

Storage Engine, High Load in PLDB

Ericsson Centralized User Database

Operating Instructions

Copyright

© Ericsson AB 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	4
2.1	Actions for Intensive Database Operations	4
2.2	Actions for High Rate of Incoming LDAP Operations	4
2.3	Actions for Hardware Error in the Blade	4
	Glossary	6





1 Introduction

This instruction concerns alarm handling for the Storage Engine, High Load In PLDB alarm.

1.1 Alarm Description

The alarm is issued when the load in the Processing Layer Database (PLDB) is above its processing capacity. A clear sign of this is when the *drop ratio* goes above a certain threshold. The *drop ratio* for the PLDB is defined as the number of Lightweight Directory Access Protocol (LDAP) operations that could not be processed because of overload in the PLDB, divided by the number of received LDAP operations which were meant to be processed by the PLDB over a period of time.

The alarm is issued in the following situation:

- The ratio defined above goes beyond the threshold configured in the `pldbClusterDropRatioAlarmThreshold` parameter. Refer to [CUDB Node Configuration Data Model Description](#) for more information on this parameter.

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
High ratio of failed operations vs. total operations in the PLDB.	The ratio of failed operations vs. total operations in the PLDB was higher during a period of time than the configured threshold.	Intensive database operations are performed in the PLDB. Such operations can include provisioning, massive searches, PLDB blade reboot and so on.	PLDB	<ul style="list-style-type: none"> — Traffic may be rejected for the PLDB. — Response time of operations addressed to the PLDB may be higher.
		<p>The rate of incoming LDAP operations is too high. This can occur in the following cases:</p> <ul style="list-style-type: none"> — The rate of incoming LDAP operations per subscriber is very high, even if the number of subscribers is low. — The number of subscribers is very high, even if the rate of 		



Alarm Cause	Description	Fault Reason	Fault Location	Impact
		incoming LDAP operations per subscribers is low.		
		Hardware error in the blade.		

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

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Auto Cease	Yes
Module	STORAGE-ENGINE
Error Code	17
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	.1.3.6.1.4.1.193.169.1.1.17
Alarm Model Description	High Load, Storage Engine.
Alarm Active Description	Storage Engine (PLDB): High Load.
ITU Alarm Event Type	processingErrorAlarm (4)
ITU Alarm Probable Cause	systemResourcesOverload (207)
ITU Alarm Perceived Severity	(4) - Major
Originating Source IP	Node ID where the alarm was raised.
Sequence Number	Number which indicates the order in which alarms were raised.

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 Logchecker
- CUDB Node Configuration Data Model Description
- CUDB Node Fault Management Configuration Guide



1.2.2 Tools
Not applicable.

1.2.3 Conditions
Not applicable.



2 Procedure

This section describes the procedure to follow when this alarm is received.

2.1 Actions for Intensive Database Operations

Database processing-intensive tasks, such as massive operations, provisioning or PLDB blade reboot can explain the high load. If such an operation is running when the alarm is raised, do the following:

Steps

1. Wait for the alarm to be automatically cleared.

2.2 Actions for High Rate of Incoming LDAP Operations

Occasional high load situations can be expected in any traffic-processing system, since there might be times when the incoming traffic level is higher than foreseen. Nevertheless, if this alarm is raised too frequently, or stays raised for long periods of time, then do the following:

Steps

1. Check if the application Front Ends (FEs), LDAP clients using the CUDB system are configured in a way that results in the balanced distribution of load across all CUDB nodes.

In case too many application FEs are connected to a specific CUDB node, it can result in the high load of the the PLDB. In this case, consult the next level of maintenance support. Further actions are outside the scope of this instruction.

2. If the application FEs seem to be properly configured, then the incoming traffic may be higher than originally expected, and the current CUDB system dimensioning may no longer be enough to cope with it.
3. If the alarm does not cease, contact the next level of maintenance support. Further actions are outside the scope of this Operating Instruction.

2.3 Actions for Hardware Error in the Blade

To see if there is a hardware error detected in the blade, perform the following steps:



Steps

1. Check if Preventive Maintenance alarm is raised.

If this alarm is raised, check if the hardware error detected in the blade is the alarm cause.

2. Go to path `/home/cudb/monitoring/preventiveMaintenance/`.

The results of the logs are saved at this path. The name of the log contains the Node ID and timestamp, as shown in `CUDB_157_201808241225.log`.

3. Choose the latest log and search for Hardware Error.

4. Contact the next level of support, if the fault cause is hardware error.

Refer to [CUDB Logchecker](#) for more information on the error.

5. If the alarm does not cease, contact the next level of maintenance support. 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