preset values for small configurations.

Standalone Deployment

You can change the appliance settings to meet the needs of the environment for which you intend to collect logs during deployment.

vRealize Log Insight provides preset VM (virtual machine) sizes that you can select from to meet the ingestion requirements of your environment. These presets are certified size combinations of compute and disk resources, though you can add extra resources afterward. A small configuration consumes the fewest resources while remaining supported. An extra small configuration is suitable only for demos.

| Preset Size | Log Ingest Rate | Virtual CPUs | Memory | IOPS | Syslog Connections (Active TCP Connections) | Events per Second |
|-------------|-----------------|--------------|--------|------|---|-------------------|
| Extra Small | 6 GB/day | 2 | 4 GB | 75 | 20 | 400 |
| Small | 30 GB/day | 4 | 8 GB | 500 | 100 | 2000 |

| Preset Size | Log Ingest Rate | Virtual CPUs | Memory | IOPS | Syslog Connections (Active TCP Connections) | Events per Second |
|-------------|-----------------|--------------|--------|------|---|-------------------|
| Medium | 75 GB/day | 8 | 16 GB | 1000 | 250 | 5000 |
| Large | 225 GB/day | 16 | 32 GB | 1500 | 750 | 15,000 |

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 virtual CPU is at least 2 GHz.
- Each ESXi host sends up to 10 messages per second with an average message size of 170 bytes/message, which is roughly equivalent to 150 MB/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 virtual CPUs. Therefore, if you plan to provision 16 virtual CPUs, you must upgrade to virtual hardware version 8 or later for ESXi 5.x. 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 \(1010675\)](#).

Cluster Deployment

Use a medium configuration, or larger, for the primary 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 (clusters must have a minimum of three nodes), the Internet in a 12-node cluster is 180,000 events per second (EPS), or 2.7 TB of events per day.

Reducing the Memory Size

To use the **Extra Small** version of the appliance when your laptop does not have enough memory, you can reduce the memory size to 2 GB.

vRealize Log Insight Sizing Calculator

A calculator to help you determine sizing for vRealize Log Insight and network and storage use is available. This calculator is intended for guidance only. Many environment inputs are site-specific, so the calculator necessarily uses estimations in some areas. See <https://www.vmware.com/go/loginsight/calculator>.

Note The overall performance of vRealize Log Insight might degrade if forwarders are defined against the text field with complex or multiple conditions involving regular expressions, for example "**text=~\"Deleting the machine\"**". In such cases, specifically when the overall load on the cluster is high, performance might be delayed and disk blocks might be accumulated on each node of the cluster.

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 [Configure vRealize Log Insight to Send Notification Events to vRealize Operations Manager](#) in *Administering vRealize Log Insight*.

- 4 Enable vRealize Operations Launch In Context to query logs in vRealize Log Insight.

See [Enable Launch in Context for vRealize Log Insight in vRealize Operations Manager](#) in *Administering vRealize Log Insight*.

Life Cycle of an Event

2

Understanding how vRealize Log Insight processes messages and events is key to using vRealize Log Insight effectively.

The life cycle of a log message or event has multiple stages including reading, parsing, ingestion, indexing, alerting, query application, archiving, and deletion.

Events and messages transition through the following stages.

- 1 It is generated on a device (outside of vRealize Log Insight).
- 2 It is picked up and sent to vRealize Log Insight in one of the following ways:
 - By a vRealize Log Insight agent using ingestion API or syslog
 - Through a third-party agent such as rsyslog, syslog-ng, or log4j using syslog
 - By custom writing to ingestion API (such as log4j appender)
 - By custom writing to syslog (such as log4j appender)
- 3 vRealize Log Insight receives the event.
 - If you are using the integrated load balancer (ILB), the event is directed to a single node that is responsible for processing the event.
 - If the event is declined, the client handles declines with UDP drops, TCP with protocol settings, or CFAPI with a disk-backed queue.
 - If the event is accepted, the client is notified.
- 4 The event is passed through the vRealize Log Insight ingestion pipeline, from which the following steps occur:
 - A keyword index is created or updated. The index is stored in a proprietary format on a local disk.
 - Machine learning is applied to cluster events.
 - The event is stored in a compressed proprietary format on the local disk in a bucket.
- 5 The event is queried.
 - Keyword and glob queries are matched against the keyword index.
 - Regex is matched against compressed events.

- 6 The event is moved to a bucket and archived.
 - A bucket is sealed and archived when it reaches 0.5 GB.
- 7 The event is deleted.
 - Buckets are deleted in FIFO order.

For More Information

For more information, see the VMware Technical Publications video,



Life Cycle of a Log Event in vRealize Log Insight.

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_horp849x/uiConfId/50138843/)

This chapter includes the following topics:

- [Key Aspects of the Event Life Cycle](#)

Key Aspects of the Event Life Cycle

As an event ages, there are key aspects of event storage and management during the event life cycle to be aware of.

Event Storage

Each event is stored in a single on-disk bucket. When working with buckets, be aware of the following behaviors and characteristics.

- Buckets can reach a maximum size of 0.5 GB. When a bucket reaches 0.5 GB, it is sealed and queued for archiving. After a sealed bucket is archived, it is marked as archived. An event can be retained locally and in the archives at the same time.
- Buckets are not replicated across vRealize Log Insight nodes. If you lose a node, you lose the data on that node.
- All buckets are stored on the `/storage/core` partition.
- vRealize Log Insight deletes old buckets when the available space on the `/storage/core` partition is less than 3%. Deletion follows a FIFO model.

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, do not attempt to store data on that partition because it can interfere with the deletion of old buckets.

Event Management

As you set up and configure your product, it is helpful to be familiar with the following characteristics and behaviors of vRealize Log Insight events and event management.

- After an event is deleted locally, it can no longer be queried unless it is imported from the archive using the command-line interface.
- After all events for a machine learning cluster are deleted from vRealize Log Insight, the cluster is removed.
- vRealize Log Insight rebalances all incoming events fairly across nodes in the cluster. For example, even if a node is explicitly sent to an event, it might 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.
- An event can exist locally on a node and on the archive.

Installing vRealize Log Insight

3

vRealize Log Insight is delivered as a virtual appliance that you deploy in your vSphere environment.

After reviewing [Sizing the vRealize Log Insight Virtual Appliance](#), go to [Deploy the vRealize Log Insight Virtual Appliance](#). Whether you have a single node deployment or a clustered deployment, follow the standard OVF deployment procedure described in this section.

Note You can use vRealize Suite Lifecycle Manager 1.2 or later to install vRealize Log Insight 4.5.1 and later releases. See [vRealize Suite documentation](#) for more information.

This chapter includes the following topics:

- [Deploy the vRealize Log Insight Virtual Appliance](#)
- [Start a New vRealize Log Insight Deployment](#)
- [Join an Existing Deployment](#)

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 have 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 Select 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.

vRealize Log Insight provides preset VM (virtual machine) sizes that you can select from to meet the ingestion requirements of your environment. These presets are certified size combinations of compute and disk resources, though you can add extra resources afterward. A small configuration consumes the fewest resources while remaining supported. An extra small configuration is suitable only for demos.

| Preset Size | Log Ingest Rate | Virtual CPUs | Memory | IOPS | Syslog Connections (Active TCP Connections) | Events per Second |
|-------------|-----------------|--------------|--------|------|---|-------------------|
| Extra Small | 6 GB/day | 2 | 4 GB | 75 | 20 | 400 |
| Small | 30 GB/day | 4 | 8 GB | 500 | 100 | 2000 |
| Medium | 75 GB/day | 8 | 16 GB | 1000 | 250 | 5000 |
| Large | 225 GB/day | 16 | 32 GB | 1500 | 750 | 15,000 |

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 Select Storage 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 later, 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 expands as the amount of data saved on it increases. 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 Select networks page, set the networking parameters for the vRealize Log Insight virtual appliance. You can select the IPv4 or IPv6 protocol.

If you do not provide network settings, such as an IP address, DNS servers, and gateway information, vRealize Log Insight uses 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 a comma-separated list to specify domain name servers.

- 6 (Optional) On the Customize template page, set network properties if you are not using DHCP. Under Application, select the **Prefer IPv6 addresses** check box if you want to run the virtual machine in a dual stack network.

Caution Do not select the **Prefer IPv6 addresses** check box if you want to use pure IPv4 even with IPv6 supported in your network. Select the check box only if your network has a dual stack or pure stack support for IPv6.

- 7 (Optional) On the Customize template page, select **Other Properties** and set the root password for the vRealize Log Insight virtual appliance.

The root password is required for SSH. You can also set this password through the VMware Remote Console.

- 8 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.

- 9 Navigate to the **Console** tab and verify the IP address of the vRealize Log Insight virtual appliance.

| IP Address Prefix | Description |
|-------------------|--|
| https:// | The DHCP configuration on the virtual appliance is correct. |
| http:// | <p>The DHCP configuration on the virtual appliance failed.</p> <ul style="list-style-type: none"> a Power off the vRealize Log Insight virtual appliance. b Right-click the virtual appliance and select Edit Settings. c Set a static IP address for the virtual appliance. |

What to do next

- 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 a New vRealize Log Insight 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 finish 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 when you participate in the Customer Experience Improvement Program, see [Chapter 4 The Customer Experience Improvement Program](#).

Prerequisites

- In the vSphere Client, note the IP address of the vRealize Log Insight virtual appliance. For information about locating the IP address, see [Deploy the vRealize Log Insight Virtual Appliance](#).
- Verify that you are using a supported browser. See [Minimum Requirements](#).
- Verify that you have a valid license key. You can request an evaluation or permanent license key through your account on My VMware™ at <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](#).

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 **Add License Key**, and click **Save and Continue**.
- 5 On the General Configuration page, enter the email address to receive system notifications from vRealize Log Insight.
- 6 If you are using webhooks to send notifications to vRealize Operations Manager or a third-party application, enter a space-separated list of URLs in the **Send HTTP Post System Notifications To** text box.
- 7 (Optional) To leave the Customer Experience Improvement Program, deselect the **Join the VMware Customer Experience Program** option. Click **Save and Continue**.
- 8 On the Time Configuration page, set how time is synchronized on the vRealize Log Insight virtual appliance and click **Test**.

| Option | Description |
|---------------------------------|---|
| NTP server (recommended) | 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. |
| ESX/ESXi host | If no NTP servers are available, you can sync the time with the ESXi host where you deployed the vRealize Log Insight virtual appliance. |

- 9 Click **Save and Continue**.
- 10 (Optional) To enable outgoing alert and system notification emails, specify the properties of an SMTP server.
To verify that the SMTP configuration is correct, enter a valid email address and click **Test**. vRealize Log Insight sends a test email to the address that you provided.
- 11 (Optional) To provide a custom SSL certificate, upload a certificate file to the cluster in a PEM format. You can also view the details of the existing certificate.
The system adds the certificate to the truststores of all the nodes of the cluster and saves it for later use.
For information about the prerequisites of the custom SSL certificate, see [Install a Custom SSL Certificate](#).

12 Click **Save and Continue**.

Results

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

What to do next

- Navigate to the **Administration** tab. From the **vSphere Integration** page, 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](#) in *Administering vRealize Log Insight*.
- Configure the vRealize Log Insight adapter in vRealize Operations Manager to enable launch in context. See *Configuring vRealize Log Insight with vRealize Operations Manager* in the *vRealize Operations Manager Configuration Guide*.
- Install the vRealize Log Insight Windows Agent to collect events from Windows event channels, Windows directories, and flat text log files. See [Installing Windows Agents](#) in *Working with vRealize Log Insight Agents*.

Join an 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 in clusters. Clusters enable linear scaling of ingestion throughput, increase query performance, and allow high-availability ingestion. In cluster mode, vRealize Log Insight provides primary and worker nodes. Both primary and worker nodes are responsible for a subset of data. Primary nodes can query all subsets of data and aggregate the results. You might require more nodes to support site needs. You can use from three to 12 nodes in a cluster. This means a fully functional cluster must have a minimum of three healthy nodes. The majority of nodes in a larger cluster must be healthy. For example, if three nodes of a six-node cluster fail, none of the nodes functions fully until the failing nodes are removed.

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 primary vRealize Log Insight virtual appliance.
- Verify that you have an administrator account on the primary vRealize Log Insight virtual appliance.

- Verify that the versions of the vRealize Log Insight primary and worker nodes are in sync. Do not add an older version vRealize Log Insight worker to a newer version vRealize Log Insight primary 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 primary and click **Go**.

The worker sends a request to the vRealize Log Insight primary node to join the existing deployment.

- 4 Click **Click here to access the Cluster Management page**.
- 5 Log in as an administrator.

The Cluster page loads.

- 6 Click **Allow**.

The worker node joins the existing deployment and vRealize Log Insight begins to operate in a cluster.

What to do next

- Add more worker nodes as needed. The cluster must have a minimum of three nodes.

The Customer Experience Improvement Program

4

This product participates in VMware's Customer Experience Improvement Program (CEIP).

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at <https://www.vmware.com/solutions/trustvmware/ceip.html>.

To join or leave the CEIP for this product, see "Join or Leave the VMware Customer Experience Program" in *Administering vRealize Log Insight*.