VMware vRealize Log Insight Security Guide

vRealize Log Insight 2.5

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-001662-00

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About VMware vRealize Log Insight Security Guide

The *VMware vRealize Log Insight Security Guide* provides a concise reference to the security features of Log Insight.

To help you protect your Log Insight installation, this guide describes security features built in to Log Insight and the measures that you can take to safeguard it from attack.

- External interfaces, ports, and services that are necessary for the proper operation of Log Insight
- Configuration options and settings that have security implications
- Location of log files and their purpose
- Required system accounts
- Information on obtaining the latest security patches

Intended Audience

This information is intended for IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of Log Insight.

Log Insight Security Reference 1

Use the Security Reference to learn about the security features of your Log Insight installation and the measures that you can take to safeguard your environment from attack.

This chapter includes the following topics:

Ports and External Interfaces that the Log Insight Virtual Appliance Uses

The operation of Log Insight depends on certain services, ports, and external interfaces.

Communication Ports

Log Insight uses several communication ports and protocols.

Log Insight network traffic has several sources.

Admin workstation	The machine that a system administrator uses to manage the Log Insight virtual appliance remotely.
User workstation	The machine on which a Log Insight user uses a browser to access the web interface of Log Insight.
System sending logs	The endpoint that sends logs to Log Insight for analysis and search. For example, endpoints include ESXi hosts, VMs or any system with an IP address.
Log Insight Windows Agent	The agent that resides on a Windows machine and sends Windows events and logs to Log Insight over APIs.

Log Insight appliance Any Log Insight virtual appliance, master or worker, where the Log Insight services reside. The base operating system pf the appliance is SUSE 11 SP3.

Log Insight master node In cluster mode, Log Insight consists of multiple nodes, including one master node and several worker nodes. When you issue a query, it goes first to the master node. The master node processes the query, distributes the work to multiple worker nodes, collects and aggregates the result, and sends it back to you. You use the Log Insight master node to configure the entire system. In standalone mode, the only node is both the master node and the worker node.

Source	Destination	Port	Protocol	Service Description
Admin workstation	Log Insight appliance	22	TCP	SSH: Secure Shell connectivity
User workstation	Log Insight appliance	80	TCP	HTTP: Web interface
User workstation	Log Insight appliance	443	TCP	HTTPS: Web interface
System sending logs	Log Insight appliance	514	TCP, UDP	Syslog data
System sending logs	Log Insight appliance	1514	TCP	Syslog data over SSL
Log Insight Windows Agent	Log Insight appliance	9000	TCP	Log Insight Ingestion API
Log Insight appliance	NTP server	123	UDP	NTPD: Provides NTP time synchronization **NOTE** The port is open only if you choose to use NTP time synchronization
Log Insight appliance	Log Insight appliance	59778, 16520-16580	TCP	Log Insight services
Log Insight appliance	Mail Server	465	TCP	SMTPS: MTP mail service over SSL
Log Insight appliance	Log Insight master node	12543	TCP	Postgres database server **NOTE** Port 12543 is open only on the Log Insight master node. The Postgres database server runs on the master node.
Log Insight master node	DNS server	53	TCP, UDP	DNS
Log Insight master node	AD server	389	TCP, UDP	Active Directory **NOTE** The port is open only if you enable Active Directory integration.

Source	Destination	Port	Protocol	Service Description
Log Insight master node	AD server	636	TCP	Active Directory over SSL NOTE The port is open only if you enable Active Directory integration.
Log Insight master node	AD server	3268	TCP	Active Directory Global Catalog NOTE The port is open only if you enable Active Directory integration.
Log Insight master node	AD server	3269	TCP	Active Directory Global Catalog SSL NOTE The port is open only if you enable Active Directory integration.
Log Insight appliance	Log Insight appliance	7000	TCP	Cassandra replication and query
Log Insight appliance	Log Insight appliance	9042	TCP	Cassandra query

The following ports are open but not used by Log Insight, and can be safely blocked by a firewall. They will be closed by default in a future release.

Destination	Port	Protocol	Service Description
Log Insight appliance	111	TCP, UDP	RPCbind service that converts RPC program numbers into universal addresses
Log Insight appliance Tomcat service	9007	TCP	Tomcat services

Log Insight Configuration Files

Some configuration files contain settings that affect Log Insight security.

NOTE All security-related resources are accessible by the root account. Protecting this account is critical to the security of Log Insight.

Table 1-1. Log Insight Configuration Files

File	Description
`/usr/lib/loginsight/application/etc/loginsight-config-base.xml`	The default system configuration for Log Insight.
`/storage/core/loginsight/config/loginsight-config.xml#number`	The modified (from the default) system configuration forLog Insight.
`/usr/lib/loginsight/application/etc/jaas.conf`	The configuration for active directory integration.
`/usr/lib/loginsight/application/etc/3rd_config/server.xml`	The system configuration for Apache Tomcat server.
`/storage/var/loginsight/apache-tomcat/conf/tomcat-users.xml`	The system configuration for Apache Tomcat server.

Table 1-1. Log Insight Configuration Files (Continued)

File	Description
`/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/server.xml`	The system configuration for Apache Tomcat server.
`/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/tomcat-users.xml`	User information for Apache Tomcat server.

Log Insight Public Key, Certificate, and Keystore

The public key, the certificate, and the keystore of Log Insight are located on the Log Insight virtual appliance.

NOTE All security-related resources are accessible by the root account. Protecting this account is critical to the security of Log Insight.

- `/usr/lib/loginsight/application/etc/public.cert`
- `/usr/lib/loginsight/application/etc/loginsight.pub`
- `/usr/lib/loginsight/application/etc/3rd_config/keystore`
- `/usr/lib/loginsight/application/etc/truststore`
- `/usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/keystore`

Log Insight License and EULA File

The end-user license agreement (EULA) and license file are located on the Log Insight virtual appliance.

NOTE All security-related resources are accessible by the root account. Protecting this account is critical to the security of Log Insight.

File	Location
License	`/usr/lib/loginsight/application/etc/license/loginsight_dev.dlf`
License	`/usr/lib/loginsight/application/etc/license/loginsight_cpu.dlf`
License	`/usr/lib/loginsight/application/etc/license/loginsight_osi.dlf`
License Key file	`/usr/lib/loginsight/application/etc/license/loginsight_license.txt`
End-user license agreement	`/usr/lib/loginsight/application/etc/license/eula.txt`

Log Insight Log Files

The files that contain system messages are located on the Log Insight virtual appliance.

File	Description
`/storage/var/loginsight/runtime.log`	Used to track all run time information related to Log Insight
`/storage/var/loginsight/pi.log`	Used to track database start or stop events
`/storage/var/loginsight/usage.log`	Used to track all queries
`/storage/var/loginsight/ui.log`	Used to track events related to the Log Insight user interface

File	Description
/storage/var/loginsight/watchdog_log*	Used to track the run time events of the watch dog process, which is responsible for restarting Log Insight if it is shutdown for some reason
/storage/var/loginsight/vcenter_operations.log	Used to track events related to the vRealize Operations Manager integration
/storage/var/loginsight/loginsight_daemon_stdout.log	Used for the standard output of Log Insight daemon
/storage/var/loginsight/upgrade.log	Used to track events that occur during Log Insight upgrade
/storage/var/loginsight/apache-tomcat/logs/*.log	Used to track events from Apache Tomcat server
/storage/var/loginsight/plugins/vsphere/li-vsphere.log	Used to trace events related to integration with vSphere
/storage/var/loginsight/pgsql.log	Used to track the events of the Postgres server
/var/log/firstboot/stratavm.log	Used to track the events that occur at first boot and configuration of the Log Insight virtual appliance
/storage/var/loginsight/phonehome.log	Used to track information about trace data collection sent to VMware (if enabled).
/storage/var/loginsight/alert.log	Used to track information about user defined alerts that have been triggered.
/storage/var/loginsight/systemalert.log	Used to track information about system alerts that Log Insight sends. Each alert is listed as a JSON entry.
/storage/var/loginsight/systemalert_worker.log	Used to track information about system alerts that a Log Insight worker node sends. Each alert is listed as a JSON entry.

Log Messages Related to Security

The `runtime.log` file contains user audit log messages in the following format.

- `[2013-05-17 20:40:18.716+0000] [http-443-5 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged in: Name: admin | Role: admin]`
- `[2013-05-17 20:39:51.395+0000] [http-443-5 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged out: Name: admin | Role: admin]`
- `[2013-09-18 12:39:34.823-0700] [http-9443-3 WARN /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][Bad username/password attempt (username: myusername)]`
- `[2013-09-18 12:40:08.761-0700] [http-9443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged in: Active Directory User: SAM=myusername, Domain=vmware.com,UPN=myusername@vmware.com]`
- `[ 2013-09-18 12:40:20.232-0700] [http-9443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged out: Active Directory User: SAM=myusername, Domain=vmware.com,UPN=myusername@vmware.com]`
- `[2013-09-18 12:40:36.933-0700] [http-9443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged in: Local User: Name=myusername, Role=user]`

- [2013-09-18 12:40:40.429-0700] [http-9443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean][User logged out: Local User: Name=myusername, Role=user
- [2013-11-13 23:26:21.569+0000] [http-443-4 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new user: Active Directory User: SAM=username, Domain=vmware.com, UPN=username@vmware.com]
- [2013-11-14 22:44:11.017+0000] [http-443-6 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new user: Local User: Name=username, Role=admin]
- [2013-12-05 21:03:36.751+0000] [http-443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed users: [Active Directory User: SAM=username, Domain=vmware.com, UPN=username@vmware.com]]
- [2013-12-05 21:04:16.707+0000] [http-443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed users: [Local User: Name=username, Role=admin]]
- [http-9443-3 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new group: (domain=vmware.com, group=VMware Employees, role=user)]
- [2013-12-05 13:07:04.108-0800] [http-9443-2 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed groups: [(domain=vmware.com, group=VMware Employees, role=user)]]

Log Insight Firewall Recommendations

To protect sensitive information gathered by Log Insight, place the server or servers on a management network segment protected by a firewall from the rest of your internal network.

Required Ports

The following ports need to be open to network traffic from sources that send data to Log Insight.

Port	Protocol
514/UDP, 514/TCP	Syslog
1514/TCP	Syslog-TLS (SSL)
9000/TCP	Log Insight Ingestion API

The following ports need to be open to network traffic that needs to use the Log Insight UI.

Port	Protocol
80/TCP	HTTP
443/TCP	HTTPS

The following set of ports should only be open on a Log Insight master node for network access from worker nodes for maximum security.

Port	Protocol
16520:16580/TCP	Thrift RPC
59778/TCP	log4j server
12543/TCP	database server

Log Insight User Accounts

You must set up a system and a root account to administer Log Insight.

Log Insight Root User

Log Insight currently uses the root user account as the service user. No other user is created.

Unless you set the root password property during deployment, the default root password is blank. You must change the root password when you log in to the Log Insight console for the first time.

SSH is disabled until the default root password is set.

The root password must meet the following requirements.

- Must be at least 8 characters long
- Must contain at least one uppercase letter, one lowercase letter, one digit, and one special character
- Must not repeat the same character four times

Log Insight Admin User

When you start the Log Insight virtual appliance for the first time, Log Insight creates the admin user account for its Web user interface.

The default password for admin is blank. You must change the admin password in the Web user interface during the initial configuration of Log Insight.

Active Directory Support

Log Insight supports integration with Active Directory. When configured, Log Insight can authenticate or authorize a user against Active Directory.

See topic Enable User Authentication Through Active Directory in the Log Insight Administration Guide.

Privileges Assigned to Default Users

The Log Insight service user has root privileges.

The Web user interface admin user has the administrator privileges only to the Log Insight Web user interface.

Security Updates and Patches

The Log Insight virtual appliance uses SUSE Linux Enterprise Server 11 (x86_64), version 11, patch level 3 as the guest operating system.

You can apply the latest security update or patch by using a conventional approach, for example, rpm upgrade.

Before you apply an upgrade or patch to the guest operating system, take into account the dependencies. See "Ports and External Interfaces that the Log Insight Virtual Appliance Uses," on page 7.

Index