

Security, Root Login Failed

Ericsson Centralized User Database

Operating Instructions

Copyright

© Ericsson AB 2016-2018. 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
1.1	Alarm Description	1
1.2	Prerequisites	2
2	Procedure	3
	Glossary	4



Security, Root Login Failed



1 Introduction

This document provides the description and troubleshooting steps to take for the Security, Root Login Failed alarm.

1.1 Alarm Description

This alarm is raised when a user fails logging in to a Ericsson Centralized User Database (CUDB) node as root.

The possible alarm causes and the corresponding fault reasons, fault locations, and impacts are described in [Table 1](#).

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
A user has failed logging in to a CUDB node using root access.	Authentication Fault.	A user has failed logging in to a CUDB node using root access.	Operating System.	User is not correctly authenticated and root access to the system is not granted.

Note: An alarm can appear as a result of the maintenance activity.

The alarm attributes are listed and explained in [Table 2](#).

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Auto Cease	No
Module	SECURITY(11)
Error Code	2
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	.1.3.6.1.4.1.193.169.11.2. <IP representation>
Alarm Model Description	Root Login Failed, Security.
Alarm Active Description	Security: Root Login Failed @ <IP>
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 2](#), the indicated variables are as follows:



- `<IP representation>` : The representation of the Internet Protocol (IP) address of the node from which the login attempt was made towards the CUDB node.

In case of IPv4 type, the address is represented in original format, that is `[0-255] . [0-255] . [0-255] . [0-255]`.

In case of IPv6 type, the address is represented in decimal format, by replacing each hexadecimal block with its decimal representation, for example, IPv6 address `2001:1b70:8294:3d84::3` is represented by `8193.7024.33428.15748.0.3`.

- `<IP>` : The original IP address of the node from which the login attempt was made towards the CUDB node.

For further information about attribute descriptions, refer to [CUDB Node Fault Management Configuration Guide](#).

1.2 Prerequisites

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

1.2.1 Documents

This instruction references the following documents:

- [CUDB Node Fault Management Configuration Guide](#).
- [CUDB Node Logging Events](#)
- [CUDB Security and Privacy Management](#)

1.2.2 Tools

Not applicable.

1.2.3 Conditions

Not applicable.



2 Procedure

If the alarm is raised, perform the following steps:

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](#).
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](#).
4. Once system security has been reestablished, refer to [CUDB Node Fault Management Configuration Guide](#) to manually clear the alarm.
5. If the alarm does not cease, contact the next level of maintenance support. Further actions are outside the scope of this Operating Instruction.

After This Task

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