

VMware vCenter Log Insight Getting Started Guide

vCenter Log Insight 1.5

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see <http://www.vmware.com/support/pubs>.

EN-001297-00

vmware[®]

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

<http://www.vmware.com/support/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2014 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

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

Contents

VMware vCenter Log Insight Getting Started Guide	5
1 Before You Install Log Insight	7
Supported Log Files and Archive Formats in Log Insight	7
Security Requirements	7
Product Compatibility	8
Minimum Requirements	9
Sizing the Log Insight Virtual Appliance	10
2 Installing Log Insight	11
Deploy the Log Insight Virtual Appliance	11
Configure Log Insight	13
3 The Customer Experience Improvement Program	15
Trace Data that Log Insight Collects	15
Index	17

VMware vCenter Log Insight Getting Started Guide

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

Intended Audience

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

Before You Install Log Insight

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

This chapter includes the following topics:

- [“Supported Log Files and Archive Formats in Log Insight,”](#) on page 7
- [“Security Requirements,”](#) on page 7
- [“Product Compatibility,”](#) on page 8
- [“Minimum Requirements,”](#) on page 9
- [“Sizing the Log Insight Virtual Appliance,”](#) on page 10

Supported Log Files and Archive Formats in Log Insight

You can use Log Insight to analyse historic data from imported log files.

You can import only log files that were archived by Log Insight.

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

Security Requirements

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

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

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

Product Compatibility

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

Virtual Appliance Deployment

Always use a vSphere Client to connect to a vCenter Server and deploy the Log Insight virtual appliance through the vCenter Server. The 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

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 Log Insight.

vSphere Integration

You can configure Log Insight to pull data for tasks, events, and alarms that occurred in one or more vCenter Server instances. 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 Log Insight.

Table 1-1. Supported vSphere Product Versions

Type of Integration	Supported Product Versions
Tasks, events, and alarms data collection	vCenter Server 5.1 and later
Syslog feeds	ESXi 4.1 and later

See topic *Connect Log Insight to vCenter Server 5.1.x Systems* in the Log Insight Administration Guide.

vCenter Operations Manager Integration

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

- Log Insight can send notification events to vCenter Operations Manager.
See the topic *Enable the Sending of notification Events to vCenter Operations Manager* in the Log Insight Administration Guide.
- The launch in context menu of vCenter Operations Manager can display actions related to Log Insight.
See topic *Enable Launch in Context for Log Insight in vCenter Operations Manager* in the Log Insight Administration Guide.

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

Product Deliverable	Notification Events	Launch in Context
vCenter Operations Manager vApp	<ul style="list-style-type: none"> ■ vSphere UI 5.7.1 and later ■ Custom UI 5.6 and later 	5.7.1 and later
vCenter Operations Manager Installable	5.7.0 Hot Fix 1 and later	5.7.1 and later

Minimum Requirements

VMware distributes Log Insight as a virtual appliance in OVA file format. Various resources and applications must be available for the virtual appliance to run successfully.

Virtual Hardware

To support log volumes of 1GB per hour for about 10 users, the Log Insight virtual appliance requires the following virtual resources. During deployment of the 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 Log Insight Virtual Appliance,”](#) on page 10

Supported Browsers

You can use one of the following browsers to connect to the Log Insight Web user interface.

IMPORTANT Cookies must be enabled in your browser.

- Mozilla Firefox 10.x, 19.x, 20.x, 21.0, and 23
- Safari 6.0
- Google Chrome 25.x, 26.x, 27.x, and 29
- Internet Explorer 9.x and 10.x

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

Adobe Flash Player is required for file upload operations, such as importing content packs, uploading custom content pack icon files, upgrading Log Insight through the Administration UI, and uploading custom SSL certificates.

Required Network Ports

The following network ports must be externally accessible.

Port	Protocol
22/TCP	SSH
80/TCP	HTTP
443/TCP	HTTPS

Port	Protocol
514/UDP, 514/TCP	Syslog
1514/TCP	Syslog

Sizing the Log Insight Virtual Appliance

By default, the Log Insight virtual appliance has 2 vCPUs, 4GB of virtual memory, and 144GB of disk space provisioned. Log Insight uses 100GB of the disk space to store raw data, index, metadata, and so on.

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.

Option	Environment size	Log Ingest Rate	vCPUs	Memory	IOPS
Extra Small	Up to 20 hosts	3GB/day	2	4GB	75
Small	Up to 100 hosts	15GB/day	4	8GB	500
Medium	Up to 250 hosts	37.5GB/day	8	16GB	1000
Large	Up to 750 hosts	112.5GB/day	16	32GB	1500

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 Log Insight virtual machine. 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 at the minimum (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 \(1010675\)](#).

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.

Installing Log Insight

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

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

This chapter includes the following topics:

- [“Deploy the Log Insight Virtual Appliance,”](#) on page 11
- [“Configure Log Insight,”](#) on page 13

Deploy the Log Insight Virtual Appliance

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

Prerequisites

- Verify that you have a copy of the Log Insight virtual appliance .ova file.
- Verify that you have permissions to deploy OVF templates to the inventory.
- Verify that your environment has enough resources to accommodate the minimum requirements of the Log Insight virtual appliance. See [“Minimum Requirements,”](#) on page 9.
- Verify that you read and understand the virtual appliance sizing recommendations. See [“Sizing the Log Insight Virtual Appliance,”](#) on page 10.

Procedure

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

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

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

- 4 On the Disk Format page, select a disk format.
 - **Thick Provision Lazy Zeroed** creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. The data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time, on first write from the virtual appliance.
 - **Thick Provision Eager Zeroed** creates a type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks.

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

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

NOTE Shrinking disks on the Log Insight virtual appliance is not supported and might result in data corruption or data loss.

- 5 (Optional) On the Properties page, set the networking parameters for the Log Insight virtual appliance. If you do not provide network settings, such as IP address, DNS servers, and gateway, Log Insight utilizes DHCP to set those settings.



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

Use comma to separate domain name servers.

- 6 Follow the prompts to complete the deployment.

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

After you power on the virtual appliance, an initialization process begins. The initialization process takes several minutes to complete. At the end of the process, the virtual appliance restarts.
- 7 Navigate to the **Console** tab and check the IP address of the Log Insight virtual appliance.

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

What to do next

- To enable SSH connections to the Log Insight virtual appliance, configure the root password in the virtual appliance console. See topic Configure the Root SSH Password for the Log Insight Virtual Appliance in the [Log Insight Administration Guide](#).

- Log in to the Log Insight Web interface to verify that the application is installed properly, and apply the initial configuration. See [“Configure Log Insight,”](#) on page 13.

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

Configure Log Insight

When you access the Log Insight Web interface for the first time after the virtual appliance deployment, you must complete the initial configuration steps.

All settings that you modify during the initial configuration are also available in the Administration Web user interface. You can change any setting at a later stage.

Prerequisites

- In the vSphere Client, check the IP address of the Log Insight virtual appliance.
- For information about the trace data that Log Insight might collect and send to VMware if you choose to participate in the Customer Experience Improvement Program, see [Chapter 3, “The Customer Experience Improvement Program,”](#) on page 15.
- For information on supported browser versions, see [“Minimum Requirements,”](#) on page 9.
- Verify that you have a valid license key. You can request an evaluation or permanent license key by using your account to My VMware™.
- If you want to use local, vCenter Server, or Active Directory credentials to integrate Log Insight with vCenter Operations Manager, verify that these users are imported in vCenter Operations Manager Custom user interface. For instructions about configuring LDAP, see the vCenter Operations Manager [Administration Guide](#).

Procedure

- 1 Use a supported browser to navigate to the Web user interface of Log Insight.
The URL format is [https:// log_insight-host/](https://log_insight-host/), where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.
The initial configuration wizard opens.
- 2 Set the password for the admin user, and click **Save and Continue**.
Optionally, you can provide an email address for the admin user.
- 3 Type the license key, click **Set Key**, and click **Continue**.
- 4 On the General Configuration page, type the email address to receive system notifications from Log Insight.
- 5 If you want to participate in the Customer Experience Improvement Program, select **Send weekly Trace Data to VMware as part of the Customer Experience Improvement Program**.
- 6 Click **Save and Continue**.

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

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

- 8 Click **Save and Continue**.
- 9 (Optional) To allow active directory users access in Log Insight, select **Enable Active Directory support** and click **Save and Continue**.

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

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

- 12 Click **Save and Continue**.

- 13 (Optional) Configure the integration between Log Insight and vCenter Operations Manager.
 - a Type the hostname and user credentials for the UI VM of the vCenter Operations Manager vApp, and click **Test Connection** to verify the connection.

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

- b To allow Log Insight to send alert notifications triggered by Log Insight alarms, select **Enable alerts integration**.
 - c To allow vCenter Operations Manager to launch Log Insight with an object-specific query, click **Enable Launch in Context**.

This operation might take a few minutes.

- 14 Click **Save and Continue**.


- 15 (Optional) To archive log data to an NFS location, select **Enable Data Archiving**, type the path to the storage location, and click **Test** to verify that Log Insight can connect to that storage.

- 16 Click **Save and Continue**.

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

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

What to do next

- Go to the **Administration** page by selecting the drop-down menu icon  in the navigation bar and use the **vSphere Integration** page to configure Log Insight to pull tasks, events, and alerts from vCenter Server instances, and to configure ESXi hosts to send syslog feeds to Log Insight.
- See the topic *Assign a Permanent License to Log Insight* in the *Log Insight Administration Guide*.
- See the topic *Install the Log Insight Adapter in vCenter Operations Manager Standalone* in the *Log Insight Administration Guide*.

The Customer Experience Improvement Program

3

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

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

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

Trace Data that Log Insight Collects

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

Categories of Information in Trace Data

Trace data contains the following categories of information.

runtime.log	Contains information about low-level system trace activities conducted by Log Insight, including indexing, garbage collection, and monitoring activities. If an error occurs while Log Insight is processing data or a query, information about the error appears in the <code>runtime.log</code> file.
ui.log	Contains information regarding interactions with user interface components and parameters, such as which buttons were pressed or which options were selected from a drop-down menu.
usage.log	Contains information regarding the queries that the query engine runs. Each line has the exact query that the search engine runs, including the time it was started, the length of time it ran, and if an error occurred during its execution.
watchdog.log	Contains information from the watchdog process that monitors Log Insight and restarts the application if it fails or becomes unresponsive. The <code>watchdog.log</code> file contains information documenting when such failures are detected.

Personal Information in Trace Data

Trace data can also contain personal information, including:

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

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

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

You can stop the transfer of trace data to VMware at any time. See the topic *Stop Sending Trace Data to VMware* in the *Log Insight Administration Guide*.

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

Index

A

about this guide **5**
appliance deployment **11**
appliance sizing **10**

B

before you start **7**

C

compatibility **8**
customer experience **15**

D

deployment **11**
disk size **10**

H

hardware version **10**

I

importing logs **7**
initial configuration **13**
installation **11**

L

log formats **7**
Log Insight, installing **11**

M

memory **10**

Q

quick start **7**

R

requirements **9**
runtime.log **15**

S

security **7**
setting up Log Insight **13**
supported logs **7**

T

trace data **15**

U

ui.log **15**
usage.log **15**

V

vCPU **10**
virtual hardware **10**
virtual appliance deployment **11**
virtual appliance setup **13**

W

watchdog.log **15**

