VMware vCenter Log Insight Security 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-001299-00

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 vCenter Log Insight Security Guide

The *VMware vCenter 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 Insightinstallation and the measures that you can take to safeguard your environment from attack.

This chapter includes the following topics:

Services, Ports, and External Interfaces that the Log Insight Virtual Appliance Uses

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

Log Insight Services

The operation of Log Insight depends on several services that run on the Log Insight virtual appliance.

Table 1-1. Log Insight Services

Service Name	Startup Type	Description
loginsight	Automatic	Core service for log aggregation, search, and analytics.
sendmail	Automatic	Used to send system notifications alerts, email alerts, and phone home.
sshd	Automatic (Disabled before the root password is set)	Secure remote console access.
ntp	Automatic	Time service for syncing-up with Internet Time Server through Network Time Protocol.
rpcbind	Automatic	Service that convert RPC program numbers into universal addresses.

Table 1-1. Log Insight Services (Continued)

Service Name	Startup Type	Description
cron	Automatic	Scheduled command service for phone home.
vaos	Automatic	Guest OS initialization that drives network setting, host name setting, ssh keys creation, #EULA acceptance, ISV boot scripts execution, and VAMI initialization.
jexec	Automatic	Supports the direct execution of binary formats.

Communication Ports

Log Insight uses several communication ports and protocols.

Port	Protocol
22/TCP	SSH
80/TCP	HTTP
443/TCP	HTTPS
514/UDP, 514/TCP	Syslog
1514/TCP	Syslog
9006 - 9007/TCP	Tomcat
9240/TCP	vAPI
111/TCP, 111/UDP	rpcbind
736/UDP	rpcbind
123/UDP	ntpd
16520-16580/TCP	loginsight
127.0.0.1:25/TCP	SMTP
127.0.0.1:465/TCP	SMTP
127.0.0.1:12543/TCP	Postgres

Third-Party Components

Log Insight uses the following third-party components.

Third-Party Component	Version
Java Runtime Environment	1.7 or later
Python	2.6 or later
Openssl	0.9.8j or later

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 1-2. Log Insight Configuration Files

File	Description
`/usr/lib/loginsight/application/etc/loginsight-config-base.xml`	The default system configuration for log insight.
`/usr/lib/loginsight/application/etc/loginsight-config-projects.xml`	The user-defined configuration for log insight, such as NTP server, NFS archiving location, and so on.
`/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.
`/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/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.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
/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 trace events related to integration with vSphere
/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 track events related to the vCenter Operations Manager integration
/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
/var/log/li-disk.log	Used to track storage related events, such as adding a new disk to the Log Insight virtual appliance

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]`
- `[20130918 12:39:34.8230700] [http94433 WARN /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [Bad username/password attempt (username: myusername)]`
- `[20130918 12:40:08.7610700] [http94433 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]`
- `[ 20130918 12:40:20.2320700] [http94433 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]`

- [20130918 12:40:36.9330700] [http94433 INFO /127.0.0.1] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User logged in: Local User: Name=myusername, Role=user]
- [20130918 12:40:40.4290700] [http94433 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 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.

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 changed.

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 2 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 "Services, Ports, and External Interfaces that the Log Insight Virtual Appliance Uses," on page 7.

Index