

Security, OAM User Privilege Raise To Root Failed

Ericsson Centralized User Database

OPERATING INSTRUCTION

Copyright

© Ericsson AB 2015, 2016. 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	Overview	1
1.1	Description	1
1.2	Prerequisites	2
2	Procedure	3
	Glossary	5
	Reference List	7





1 Overview

This document provides the description and troubleshooting steps to take for the Security, OAM User Privilege Raise To Root Failed alarm.

1.1 Description

This alarm is raised when an Operation and Maintenance (OAM) user enters an unsuccessful `su` or `sudo` command to root.

The alarm attributes are listed and explained in Table 1:

Table 1 Alarm Attributes

Attribute Name	Attribute Value
Auto Cease	No
Module	SECURITY(11)
Error Code	6
Timestamp First	Date and time when the alarm was raised for the first time.
Repeated Counter	Number which indicates how many times the alarm was raised.
Timestamp Last	Date and time of the most recent alarm raised.
Resource ID	1.3.6.1.4.1.193.169.11.6. <i>IP</i> .<usernameLength>.<usernameASCII Code>
Alarm Model Description	OAM User Privilege Raise To Root Failed, Security.
Alarm Active Description	OAM User Privilege Raise To Root Failed @<IP> by user <username>
ITU Alarm Event Type	securityServiceOrMechanismViolation (10)
ITU Alarm Probable Cause	authenticationFailure (600)
ITU Alarm Perceived Severity	(6) - Warning
Originating Source IP	Node IP where the alarm was raised.
Sequence Number	Number which indicates the order in which alarms were raised.

In Table 1, the indicated variables are as follows:

- <usernameLength>: The number of characters in the user name.
- <usernameASCII Code>: A series of dot-separated numbers where each number corresponds to the ASCII code of each character in the user name. For example:

79.97.109.85.115.101.114 stands for OamUser.



- `<IP>`: The IP address of the server node.
- `<username>`: The name of the user in text.

For more information about attribute descriptions, refer to *CUDB Node Fault Management Configuration Guide*, Reference [1].

The possible causes of the alarm are as follows:

- A user has unsuccessfully tried to increase their access permissions to root using `su` or `sudo` command.

1.2 Prerequisites

This section provides information on the documents, tools and conditions that apply to the procedure.

1.2.1 Documents

Refer to *CUDB Node Fault Management Configuration Guide*, Reference [1] for further information.

1.2.2 Tools

Not applicable.

1.2.3 Conditions

Not applicable



2 Procedure

Perform the following steps:

1. Make backup copies of the log files to preserve evidence of the (attempted) intrusion.
2. Examine the security log file to determine the source of the intrusion. For more information about logging information in CUDB, refer to *CUDB Node Logging Events*, Reference [2].
3. If the log file analysis indicates that an unauthorized operation was successful, seek further advice in order to secure the system again. For more information about security configuration in CUDB, refer to *CUDB Security and Privacy Management*, Reference [3].
4. Once system security has been reestablished, manually clear the alarm according to the procedure described in *CUDB Node Fault Management Configuration Guide*, Reference [1] .
5. Further actions are outside the scope of this Operating Instruction.





Glossary

For the terms, definitions, acronyms and abbreviations used in this document, refer to *CUDB Glossary of Terms And Acronyms*, Reference [4].





Reference List

CUDB Documents

- [1] *CUDB Node Fault Management Configuration Guide*
- [2] *CUDB Node Logging Events*
- [3] *CUDB Security and Privacy Management*
- [4] *CUDB Glossary of Terms and Acronyms*