

Storage Engine, High Load In DS

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 | 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 | 5 |
| | Glossary | 6 |
| | Reference List | 7 |





1 Introduction

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

1.1 Alarm Description

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

The alarm is issued in the following situation:

- The ratio defined above goes beyond the threshold configured in the `dsClusterDropRatioAlarmThreshold` 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 on a database cluster. | The ratio of failed operations vs. total operations on a database cluster was higher during a period of time than the configured threshold. | Intensive database operations are performed in the affected DS cluster. Such operations can include provisioning, massive searches, DS blade reboot and so on. | Affected DS cluster. | <ul style="list-style-type: none"> — Traffic may be rejected for the affected DS cluster. — Response time of operations addressed to this cluster 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 incoming LDAP operations per | | |



| Alarm Cause | Description | Fault Reason | Fault Location | Impact |
|-------------|-------------|------------------------------|----------------|--------|
| | | 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 | .1.3.6.1.4.1.193.169.1.2.17.<DG> |
| Alarm Model Description | High Load, Storage Engine. |
| Alarm Active Description | Storage Engine (DS-group #<DG>): High Load. |
| ITU Alarm Event Type | processingErrorAlarm (4) |
| ITU Alarm Probable Cause | systemResourcesOverload (207) |
| ITU Alarm Perceived Severity | (4) - Major |
| 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:

- <DG> is the Data Store Unit Group (DSG) the DS cluster belongs to.

For further information about attribute descriptions, refer to the Alarm Format and Description section of 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

Before starting this procedure, ensure that you have read the following documents:

- CUDB Node Fault Management Configuration Guide
- System Safety Information



— Personal Health and Safety Information

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 DS 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, move some subscriber data out of the DSG whose data are stored in the highly loaded DS cluster to decrease the traffic load on it. Do the following:

Steps

1. Use the `cudbDsgProvisioningManage` command with the `--disable` option to prevent the newly distributed data from being added to the referred DSG.

For more information, refer to [CUDB Node Commands and Parameters](#).

2. Move the distributed data out of the referred DSG to decrease memory usage by using the `cudbReallocate` command.

Either specify the amount of percentage of distributed data to be moved with the `--entriespercentage` option, or export the data and use the `--list` option. Refer to [CUDB Node Commands and Parameters](#) for more information on the `cudbReallocate` command and its options.

3. Check if the alarm is cleared, and depending on the result, perform one of the below steps:
 - a. If the alarm is cleared, then use the `cudbDsgProvisioningManage` command with the `--enable` option to allow the newly distributed data to be added to the referred DSG again.

For more information, refer to [CUDB Node Commands and Parameters](#).



- b. If the alarm remains, then consult the next level of maintenance support. Further actions are outside the scope of this 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 the OS section of *CUDB Logchecker* for more information on the error.



Glossary

For the terms, definitions, acronyms and abbreviations used in this document, refer to CUDB Glossary of Terms and Acronyms



Reference List

CUDB Documents

1. CUDB Node Configuration Data Model Description
2. CUDB Node Fault Management Configuration Guide
3. CUDB Node Commands and Parameters
4. CUDB Logchecker
5. CUDB Glossary of Terms and Acronyms

Other Ericsson Documents

1. System Safety Information
2. Personal Health and Safety Information