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.
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 © 2013 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

About VMware vCenter Log Insight Security Guide  5

1  Log Insight Security Reference  7
   Services, Ports, and External Interfaces that the Log Insight Virtual Appliance Uses  7
   Log Insight Configuration Files  8
   Log Insight Public Key, Certificate, and Keystore  9
   Log Insight License and EULA File  9
   Log Insight Log Files  9
   Log Insight Root User Account  10
   Security Updates and Patches  10

Index  11
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.
The information herein provides reference related to Log Insight security.

This chapter includes the following topics:

- “Services, Ports, and External Interfaces that the Log Insight Virtual Appliance Uses,” on page 7
- “Log Insight Configuration Files,” on page 8
- “Log Insight Public Key, Certificate, and Keystore,” on page 9
- “Log Insight License and EULA File,” on page 9
- “Log Insight Log Files,” on page 9
- “Log Insight Root User Account,” on page 10
- “Security Updates and Patches,” on page 10

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

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Startup Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loginsight</td>
<td>Automatic</td>
<td>Core service for log aggregation, search, and analytics.</td>
</tr>
<tr>
<td>sendmail</td>
<td>Automatic</td>
<td>Used to send system notifications alerts, email alerts, and phone home.</td>
</tr>
<tr>
<td>sshd</td>
<td>Automatic</td>
<td>Secure remote console access.</td>
</tr>
<tr>
<td></td>
<td>(Disabled before</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the root password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is set)</td>
<td></td>
</tr>
<tr>
<td>ntp</td>
<td>Automatic</td>
<td>Time service for syncing-up with Internet Time Server through Network Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protocol.</td>
</tr>
<tr>
<td>rpcbind</td>
<td>Automatic</td>
<td>Service that convert RPC program numbers into universal addresses.</td>
</tr>
<tr>
<td>cron</td>
<td>Automatic</td>
<td>Scheduled command service for phone home.</td>
</tr>
</tbody>
</table>
Table 1-1. Log Insight Services (Continued)

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Startup Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vaos</td>
<td>Automatic</td>
<td>Guest OS initialization that drives network setting, host name setting, ssh keys creation, #EULA acceptance, ISV boot scripts execution, and VAMI initialization.</td>
</tr>
<tr>
<td>jexec</td>
<td>Automatic</td>
<td>Supports the direct execution of binary formats.</td>
</tr>
</tbody>
</table>

Communication Ports

Log Insight uses several communication ports and protocols.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/TCP</td>
<td>SSH</td>
</tr>
<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>
</tbody>
</table>

External Interfaces

Log Insight uses the following third-party components.

<table>
<thead>
<tr>
<th>Third-Party Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java Runtime Environment</td>
<td>1.7 or later</td>
</tr>
<tr>
<td>Python</td>
<td>2.6 or later</td>
</tr>
<tr>
<td>Openssl</td>
<td>0.9.8j or later</td>
</tr>
</tbody>
</table>

Log Insight Configuration Files

Some configuration files contain settings that affect the security of Log Insight.

**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/etc/loginsight-config-base.xml
- /usr/lib/loginsight/etc/loginsight-config-projects.xml
- /usr/lib/loginsight/etc/3rd_config/server.xml
- /usr/lib/loginsight/etc/3rd_config/tomcat-users.xml
- /usr/lib/loginsight/application/3rd_party/apache-tomcat-*/*conf/server.xml
- /usr/lib/loginsight/application/3rd_party/apache-tomcat-*/*conf/tomcat-users.xml
- /storage/core/loginsight/config/logsight-config.xml*
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/etc/public.cert
- /usr/lib/loginsight/etc/loginsight.pub
- /usr/lib/loginsight/etc/3rd_config/keystore
- /usr/lib/loginsight/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.

<table>
<thead>
<tr>
<th>File</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>/usr/lib/loginsight/application/etc/license/loginsight.dlf</td>
</tr>
<tr>
<td>End-user license agreement</td>
<td>/usr/lib/loginsight/application/etc/license/eula.txt</td>
</tr>
</tbody>
</table>

Log Insight Log Files

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

- /storage/var/loginsight/runtime.log
- /storage/var/loginsight/pi.log
- /storage/var/loginsight/usage.log
- /storage/var/loginsight/ui.log
- /storage/var/loginsight/watchdog_log*
- /storage/var/loginsight/vcenter_operations.log
- /storage/var/loginsight/loginsight_daemon_stdout.log
- /storage/var/loginsight/apache-tomcat/logs/*_.log
- /storage/var/loginsight/plugins/vsphere/li-vsphere.log
- /storage/core/loginsight/cidata/database/pgsql.log
- /var/log/firstboot/stratavm.log
- /var/log/li-disk.log
Log Messages Related to Security

The runtime.log file contains login and logout event 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]

Log Insight Root User Account

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.

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

A
admin privileges 10

C
certificate 9
configuration files 8

D
default root password 10
disabled SSH 10

E
EULA 9

G
glossary 5
guest OS 10

H
http 7
https 7

I
intended audience 5

K
keystore 9

L
license file 9
loginsight-config-base.xml 8
loginsight-config-projects.xml 8
loginsight.pub 9
logs 9
loginsight-config.xml 8

N
ntp 7

P
patches 10
ports 7
postgres 7
public key 9
public.cert 9

R
root privileges 10

S
security reference 7
security updates 10
sendmail 7
server.xml 8
services 7
smtp 7
SSH 10
sshd 7
syslog 7
system logs 9

T
tcp 7
tomcat-users.xml 8
truststore 9

U
udp 7