00.5em

0.00.5em

0.0.00.5em

0em

vCenter Log Insight Security Guide

Release 1.0 Beta (v0.9.1)

VMware Inc.

May 31, 2013

Contents

1 A list of all external interfaces, ports, and services necessary for proper operation of Log Insight.

1.1 Services

- jre >= 1.7
- python >= 2.6
- sendmail
- sshd
- ntp
- rpcbind
- gpg
- openssl >= 0.9.8j
- cron
- vaos
- jexec

- 127.0.0.1:25 (smtp/tcp)
- 127.0.0.1:465 (smtp/tcp)
- 127.0.0.1:12543 (postgres/tcp)

2 All resources that need to be protected, such as security-relevant configuration files and passwords, and the recommended access controls for secure operation.

All security-related resources are accessible only to the root account. Protecting this account is critical.

2.1 Configuration files

- /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*

2.2 Public key, certificate, and keystore

- /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

2.3 EULA and license

- /usr/lib/loginsight/application/etc/license/loginsight.dlf
- /usr/lib/loginsight/application/etc/license/eula.txt

3 Location of log files and information about how to interpret security related log messages.

3.1 Location of log files

- /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

3.2 Security-related log messages

- [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]

In the runtime.log, you'll see events when users logged in and logged out.

4 Log-on ID of accounts created during system install/bootstrap and instructions on how to change defaults.

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

The default root password is blank. The root is required to change its password at first login via the console. SSH is disabled until the root password is changed.

The password complexity requirements are:

- Minimum of 8 characters
- Minimum of one upper, one lower, one digit, and one special character
- You cannot repeat the same character 4 times

Log Insight creates an admin user for its web UI at first run. The admin user password is required to be created in the web UI during the initial configuration of Log Insight.

5 Privileges assigned to "service" users.

The Log Insight service user has root privileges.

The web UI admin user only has the administrator privileges to the Log Insight web UI.

6 Information on how customers can obtain and apply the latest security update/patch.

The Log Insight virtual appliance uses the following guest OS version. You can apply the latest security update/patch via the conventional approach such as rpm upgrades.

SUSE Linux Enterprise Server 11 (x86_64) VERSION = 11 PATCHLEVEL = 2

Please be aware of the dependencies listed in *A list of all external interfaces, ports, and services necessary for proper operation of Log Insight.*.