

Audit Information

USER GUIDE

Copyright

© Ericsson AB 2015, 2017. 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	Understanding Audit Information	1
1.1	Key Audit Information Concepts	1
1.2	Audit Log	1
1.3	Syslog	1
1.4	Audit Trail	1
2	Description of Syslog Entries	1
2.1	Ericsson Command-Line Interface Examples	1
2.2	NETCONF Interface Example	2





1 Understanding Audit Information

1.1 Key Audit Information Concepts

Audit information can be used to track access to files, directories, and resources of the system. It enables monitoring of the system for application misbehavior or code malfunctions.

1.2 Audit Log

The audit log record is forwarded to the syslog interface of the operating system. This provides a common audit trail that can be used for traceability of actions in the system.

1.3 Syslog

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`.

1.4 Audit Trail

The audit trail can, for example, be filtered out from the total syslog file by using keywords on the syslog entry, `<message>`.

2 Description of Syslog Entries

The format of the syslog entries is as follows: `<date> <time> <hostname> <program_name>: <message>`, for example:

```
<date> <time> <hostname> <program_name>: interface=cli ...  
<date> <time> <hostname> <program_name>: interface=netconf ...
```

2.1 Ericsson Command-Line Interface Examples

The following Ericsson Command-Line Interface (ECLI) 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.
```

2.2 NETCONF Interface Example

The following Ericsson NETCONF Interface example commands result in the following entries in the syslog:

```
<?xml version="1.0" encoding="UTF-8"?>  
<rpc message-id="1" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">  
  <edit-config>  
    <target>  
      <running/>  
    </target>  
    <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">  
      <ManagedElement>  
        <managedElementId>1</managedElementId>  
        <userLabel>Com</userLabel>  
      </ManagedElement>  
    </config>  
  </edit-config>  
</rpc>  
]]>]]>
```

```
Feb 27 09:38:35 SC-2-1 com: interface=netconf user-name=root ⇒  
session-id=1 Batch setting attribute: DN: ManagedElement=1⇒  
attrName: userLabel, numAttrValue: 1, attrType: 9, attrValue:⇒  
<userLabel>Com</userLabel>  
Feb 27 09:38:35 SC-2-1 com: interface=netconf user-name=root ⇒  
session-id=1 Session terminating (transaction commit)
```