

Storage Engine, Data Inconsistency between Replicas Repaired, DS

Ericsson Centralized User Database

OPERATING INSTRUCTION

Copyright

© Ericsson AB 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	Introduction	1
1.1	Alarm Description	1
1.2	Prerequisites	2
2	Procedure	5
	Glossary	7
	Reference List	9





1 Introduction

This instruction concerns alarm handling for the Storage Engine, Data Inconsistency between Replicas Repaired, DS alarm.

1.1 Alarm Description

This alarm is raised as a notification when the Data Repair procedure was invoked for the current Data Store (DS) master replica, and some of the inconsistencies between the current and the former master replicas have been successfully repaired.

The alarm is issued in the following situations:

- A Data Repair task has been completed, and there are `repaired` entries recorded in the output log.

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
Some of the detected data inconsistencies between the current and former DS master replicas have been repaired.	Data Repair was executed with the identified LDAP entries that might not have been correctly replicated between the former and current master replicas, and it managed to repair some of these entries. These LDAP entries are recorded in the <code>repaired</code> log.	<p>This is not a fault, but information about how the repair was performed. Information is provided in the <code>repaired</code> log as repair status. The meaning of the possible repair status values are as follows:</p> <ul style="list-style-type: none"> • The entry has been repaired by the Data Repair procedure. • The entry has been repaired by LDAP traffic before Data Repair attempted to repair it. • The entry has been deleted by LDAP traffic before Data Repair attempted to delete it. 	Current and former DS master replicas.	Some provisioning and traffic data has been repaired with a marginal chance for data loss in CUDB.

The following are the consequences for the node if the alarm is not acted upon:

- The repaired Lightweight Directory Access Protocol (LDAP) entries might be unchecked for the correctness of the update.

The alarm attributes are listed and explained in Table 2:

**Table 2 Alarm Attributes**

Attribute Name	Attribute Value
Auto Cease	No
Module	STORAGE-ENGINE
Error Code	24
Time	Date when the alarm was raised.
Resource ID	.1.3.6.1.4.1.193.169.1.2.24.<DG>.<TIMESTAMP>
Alarm Model Description	Data Inconsistency between Replicas Repaired, Storage Engine
Alarm Active Description	Storage Engine (DS-Group #DG): Data inconsistency between replicas repaired (task <TASKID>, blade <BLADE>)
ITU Alarm Event Type	processingErrorAlarm (4)
ITU Alarm Probable Cause	databaseInconsistency (160)
ITU Alarm Perceived Severity	(6) - Warning
Originating Source IP	Node ID where the alarm was raised.

In Table 2, the indicated variables are as follows:

- <DG> is the Data Store Unit Group (DSG) the DS cluster belongs to.
- <TIMESTAMP> is an integer representing the seconds since the Unix epoch when the Data Repair task was started.
- <BLADE> is the CUDB blade or Virtual Machine (VM) identifier the replica is located at.
- <TASKID> is the identifier of the repair task.

For further information about attribute descriptions, refer to *CUDB Node Fault Management Configuration Guide*, Reference [1]. The alarm must be cleared manually.

For the interpretation of the `repaired` logs, refer to *CUDB Automatic Handling of Network Isolation Output Description*, Reference [2].

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*, Reference [1], regarding alarm configuration.
- *System Safety Information*, Reference [4]
- *Personal Health and Safety Information*, Reference [5]

1.2.2 Tools

Not applicable.

1.2.3 Conditions

Not applicable.





2 Procedure

When this alarm is raised, no particular action is required. The operator may proceed as follows to find the list of `repaired` entries and clear the alarm manually:

- Locate and identify the `repaired` log based on the `<BLADE>` and `<TASKID>` parameters in the alarm as follows:
 - Log in to the alarm originator CUDB node.
 - Search for the file(s) `/local2/cudb/ahsi/replica_repair/d`
`atarepair_TASKID_repaired_*.ldif.gz` on the blade or VM
`<BLADE>`.

It is preferred to copy these files from the node to an external machine for further analysis if needed.

Note: The files must be transferred and stored appropriately, as they may contain confidential subscriber data.

- To clear the alarm, refer to *CUDB Node Fault Management Configuration Guide*, Reference [1].





Glossary

For the terms, definitions, acronyms, and abbreviations used in this document, refer to *CUDB Glossary of Terms and Acronyms*, Reference [3].





Reference List

CUDB Documents

- [1] *CUDB Node Fault Management Configuration Guide*
- [2] *CUDB Automatic Handling of Network Isolation Output Description*
- [3] *CUDB Glossary of Terms and Acronyms*

Other Ericsson Documents

- [4] *System Safety Information*
- [5] *Personal Health and Safety Information*