

Security, OAM User Exceeded Number Of Failed Logins

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, OAM User Exceeded Number Of Failed Logins



1 Introduction

This document provides the description and troubleshooting steps to take for the Security, OAM User Exceeded Number Of Failed Logins alarm.

1.1 Alarm Description

This alarm is raised when the number of Operation and Maintenance (OAM) user login failures exceeds a configured threshold. Refer to [CUDB Node Configuration Data Model Description](#) for more information.

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
Too many failed OAM user login attempts.	The number of OAM user login failures exceeded a configured threshold.	Wrong password entered too many times at the login procedure, possibly by an unauthorized user.	OAM server node.	After a configured number of failed login attempts, the user account is blocked for a certain period of time. The node cannot be accessed by that user.

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	1
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	.1.3.6.1.4.1.193.169.11.1. <IP> . <usernameLength> . <usernameASCIICode>
Alarm Model Description	Too Many Failed OAM Login Attempts, Security.
Alarm Active Description	Security: Too Many Failed OAM Login Attempts @ <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 ID 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:



- `<usernameLength>` : The number of characters in the user name.
- `<usernameASCIICode>` : 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 for OamUser.
- `<IP>` : The IP address of the blade or Virtual Machine (VM), where the number of user login failures exceeded the configured threshold.
- `<username>` : The name of the user in text. For example:

OamUser

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 Configuration Data Model Description
- 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 possible (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 intrusion 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, manually clear the alarm according to the procedure described in [CUDB Node Fault Management Configuration Guide](#).
5. Wait for the configured time for unlock (for more information, refer to [CUDB Node Configuration Data Model Description](#)), otherwise log in as OAM administrator and manually unlock the user using the following command on the System Controller (SC) given in the Alarm Active Description attribute of the alarm (<IP> variable):

```
pam_tally2 -r -u <username>
```

6. 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