Accenture Security Quick Start Guide for Unix® OS Logging Configuration

accenture

This quick start guide will help Accenture Security customers configure Unix® Servers to send logs to the Log collection Platform (LCP).

This document includes the following topics:

- Supported Versions
- Port Requirements
- Configuring Unix OS
- LCP Configuration Parameters
- Sample Logs

Supported Versions

A list of supported versions is available in the Accenture Security Supported Products List document *(Accenture_MSS_Supported_Products_List.xlsx)* which can be found at Accenture Portal - https://mss.accenture.com/PortalNextGen/Reports/Documents

Port Requirements

Table 1-1: Port requirements for LCP communication.

Source	Destination	Port	Description
Unix/Linux/Solaris server	LCP	• 514 (UDP) or • 601 (TCP)	Default port

Configuring Unix OS

You can configure Unix OS devices using different syslog daemons to send event logs to the LCP.

- For syslogd configuration, see Configuring Syslog Message Forwarding Using syslogd.
- For rsyslogd configuration, see Configuring Syslog Message Forwarding Using rsyslogd.
- For syslog-ng configuration, see Configuring Syslog Message Forwarding Using syslog-ng.
- For Nokia IPSO syslog configuration, see Configuring Syslog Message Forwarding for Nokia IPSO.

In addition, we recommend configuring iptables and auditd logging.

- To configure iptables, see Configuring Logging for Linux iptables.
- To configure auditd logging, see Configuring Syslog Plugin for auditd.

Note: Additional configuration is required for IBM AIX and SUSE Linux 12.

- To configure FTP to log FTP sessions and debug information for IBM AIX, see Configuring FTP to Log FTP Sessions and Debug Information for IBM AIX.
- To configure event date format for SUSE Linux 12, see Configuring Event Date Format for SUSE Linux.

Configuring Syslog Message Forwarding Using syslogd

To configure syslog message forwarding using syslogd:

1. From a Unix server, login with root privileges.
2. To stop syslogd, at the command prompt, type the following command as required:

HP-UX	/sbin/init.d/syslogd stop
IBM AIX	stopsrc -s syslogd
Solaris 8 and 9	/etc/init.d/syslog stop

3. Use a text editor, such as vi, to open and edit the ***/etc/syslog.conf*** file.
   Add the following line in the syslog.conf file: ***.info @IP_address_of_the_LCP**
   For example: ***.info @192.0.2.1**, where 192.0.2.1 is the IP address of the LCP.
4. Save and close the ***syslog.conf*** file.
5. To start or restart syslogd, type the following command as required:

HP-UX	*/sbin/init.d/syslogd start*
IBM AIX	*startsrc -s syslogd*
Solaris 8 and 9	*/etc/init.d/syslog start*
Solaris 10 and 11	*svcadm restart svc:/system/system-log*
Red Hat Linux 3-5, Debian Linux 3 - 4.9	*/etc/init.d/syslogd restart*
Red Hat Linux 6, Oracle Linux 5.0 - 6.5, CentOS 5.0 - 6.5	*/etc/init.d/rsyslog restart*
Mac OS X	Run the terminal utility and then at the command prompt, type the following command to restart syslogd: *launchctl unload /System/Library/ LaunchDaemons/com.apple.syslogd.plist; sleep1;* *launchctl load /System/Library/ LaunchDaemons/com.apple.syslogd.plist* **Note**: This command must be entered in one line, there is no carriage return or linefeed.

Configuring Syslog Message Forwarding Using rsyslogd

To configure syslog message forwarding using rsyslogd:

1. From a Unix server, login with root privileges.
2. To stop rsyslogd, at a command prompt, type the following command:

- For SUSE Linux and Ubuntu Linux: service rsyslog stop
- For other Linux distributions: /etc/init.d/rsyslog stop

3. Use a text editor, such as vi, to open and edit the following file:

- For Ubuntu Linux: /etc/rsyslog.d/50-default.conf
- For other Linux distributions: /etc/rsyslog.conf

4. Add one of the following lines at the end of the rsyslog.conf file:

- For UDP forwarding, add *.info @IP_address_of_the_LCP
- For TCP forwarding, add *.info @@IP_address_of_the_LCP

Examples:
For UDP forwarding: *.info @192.0.2.1, where 192.0.2.1 is the IP address of the LCP.
For TCP forwarding: *.info @@192.0.2.1, where 192.0.2.1 is the IP address of the LCP.

5. Save and close the rsyslog.conf file.
6. To restart rsyslogd, at a command prompt, type the following command:

- For SUSE Linux and Ubuntu Linux: service rsyslog restart
- For other Linux distributions: /etc/init.d/rsyslog restart

Configuring Syslog Message Forwarding Using syslog-ng

To configure syslog message forwarding using syslog-ng:

1. From a Unix server, login with root privileges.
2. Use a text editor, such as vi, to open and edit the following file: */etc/syslog-ng/syslog-ng.conf*
3. Add the following lines in the syslog-ng.conf file:
   destination d_label_for_lcp { udp(lcp_ip_address port(preferred_port_number)); };
   filter f_label_that_identifies_the_filter { facility(info..emerg) and not facility (mail,cron); };
   log { source(src); filter(f_label_that_identifies_the_filter); destination(d_label_for_lcp); };
   For example:
   destination d_lcp { udp(192.0.2.1 port(514)); }; filter f_lcpfilter { facility(info..emerg) and not facility (mail,cron); }; log { source(src); filter(f_lcpfilter); destination(d_lcp); };
   Where:

- udp - Protocol configured.
- 192.0.2.1 - IP address of the LCP.
- 514 - Default port on which the LCP is configured to listen (preferred).
- source (src) - default syslog-ng, "source src" should already be defined in the syslog-ng.conf file.
- The filter parameter is optional.

Note: To configure TCP protocol, follow steps 1-3 and use "tcp" instead of "udp". Also use "601" instead of "514", where 601 is the default TCP port.

4. Save and close the *syslog-ng.conf* file.
5. To restart syslog-ng, at a command prompt, type the following command: service syslog restart

Configuring Logging for Linux iptables

Linux iptables use the following options to set the logging format for events:

- -- log-level
- -- log-prefix
- -- log-tcp-sequence
- -- log-tcp-options
- -- log-ip-options

Sample iptables Rule

iptables -A INPUT -i eth0 -p tcp -s 192.0.2.1--dport 22 -j LOG --log-prefix "IPT: SSH DENY "--log-level info --log-tcp-sequence --log-tcp-options--log-ip-options

Configuring Syslog Plugin for auditd

Note: If syslog plugin for auditd is not installed on the server, refer to the vendor repository for installation.

To configure syslog plugin for auditd:

1. From a Unix server, login with root privileges.
2. To stop the audit process, at a command prompt, type the following command: /etc/init.d/auditd stop
3. Use a text editor, such as vi, to open and edit the following file: /etc/audisp/plugins.d/syslog.conf
4. Add the following line to the /etc/audisp/plugins.d/syslog.conf file: active = yes
5. Save and close the /etc/audisp/plugins.d/syslog.conf file.
6. To restart the audit process, at a command prompt, type the following command: /etc/init.d/auditd start

Configuring FTP to Log FTP Sessions and Debug Information for IBM AIX

To configure FTP to log FTP sessions and debug information for IBM AIX:

1. On an AIX server, at the Unix prompt, login with root privileges.
2. Use an editor, such as vi, to open and edit the following file: /etc/inetd.conf
3. Configure the FTP daemon with -l and -d parameters. A sample configuration is as follows: ftp stream tcp nowait root /usr/sbin/ftpd -l -d
4. Save and close the inetd.conf file.
5. Stop and restart the FTP subserver by typing the following commands:

- stopsrc -t ftp
- startsrc -t ftp

Configuring Syslog Message Forwarding for Nokia IPSO

To configure syslog message forwarding for Nokia IPSO:

1. Login to the Nokia Network Voyager Web console with root privileges.
2. Click System Configuration > System Logging.
3. Under Remote system logging, in the Add new remote IP address to log to field, enter the IP address of the LCP.
4. Click Apply. The IP address of the LCP should appear in the list.
5. From the Log at or above severity list, select Info.
6. Click Apply and then Save.

Configuring Event Date Format for SUSE Linux

To configure event date format for SUSE Linux:

1. From a SUSE Linux server, login with root privileges.
2. To stop rsyslogd, at a command prompt, type the command: service rsyslog stop-
3. Use a text editor, such as vi, to open and edit the following file: /etc/rsyslog.conf
4. Add the following line to the /etc/rsyslog.conf file: $ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
5. Save and close the /etc/rsyslog.conf file.
6. To restart rsyslog, at a command prompt, type the command: service rsyslog start

LCP Configuration Parameters

Table 1-2: The Unix OS event collector properties to be configured by Accenture are given in the table.

Property	Default Value	Description
Protocol	UDP	The default protocol for syslog. The collector can also accept logs in TCP. Note: While TCP offers guaranteed delivery of log packets, it places a larger overhead on the LCP. To balance TCP for reliability over UDP for speed/simplicity, contact the Accenture Security Onboarding team.
IP Address	Unix OS Interface IP address	Logging device IP address mentioned in the Pre-Installation Questionnaire (PIQ). Note: If the device sends logs using multiple interfaces, contact the Accenture Security Onboarding team.
Signatures	ipmon, audispd:, named, httpd:, login:, dhclient, sshd, su, LOGIN, pam_unix, xinetd, kernel, useradd, adduser, userdel, gdm, rpc.statd, usermod, init:, reboot:, ftpd, last message repeated, shutdown:, Firewall[, passwd, shadow, in.telnetd, audit:, SuSEfirewall2:, auditd, gnome-keyring-daemon, vsftpd:, chage, groupdel, groupadd, vsftpd[, , login[, groupmod, unix_chkpwd, chpasswd, gdm-session-worker	Accenture Security recommended signatures processed by the Unix event collector.
Port Number	514	The default port for UDP. For TCP, the default port is 601. Note: The LCP can be configured to listen on a non-standard port, please advise the Accenture Security Onboarding team if this is a requirement.

Sample Logs

RHEL Linux

Sep 27 18:15:10 192.0.2.1 sshd[8406]: Failed password for root from ::ffff:192.0.2.2 port 3162 ssh2

SUSE Linux

Dec 18 21:10:47 Test sshd[10067]: Accepted keyboard-interactive/pam for root from 192.0.2.2 port 58996 ssh2

AIX

May 26 14:35:34 Test ftpd[491726]: connection from ::ffff:192.0.2.1 at Fri May 26 14:35:34 2006

Solaris

Aug 11 11:43:02 Test su: [ID 366847 auth.notice] 'su root' succeeded for matt on /dev/pts/2

ISC BIND

9 Apr 7 13:45:27 Test named[8186]: 07-Apr-2009 13:45:27.191 queries: info: client 192.0.2.1#39588: query: Domain.com IN A +

Debian

May 20 05:09:20 Test sshd[29765]: Accepted password for root from 192.0.2.1 port 53170 ssh2

Oracle Linux

Mar 14 07:55:33 Test kernel: IPT: New OutBound: IN= OUT=eth0 SRC=192.0.2.1 DST=192.0.2.5 LEN=60 TOS=0x00 PREC=0x00 TTL=1 ID=38606 PROTO=UDP SPT=44852 DPT=33434 LEN=40

Ubuntu Linux

Apr 14 03:35:13 Test sshd[13359]: Received disconnect from 192.0.2.24: disconnected by user

HP-UX

Jun 2 18:28:50 Test ftpd[5589]: FTP LOGIN FROM <FQDN> 192.0.2.5, root Linux IPTables Apr 8 13:26:57 Test kernel: IPT: New Forwarded Conn: IN=br0 OUT=br1 PHYSIN=eth0 SRC=198.51.100.5 DST=64.34.180.101 LEN=76 TOS=0x00 PREC=0x00 TTL=63 ID=0 DF PROTO=UDP SPT=123 DPT=123 LEN=56

Auditd

Mar 18 19:01:01 Test audispd: node=<FQDN> type=USER_START msg=audit(1237417261.745:3029): user pid=3936 uid=0 auid=0 ses=376 subj=system_u:system _r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_open acct="root" exe=2F7573722F7362696E2F63726F6E64202864656C6574656429 (hostname=?, addr=?, terminal=cron res= success)'

accenture