

Audit Logs

USER GUIDE

Copyright

© Ericsson AB 2015. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
2	Audit Log	3
2.1	Location of Audit Log File	3
2.2	Description of Audit Log Entries	3
3	Syslog	7
3.1	Location of Syslog File	7
3.2	Description of Syslog Entries	7





1 Introduction

This document describes the Linux[®] audit log.

The audit log enables logging and tracking access to files, directories, and resources of the system, as well as tracing system calls. It enables monitoring of the system for application misbehavior or code malfunctions.





2 Audit Log

This section describes where to find the audit log file, and how to read the log file.

2.1 Location of Audit Log File

The audit log file is located in `/var/log/audit/audit.log`.

2.2 Description of Audit Log Entries

Each event record in the audit log file consists of the event type (`type=<keyword>`) and several event fields (`<name>=<value>` pairs) separated by a white space or a comma.

The following is an example of a simple audit event record extracted from the audit log file:

```
type=DAEMON_START msg=audit(1402643479.057:5760): auditd start, ⇒
ver=1.8 format=raw kernel=3.0.101-0.15.1.6550.0.PTF-default ⇒
auid=4294967295 pid=2320 subj=unconfined res=success
```

The fields of the audit log entry are described in Table 1.

Table 1 Fields of Event Records in Audit Log

Field	Description
<code>type=DAEMON_START</code>	The type of event record. <code>DAEMON_START</code> type is triggered when the <code>auditd</code> daemon is started.
<code>msg=audit(1402643479.057:5760)</code>	The <code>msg</code> field records the following: <ul style="list-style-type: none"> A time stamp (Epoch time) and unique ID of the record in the format of <code>audit(<time_stamp>:<ID>)</code>. All events that are logged from the system call of one application have the same event ID. Various event-specific <code><name>=<value></code> pairs provided by the kernel or user space applications.
<code>auditd start</code>	Indicates that the <code>auditd</code> daemon is started.
<code>ver=1.8</code>	The version of the audit daemon.

**Table 1** *Fields of Event Records in Audit Log*

Field	Description
format=raw	Describes how the information is to be stored on disk. The value <code>raw</code> means that the audit records are stored in a format exactly as the kernel sends it.
kernel=3.0.101-0.15.1.6550.0.PTF-default	The kernel version of the system.
audit=4294967295	Records the audit user ID. Any process that runs before auditing capability is turned on in the kernel gets <code>loginuid 4294967295</code> .
pid=2320	Records the process ID. 2320 is the process ID of the <code>auditd</code> daemon.
subj=unconfined	Records the SELinux context with which the process was labeled at the time of execution.
res=success	Records the result of the operation that triggered the audit event. In this case, the <code>auditd</code> daemon has been started successfully.

2.2.1 Example of Successful Logon

The following example shows audit events step by step from when a user logs on to a system through SSH:

1. The Pluggable Authentication Module (PAM) reports that it has successfully requested user authentication for root from a remote host (192.168.1.1). The terminal where this occurs is SSH:

```
type=USER_AUTH msg=audit(1430213659.716:118): user pid=13151 uid=0 ⇒  
audit=4294967295 ses=4294967295 msg='op=PAM:authentication ⇒  
acct="root" exe="/usr/sbin/sshd" (hostname=192.168.1.1, ⇒  
addr=192.168.1.1, terminal=ssh res=success) '
```

2. PAM reports that it has successfully determined whether the user is authorized to log on:

```
type=USER_ACCT msg=audit(1430213659.716:119): user pid=13151 uid=0 ⇒  
audit=4294967295 ses=4294967295 msg='op=PAM:accounting acct="root" ⇒  
exe="/usr/sbin/sshd" (hostname=192.168.1.1, addr=192.168.1.1, ⇒  
terminal=ssh res=success) '
```

3. PAM reports that the appropriate credentials to log on have been acquired:



```
CRED_ACQ msg=audit(1430213659.720:122): user pid=13151 uid=0 ⇒
auid=4294967295 ses=4294967295 msg='op=PAM:setcred acct="root" ⇒
exe="/usr/sbin/sshd" (hostname=192.168.1.1, addr=192.168.1.1, ⇒
terminal=ssh res=success)'
```

```
type=LOGIN msg=audit(1430213659.720:123): login pid=13151 uid=0 old ⇒
auid=4294967295 new auid=0 old ses=4294967295 new ses=18
```

4. PAM reports that it has successfully opened a session for root:

```
type=USER_START msg=audit(1430213659.720:124): user pid=13151 uid=0 ⇒
auid=0 ses=18 msg='op=PAM:session_open acct="root" ⇒
exe="/usr/sbin/sshd" (hostname=192.168.1.1, addr=192.168.1.1, ⇒
terminal=ssh res=success)'
```

5. The user has successfully logged on and the terminal has changed to /dev/pts/1:

```
type=USER_LOGIN msg=audit(1430213659.724:125): user pid=13155 uid=0 ⇒
auid=0 ses=18 msg='op=login id=0 exe="/usr/sbin/sshd" ⇒
(hostname=192.168.1.1, addr=192.168.1.1, terminal=/dev/pts/1 ⇒
res=success)'
```

6. PAM reports that the credentials have been successfully reacquired:

```
type=CRED_REFR msg=audit(1430213659.724:129): user pid=13155 uid=0 ⇒
auid=0 ses=18 msg='op=PAM:setcred acct="root" exe="/usr/sbin/sshd" ⇒
(hostname=192.168.1.1, addr=192.168.1.1, terminal=ssh res=success)'
```

2.2.2 Example of Failed Logon Entry

The following example shows the audit log entry of an unsuccessful attempt to log on to machine 192.168.1.11 from machine 192.168.1.1, as the provided password was incorrect:

```
type=USER_AUTH msg=audit(1430205761.536:58): user pid=8951 uid=0 ⇒
auid=4294967295 ses=4294967295 msg='op=password acct="root" ⇒
exe="/usr/sbin/sshd" (hostname=?, addr=192.168.1.1, terminal=ssh ⇒
res=failed)
```





3 Syslog

COM SA implements a Middleware (MW) Support Agent (SA) for the Ericsson Common Operation and Maintenance (COM) component. The log record is forwarded to the `syslog` interface of the operating system. This provides a common audit trail that can be accessed not only through the Northbound Interface (NBI).

3.1 Location of Syslog File

The syslog can be read from `/var/log/messages`, which in turn is a symbolic link to, for example, `/var/log/SC-2-1/messages`.

3.2 Description of Syslog Entries

The format of the syslog entries is as follows: `<date> <time> <hostname> <program_name> [<process_id>]: <message>`

3.2.1 Example of Syslog Entries

The following Ericsson Command-Line Interface example commands result in the following entries in the syslog:

```
>ManagedElement=NODE06ST
(ManagedElement=NODE06ST)>configure
(config-ManagedElement=NODE06ST)>siteLocation=SEKI2707353A
(config-ManagedElement=NODE06ST)>commit
>exit
```

```
Feb  4 13:35:22 SC-1 com: interface=cli  user-name=root  session-id=3 =>
cmd-grp-name=ComBasicCommands CLI agent connection start.
Feb  4 13:36:12 SC-1 com: interface=cli  user-name=root  session-id=3 =>
Invoke setMo(): DN: ManagedElement=NODE06ST class: ManagedElement, =>
attribute: siteLocation, value: 'SEKI2707353A'
Feb  4 13:36:35 SC-1 com: interface=cli  user-name=root  session-id=3 =>
Transaction 82 Commit
Feb  4 13:38:09 SC-1 com: User name: root, Session Id: 3. Cli agent =>
connection end.
```