

# CUDB Logchecker

## User Guide

## **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

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Document Purpose and Scope	1
1.2	Revision Information	1
<b>2</b>	<b>Overview</b>	<b>3</b>
<b>3</b>	<b>Usage Information</b>	<b>4</b>
3.1	General Information	4
3.2	Automatic Log Collection and Log Analysis	4
3.3	Manual Log Collection and Analysis	6
<b>4</b>	<b>Troubleshooting cudbAnalyser Results</b>	<b>7</b>
4.1	cudbSystemStatus	7
4.2	NDB	8
4.3	OS	9
4.4	Config	12
4.5	SWM	12
4.6	Database Cluster	13
4.7	LDAP	14
4.8	System Monitor	16
4.9	BC Server	17
4.10	Master Unavailability	18
4.11	Software Platform	18
4.12	Alarm	19
4.13	Log	20
	<b>Glossary</b>	<b>22</b>
	<b>Reference List</b>	<b>23</b>





# 1 Introduction

This section contains the purpose and scope of the document, and also the revision information.

## 1.1 Document Purpose and Scope

The purpose of this document is to provide the instructions and tools needed to automate CUDB log collection and log analysis. This document requires knowledge of the product. It is addressed to both Ericsson personnel and system administrators. If the contents of this document and the [Preventive Maintenance, Logchecker Found Error\(s\)](#) document are not enough to fix a fault, then contact next level of maintenance support.

## 1.2 Revision Information

### Rev. A

This document is based on 12/1553-CSH 109 067/9 with the following changes:

- Terminology updates throughout the document because of virtualized deployment support.

### Rev. B

Other than editorial changes, this document has been revised as follows:

- Updated Network Management System (NMS) terminology.

### Rev. C

Other than editorial changes, this document has been revised as follows:

- [Troubleshooting cudbAnalyser Results](#) on page 7: New section. Content removed from section Check Log Faults in [CUDB Node Preventive Maintenance](#).
- [cudbSystemStatus](#) on page 7, [OS](#) on page 9, [Config](#) on page 12, and [Database Cluster](#) on page 13: Added error codes.
- [cudbSystemStatus](#) on page 7, [NDB](#) on page 8, [OS](#) on page 9, [Database Cluster](#) on page 13, [LDAP](#) on page 14, [System Monitor](#) on page 16, [Master Unavailability](#) on page 18, and [Software Platform](#) on page 18: Updated actions.
- [LDAP](#) on page 14, [Alarm](#) on page 19, and [Log](#) on page 20: New sections.



## Rev. D

Other than editorial changes, this document has been revised as follows:

- [OS](#) on page 9: Added hardware error to [Table 3](#).
- [Software Platform](#) on page 18: Updated SAF: there are unassigned HA states (Severity: Warning) error message in [Table 11](#).



## 2 Overview

CUDB Logchecker is a software monitoring component on top of the current monitoring processes that aims to work as a preventive maintenance tool.



## 3 Usage Information

This section provides usage information about CUDB Logchecker.

### 3.1 General Information

CUDB Logchecker consists of the following two scripts:

- `cudbGetLogs`

The purpose of this script is to collect preventive maintenance logs for log analysis. Log collection takes approximately 4-5 minutes, and the resulting log is saved under the `/home/cudb/monitoring/preventiveMaintenance/` directory. The name of the log file contains the Node ID and a timestamp in the following format:

```
<CUDB_node_id>_<YYYYmddHHMM>.log
```

For example:

```
CUDB_99_201201020025.log
```

**Note:** Logs are deleted automatically from the `/home/cudb/monitoring/preventiveMaintenance/` directory, if they are older than 180 days.

- `cudbAnalyser`

`cudbAnalyser` is a tool to analyze logs gathered and preprocessed by `cudbGetLogs`. It looks for certain patterns that can indicate malfunctions already present in the CUDB system, and also searches for traces of suspicious events that can lead to system failures if proper preventive maintenance actions are not carried out in time. `cudbAnalyser` categorizes its findings, determines the risk levels, and presents the results on the standard output. The automatic log analysis also sends an alarm to the Network Management System (NMS), if it finds problems. All these faults are weighted by CUDB Logchecker. The severity of the alarm depends on the accumulated weights of the faults (this means that multiple minor faults can also result in a major alarm). Severity levels are warning, minor, major or critical.

**Note:** These scripts can be executed only on the active System Controller (SC).

### 3.2 Automatic Log Collection and Log Analysis

CUDB log collection starts automatically every day at 00:25 and 12:25.



At 00:50 and 12:50, there is a scheduled CUDB log analysis, which saves the detailed result under the following location:

```
/home/cudb/monitoring/preventiveMaintenance/
cron_analysis.<SC_NAME>.log
```

In the above path, <SC\_NAME> can be SC\_2\_1 or SC\_2\_2.

The automatic log analysis can also send alarms: see [General Information](#) on page 4 for more information.

**Note:** Automatic log collection and analysis is performed only in the active SC.

The alarm severity is calculated by the number and the severity of faults found during the last analysis (that is, multiple minor faults can result in a major alarm). All these faults are weighted by CUDB Logchecker, then the severity of alarm is calculated and set, using the weight as input.

The severity levels of the alarm can be as follows:

- warning
- minor
- major
- critical

### 3.2.1 Defining Custom Monitoring Intervals

It is possible to define custom monitoring intervals for CUDB Logchecker. Specify monitoring for both SCs separately.

Configuration can be checked using the `crontab -l` command, as shown in [Example 1](#).

Define the same configuration files on both of the SCs. The paths of the files are as follows:

- /home/cudb/monitoring/preventiveMaintenance/  
logchecker.SC\_2\_1.conf
- /home/cudb/monitoring/preventiveMaintenance/  
logchecker.SC\_2\_2.conf

The following options are accepted, as shown in [Example 2](#):

- `<getlogs_schedule>` : To define the schedule for log collection.
- `<analyser_schedule>` : To define the schedule for log analysis.



**Note:** Follow the standard cron expression format when defining the value of options. Configuration files must take effect after the SC is rebooted. Use the `crontab -e` command to activate cron changes immediately, without rebooting the SC and defining configuration files.

If the configuration files do not exist, the following default options take effect:

- `getlogs_schedule=25 0,12 * * *`
- `analyser_schedule=50 0,12 * * *`

The absence of a configuration file means that the default values are used.

**Note:** Always leave at least 25 minutes between log collection and log analysis, in order to let the log collection finish before the log analysis starts.

### Example 1 Configuration Check

```
CUDB81 SC_2_1# crontab -l
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/var/spool/cron/tabs/root installed on Wed Oct 17 13:59:03 2012)
# (Cron version V5.0 -- $Id: crontab.c,v 1.12 2004/01/23 18:56:42 vixie Exp $)
0,15,30,45 * * * * /home/cudb/oam/performanceMgmt/appCounters/scripts/appCounters.cron >> /dev/null
25 0,12 * * * /bin/bash /opt/ericsson/cudb/OAM/bin/cudbGetLogs
50 0,12 * * * /bin/bash /opt/ericsson/cudb/OAM/bin/cudbAnalyser --auto-check --send-alarm --save-counter > \
/home/cudb/monitoring/preventiveMaintenance/cron_analysis.SC_2_1.log
37 0 * * * /bin/bash /opt/ericsson/cudb/Monitors/bin/cudbCheckConsistency --locked --alarms >/dev/null &
11 2>&1 || true
7 0 * * * /bin/bash /opt/ericsson/cudb/Monitors/bin/cudbCheckReplication --locked --alarms >/dev/null &
1 2>&1 || true
*/1 * * * * /opt/ericsson/cudb/Monitors/keepAlive/bin/keepAlive_monitor.sh 2>&1
```

### Example 2 Configuration File

```
CUDB45 SC_2_1# cat logchecker.SC_2_1.conf
getlogs_schedule=25 0,4,8,12,16,20 * * *
analyser_schedule=50 0,4,8,12,16,20 * * *
```

## 3.3 Manual Log Collection and Analysis

It is possible to use the CUDB Logchecker to help troubleshooting. For more details, refer to [CUDB Troubleshooting Guide](#).



## 4 Troubleshooting cudbAnalyser Results

The following sections describe the possible actions to take for each potential issue found during log analysis.

### 4.1 cudbSystemStatus

**Table 1** shows the cudbSystemStatus faults in different scenarios. For more information on cudbSystemStatus, refer to the cudbSystemStatus section of CUDB Node Commands and Parameters.

Table 1 cudbSystemStatus

Fault	Example Printout	Action
Process not running as expected. <sup>(1)</sup>	<pre>[ERROR] cudbSystemStatus: CU DB Process is not running as expected (Severity: Warning ) [-W-] CudbNotifications proc ess.....Not running in: PL0</pre> <p>Shows which CUDB process is not running as expected.</p>	<p>Run the <b>cudbSystemStatus -p</b> command to check if the problem is resolved.</p> <p>If the printout still shows that a CUDB process is not running, contact the next level of support.</p>
Replication delay of 1000-9999. <sup>(2)</sup>	<pre>[ERROR] cudbSystemStatus: re plication delay: 1000-9999 ( Severity: Warning) Replication in DSG3(Node=246 --Chan=1).. OK -- Delay = 10 21</pre> <p>Shows which replication channel has a delay.</p>	<p>Run the <b>cudbSystemStatus -R</b> command to verify that the replication delay is decreasing.</p> <p>If the replication delay is continuously increasing due to high load, consider reallocation.</p> <p>If the replication delay is not decreasing, contact the next level of support.</p>
Replication delay > 10000.	<pre>[ERROR] cudbSystemStatus: re plication delay &gt; 10000 (Sev erity: Minor) Replication in DSG3(Node=246 --Chan=1).. OK -- Delay = 20 001</pre> <p>Shows which replication channel has a delay.</p>	<p>Run the <b>cudbSystemStatus -R</b> command to verify that the replication delay is decreasing.</p> <p>If the replication delay is continuously increasing due to high load, consider reallocation.</p> <p>If the replication delay is not decreasing, contact the next level of support.</p>



Fault	Example Printout	Action
BC server is not in a good shape.	[ERROR] cudbSystemStatus: BC Server is not in a good shape. (Severity: Major) BC server in PL_2_5 ..... . not running	Run the <b>cudbSystemStatus -b</b> command to check if the problem persists. If yes, contact the next level of support.
Unexpected MySQL connection state.	[ERROR] cudbSystemStatus: Unexpected MySQL connection state (Severity: Critical) [-W-] MySQL Access Server connection Fault in....: DS6_0	Some maintenance actions may lead to this alert. If there are no maintenance actions ongoing at the time cudbSystemStatus is checked and the fault persists, contact the next level of support.
Unexpected cluster status.	[ERROR] cudbSystemStatus: Unexpected cluster status in CUDB system (Severity: Critical) 131080-1Unreachable 141080-1Unreachable [-W-]There are Clusters in wrong state	Some maintenance actions may lead to this alert. If there are no maintenance actions ongoing at the time cudbSystemStatus is checked and the fault persists, contact the next level of support.
Wrong cluster state or replication state.	[ERROR] cudbSystemStatus: Wrong cluster state or replication state found in CUDB system (Severity: Critical) DSG13 is in wrong state DSG14 is in wrong state	Run the <b>cudbSystemStatus -r</b> command to check if the problem persists. If yes, contact the next level of support.

(1) Storage engine process can take up to one hour to restart.

(2) Replication delay is normal in the following situations: (a) Backbone issues or right after backbone issue (b) Backup restore (c) The affected PL or DS was in maintenance mode or unavailable.

## 4.2 NDB

Table 2 shows the NDB faults due to the execution of cudbAnalyser in different scenarios.

Table 2 NDB

Fault	Example Printout	Action
NDB cluster logs.	[ERROR] NDB: Errors found in NDB cluster logs (Severity: Warning) > 2013-07-17 09:55:51 [MgmtSrvr] ALERT \\\n-- Node 3: Arbitration check won - node group majority	If this printout comes without any other alarm or explanation for the last 12-hour monitoring period, contact the next level of support to investigate the cause.
ndb_out logs.	[ERROR] NDB: Errors found in ndb_out logs (Severity: War	If this printout comes without any other alarm or explanation for the



Fault	Example Printout	Action
	ning) [ndbd] ALERT -- Node 4: Forced node shutdown completed. Caused by error 2303: 'System error, node killed during node restart by other node (Internal error, programming error or missing error message, please report a bug). Temporary error, restart node'.	last 12-hour monitoring period, contact the next level of support to investigate the cause.
Database cluster hanging in phase 4.	[ERROR] NDB: Mysql hanging in Phase 4 (Severity: Warning) > 2016-03-18 19:26:56 [ndbd] INFO -- refing dict lock to 4	It is recommended to contact the next level of support to investigate the cause.

## 4.3 OS

Table 3 shows OS faults in different scenarios.

Table 3 OS

Fault	Example Printout	Action
High CPU load. <sup>(1)</sup>	[ERROR] OS: high CPU load (Severity: Major) CUDB119 oam2 00:26am up 6 days 16:10, 0 users, load average: 25.35, 17.76, 14.16	Log in to the affected blade or VM, and run the <b>top</b> command to check if the load is still high.  If a software fault is suspected, contact the next level of support.
procs_blocked > 9, indicating high load, or hanging IO.	[ERROR] OS: Kernel printout: procs_blocked > 9, indicating high load, or hanging IO (Severity: Major) CUDB100 oam2 procs_blocked 10  This kernel printout shows which blade or VM is affected.	Check if there is another error printout by CUDB Logchecker that pinpoints an infrastructure or load related error.  Log in to the affected blade or VM and run the <b>dmesg</b> command to see if the problem is caused by IO issues.  Log in to the affected blade or VM and run the <b>top</b> command to see if the problem is caused by high load.  It is recommended to contact the next level of support to investigate the issue. <sup>(2)</sup>



Fault	Example Printout	Action
dmesg shows IO error or EXT3 filesystem error.	<pre>[ERROR] OS: dmesg shows IO error or EXT3 filesystem error (Severity: Major) Feb  2 20:55:10 PL_2_5 kernel: end_request: I/O error, device sda, sector 112313 Feb  2 20:55:10 PL_2_5 kernel: Buffer I/O error on device sda1, logical block 14039</pre> <p>Shows which blade or VM is affected.</p>	Contact the next level of support to investigate the issue. <sup>(2)</sup>
dmesg shows filesystem is mounted as read-only.	<pre>[ERROR] OS: dmesg shows that filesystem is remounted as read-only (Severity: Major) Feb  2 20:55:15 PL_2_5 kernel: Remounting filesystem read-only</pre> <p>Shows which blade or VM is affected.</p>	Contact the next level of support to investigate the issue. <sup>(2)</sup>
Network stat shows errors.	<pre>[ERROR] OS: network stat shows errors (Severity: Minor) &gt; CUDB124 oam1 eth3/statistics/rx_dropped 16467 K packets &gt; CUDB124 oam1 bond0/statistics/rx_dropped 16467 K packets &gt; CUDB124 oam2 eth3/statistics/rx_dropped 803 K packets &gt; CUDB124 oam2 bond0/statistics/rx_dropped 803 K packets</pre> <p>Shows which blade or VM is affected.</p>	Contact the next level of support to investigate the issue. <sup>(2)</sup>
For CUDB systems deployed on native BSP 8100, SMART (Self-Monitoring, Analysis and Reporting Technology) data indicates a possible imminent drive failure. <sup>(3)</sup>	<pre>[ERROR] OS: SMART Health Status is NOT OK! (Severity: Major) CUDB136 oam1 SMART Health Status: HARDWARE IMPENDING FAILURE DATA ERROR RATE TOO HIGH [asc=5d, ascq=12] CUDB136 PL2 SMART Health Status: HARDWARE IMPENDING FAILURE DATA ERROR RATE TOO HIGH [asc=5d, ascq=12]</pre>	A drive in the affected blade shows a pre-failure condition. To avoid blade failure, the blade containing the drive must be replaced. <sup>(4)</sup>



Fault	Example Printout	Action
New core dumps were generated.	[ERROR] OS: New core dumps were generated under /local2/dumps in the PLs and under /cluster/dumps in PL_2_5 (More details inside <cudb_pl_core_dumps> in log files) (Severity: Major) > -rw----- 1 root root 367984640 Feb 12 15:10 slapd.31928.PL_2_3.core	Contact the next level of support to investigate the issue.
New printouts regarding system Out of Memory Killer.	[ERROR] OS: New printouts regarding system Out of Memory Killer (Severity: Warning) > May 10 17:37:05 PL_2_3 kernel: [191935.037336] Out of memory: Kill process 26499 (slapd) score 452 or sacrifice child	Contact the next level of support to investigate the issue.
dmesg has changed.	[ERROR] OS: dmesg has changed (Severity: Warning) > CUDB31 PL0 [1052612.453321] Clock: inserting leap second 23:59:60 UTC	Contact the next level of support.
There are more than one NTP peers configured for synchronization.	[ERROR] OS: syncing from different ntp peers? (Severity: Warning)	—Check for NTP alarms. —Check the NTP status by issuing the <b>ntpq -p</b> status to the affected blade.
Payload blade has been started with the parameter NUMA enabled (Non-Uniform Memory Access).	[ERROR] OS: Kernel printout: payload blade not started with numa=off (Severity: Warning) > CUDB31 DS10_1 initrd=netboot_initrd i8042.noaux i8042.nokbd i8042.nomux panic=10 console=tty0 console=ttyS0,115200 cluster=(type=payload,disk_cache=0,clean_rootfs=0) numa=off transparent_hugepage=madvise intel_idle.max_cstate=1 BOOT_IMAGE=vmlinuz ip=192.168.0.26:192.168.0.101:0.0.0:255.255.255.0 BOOTIF=01-90-38-09-8e-62-33	Contact the next level of support.
A hardware error has been detected.	[ERROR] kernel: Hardware Error found (Severity: Major)	Contact the next level of support.



Fault	Example Printout	Action
	Jul 19 18:35:16 SC_2_1 kernel: [ 8757.942729] [Hardware Error]: Machine check events logged	

- (1) High load for the nbbd process is normal. High load is present during manual LDAP import/export operations.
- (2) This printout is never considered to be normal.
- (3) For CUDB systems deployed on a cloud infrastructure, the Hardware Monitoring function should be used instead of the SMART function.
- (4) For more information on blade replacement, refer to the *Replacing a Blade* section of Server Platform, Blade Replacement.

## 4.4 Config

Table 4 shows config fault in different scenarios.

Table 4 Config

Fault	Example Printout	Action
Error in custom cudb config checks.	[ERROR] Config: Error in custom cudb config checks (Severity: Major) ERROR: cluster alarm -l -a alarm list is not empty  Shows which config checks have failed.	Contact the next level of support to investigate the issue.
LDAP FE log rotate is not defined in cluster.conf	[ERROR] CONFIG: ldapfe log rotation not defined.	Contact the next level of support.

## 4.5 SWM

Table 5 shows SWM fault in different scenarios.

Table 5 SWM

Fault	Example Printout	Action
Multiple revisions from package: [package name].	[ERROR] SWM: Multiple revisions from package (Severity: Minor) CUDB_NODE_CONFIG-CXP9015320	Check <b>cmw-repository-list</b> on the node, and verify that the package shown in the printout has still more than one versions.



Fault	Example Printout	Action
		<p>Verify that there is no ongoing SW update or upgrade on the CUDB node, as the printout is normal in these cases.</p> <p>Contact the next level of support to investigate and resolve the issue.<sup>(1)</sup></p>

(1) Multiple revisions from one package in smf repository causes problems if an upgrade is attempted.

## 4.6 Database Cluster

Table 6 shows database cluster faults in different scenarios.

Table 6 Database Cluster

Fault	Example Printout	Action
Binlog is not written.	<pre>[ERROR] MYSQL: Binlog is not written (Severity: Major) CUDB41 DS1_0 0</pre> <p>Shows the blade or VM where the binlog is not written.</p>	Run manual log collection and manual log analysis to verify that the problem is still present. <sup>(1) (2)</sup>
Incorrect key file for table.	<pre>[ERROR] MYSQL: Incorrect key file for table (Severity: M ajor) Sep 16 09:50:54 PL_2_5 mysql d: 110916 9:50:54 [ERROR] mysqld: Incorrect ke y file for table './mysql/nd b_binlog_index.MYI'; try to repair it Sep 16 09:50:54 PL_2_5 mysql d: 110916 9:50:54 [ERROR] mysqld: Incorrect ke y file for table './mysql/nd b_binlog_index.MYI'; try to repair it</pre>	Contact the next level of support.
Unstable NTP service.	<pre>[ERROR] NDB: Time moved forw ard with 200 milliseconds (S everity: Warning) &gt; Time moved forward with 20 0 milliseconds</pre>	<p>—Check LOTC alarms.</p> <p>—Check the stability of the NTP system.</p> <p>—Strengthen the NTP system if necessary.</p>



Fault	Example Printout	Action
Data node has been crushed.	[ERROR] NDB: There are new entries in ndb error dumps (Severity: Warning) > CUDB31 PL0 Current byte-offset of file-pointer is: 3063	Contact the next level of support.
MYSQL cluster logs.	[ERROR] MYSQL: Errors found in mysql cluster logs (Severity: Warning) > May 11 13:09:02 PL_2_3 mysqld: 2017-05-11 13:09:02 0 [Warning] TIMESTAMP with implicit DEFAULT value is deprecated. Please use --explicit_defaults_for_timestamp server option (see documentation for more details).	This is a generic statement mysql cluster logs errors and can be provoked by any unexpected mysql behavior. If this printout appears without any other alarm or likely cause for the previous 12-hour monitoring period, contact the next level of support.

(1) This error printout is raised if the binlog is not written for the last 1440 minutes. This is normal for PLDB blades or VMs if there was no provisioning in the last 1440 minutes. In any other case, contact the next level of support.

(2) For more information, see [Manual Log Collection and Analysis](#) on page 6.

## 4.7 LDAP

[Table 7](#) shows LDAP faults in different scenarios.

Table 7 LDAP

Fault	Example Printout	Action
Traffic bursts or the client is not able to handle responses fast enough.	[ERROR] LDAP: Deferring operations found in ldap logs (Severity: Critical) > Sep 8 00:33:23 PL_2_16 slapd[23297]: connection_input: conn=30556 deferring operation: binding > Sep 8 00:36:40 PL_2_18 slapd[25017]: connection_input: conn=30623 deferring operation: binding	Contact the next level of support to check the LDAP FE log files of the affected blades.
Various errors found.	[ERROR] LDAP: various errors found in LDAP logs (Severity: Critical) > May 12 00:17:29 PL_2_3 slapd[17513]: conn=2611 op=1	Investigate the error codes in the log output. <sup>(1)</sup>



Fault	Example Printout	Action
	<pre> MODIFY RESULT tag=103 err=53 text=No available master replica for DSG 3 req=serv=csps,mscId=39,ou=multiSCs,CUDBNode=47,dc=ericsson,dc=com [ERROR] LDAP: err=52 errors found in LDAP logs (Severity: Critical)  &gt; May 12 01:14:46 PL_2_8 slapd[10961]: conn=6458 op=0 BIND RESULT tag=97 err=52 text=CUDB node 47 is temporarily out of service req=cn=manager,ou=ft,o=cudb, c=es </pre>	
<p>—Busy.</p> <p>—Overload or congestion in the processing layer at CUDB node level.</p> <p>—Administrative limit exceeded.</p>	<pre> [ERROR] LDAP: err=51 errors found in LDAP logs (Severity: Warning)  &gt; CUDB31 DS10_1 Aug 18 04:29:51 PL_2_3 slapd[10356]: conn=2155516 op=22 SEARCH RESULT tag=101 err=51 nentries=0 text=LDAP server overloaded in node 11 </pre>	If the alert is produced frequently, contact the next level of support for a deeper analysis. <sup>(1)</sup>
Unavailable.	<pre> [ERROR] LDAP: err=52 errors found in LDAP logs (Severity: Critical)  &gt; May 12 01:14:46 PL_2_8 slapd[10961]: conn=6458 op=0 BIND RESULT tag=97 err=52 text=CUDB node 47 is temporarily out of service req=cn=manager,ou=ft,o=cudb, c=es </pre>	<p>—Application Front Ends (FEs) should automatically re-route the traffic towards a different CUDB node. <sup>(1)</sup></p> <p>—Ongoing maintenance operations may cause this error. Contact the next level of support to perform a detailed analysis if the root for the out of service node cannot be determined. <sup>(1)</sup></p>
Unwilling to perform.	<pre> [ERROR] LDAP: err=53 errors found in LDAP logs (Severity: Critical)  &gt; May 12 00:17:29 PL_2_3 slapd[17513]: conn=2611 op=1 MODIFY RESULT tag=103 err=53 text=No available master replica for DSG 3 req=serv=csps,mscId=39,ou=multiSCs,CUDBNode=47,dc=ericsson,dc=com </pre>	No special actions are expected from the LDAP client. CUDB is handling the internal fault.



Fault	Example Printout	Action
<p>—Other error.</p> <p>—Problem in some internal component or resource that prevents it to successfully process the request. Other parts of the system may be operating under normal conditions and return successful responses.</p>	<pre>[ERROR] LDAP: err=80 errors found in LDAP logs</pre> <pre>Sep 13 10:20:39 PL_2_9 slapd[8882]: conn=305292 op=4686 RESULT tag=107 err=80 text=REDO buffers overloaded (increase RedoBuffer)</pre> <pre>Sep 13 10:20:40 PL_2_9 slapd[8882]: conn=310253 op=1875 RESULT tag=107 err=80 text=REDO buffers overloaded (increase RedoBuffer) Action:</pre>	<p>The possible cause of this error is the temporary unavailability of an internal component, or the temporary internal overload of a specific partition or node. Reduce the traffic or provisioning load to stabilize the system or speed up application and lower the number terminal retries rejected by CUDB with error 80.<sup>(2)</sup></p>
<p>REDO buffers overloaded.</p>	<pre>[ERROR] LDAP: err=80 errors with REDO buffers overloaded found in LDAP logs</pre> <pre>Sep 13 10:20:39 PL_2_9 slapd[8882]: conn=305292 op=4686 RESULT tag=107 err=80 text=REDO buffers overloaded (increase RedoBuffer)</pre> <pre>Sep 13 10:20:40 PL_2_9 slapd[8882]: conn=310253 op=1875 RESULT tag=107 err=80 text=REDO buffers overloaded (increase RedoBuffer)</pre>	<p>—This error appears when the REDO buffer of NDB cannot be written to disk. The possible root cause is either overload or hardware failure. Analyze other system health reports to determine whether the problem is hardware failure or an overload.</p> <p>—Use the <b>cudbCollectInfo -n &lt;nodeid&gt; -a all</b> command.<sup>(3) (4)</sup></p> <p>—Contact the next level of support.</p>

(1) For more information on error codes, refer to CUDB LDAP Interwork Description and CUDB LDAP Data Access.

(2) For more information on error codes, refer to CUDB LDAP Interwork Description.

(3) Refer to the *Collecting Application and Platform Logs* section of Data Collection Guideline for CUDB for more information.

(4) Refer to the *Collecting Additional Logs* section of Data Collection Guideline for CUDB for information on collecting additional logs.

## 4.8 System Monitor

Table 8 shows System Monitor faults in different scenarios.



Table 8 System Monitor

Fault	Example Printout	Action
System Monitor logs indicate there were major errors.	<pre>[ERROR] System Monitor logs indicate there were major er rors (Severity: Major) &gt; Apr 19 18:21:33 SC_2_1 SM[ 23399]: INFO  Auxiliar conne ction with site 2 has change d to LOST &gt; Apr 19 18:21:34 SC_2_1 SM[ 23399]: INFO  Connection sta tus between SM leader in sit e 1 (S1-N202-I1) and BC serv ice in site 2 has change to LOST</pre>	Run the <b>cudbSystemStatus -b</b> command to check if the problem persists. If yes, contact the next level of support.
System Monitor logs indicate there were some warnings.	<pre>[ERROR] System Monitor logs indicate there were some war nings [Towards site 2; Event count 14] (Severity: Warnin g) &gt; Apr 20 01:10:25 SC_2_1 SM[ 23399]: INFO  Auxiliar conne ction with site 2 has change d to SUSPENDED &gt; Apr 20 01:10:26 SC_2_1 SM[ 23399]: INFO  Auxiliar conne ction with site 2 has change d to RECONNECTED</pre>	Run the <b>cudbSystemStatus -b</b> command to check if the problem persists. If yes, contact the next level of support.

## 4.9 BC Server

[Table 9](#) shows BC Server faults in different scenarios.

Table 9 BC Server

Fault	Example Printout	Action
BC Server logs indicate there were minor errors.	<pre>[ERROR] BC Server logs indic ate there were minor errors (Severity: Minor) &gt; Apr 20 09:25:37 SC_2_2 BC[ myid:11]: INFO  Got user-lev el KeeperException when proc essing sessionid:0xa52fbde98 5d104a type:ping cxid:0xffff ffffffffffe zxid:0xffffffff fffffffffe txntype:unknown req</pre>	It is recommended to contact the next level of support to investigate the issue.



Fault	Example Printout	Action
	path:n/a Error Path:null Error:KeeperErrorCode = Session moved	
BC Server logs indicate there were major errors.	<pre>[ERROR] BC Server logs indicate there were major errors (Severity: Major) &gt; Feb 18 13:17:46 SC_2_2 BC[myid:11]: ERROR Unexpected exception causing shutdown while sock still open &gt; Feb 18 13:17:47 SC_2_2 BC[myid:11]: INFO Shutting down &gt; Feb 18 13:17:47 SC_2_2 BC[myid:11]: INFO Shutdown called</pre>	It is recommended to contact the next level of support to investigate the issue.

## 4.10 Master Unavailability

Table 10 shows Master Unavailability fault in different scenarios.

Table 10 Master Unavailability

Fault	Example Printout	Action
Master is not available for DSG.	<pre>[ERROR] Error: Master is not available for DSG (Severity: Major) &gt; Feb 12 14:45:06 SC_2_1 CS[14068]: Monitoring [ClusterSupervisor]: INFO - N203D0-6-BCCClient: Enter getMasterStatus: masterless &gt; Feb 12 14:45:06 SC_2_1 CS[14068]: Monitoring [ClusterSupervisor]: INFO - N203D0-6-BCCClient: Information read in node /cudb/masterList/D0 - &gt; masterless</pre>	Run the <b>cudbSystemStatus -R</b> command to check if the problem persists. If yes, contact the next level of support.

## 4.11 Software Platform

Table 11 shows Software Platform faults in different scenarios.



Table 11 Software Platform

Fault	Example Printout	Action
Not all SU have Operational State Enabled.	[ERROR] SAF: Not all SU have Operational State Enabled (Severity: Warning) saAmfNodeOperState."safAmfNode=SC-1,safAmfCluster=myAmfCluster": Disabled	Run the <b>cudbHaState</b> command to check if the problem persists. If yes, contact the next level of support.
There are unassigned HA states.	[ERROR] SAF: there are unassigned HA states (Severity: Warning) saAmfSISUHASState."safSu=SC-1,safSg=NWA,safApp=ERIC-ldews.pmcounters.sc"."safSi=ldews.pmcounters.sc-NWA-1"."safSi=NoRed8": unassigned(3)	Run the <b>cudbHaState</b> command to check if the problem persists. If yes, contact the next level of support.
One or more nodes are locked in the cluster.	[ERROR] SAF: One or more node is locked in the cluster (Severity: Warning) saAmfNodeAdminState."safAmfNode=SC-1,safAmfCluster=myAmfCluster": Locked	Run the <b>cudbHaState</b> command to check if the problem persists. If yes, contact the next level of support.
There are active cluster alarms.	[ERROR] SAF: There are active cluster alarms (Severity: Major) Node Hostname Severity Type Problem Information 1 SC_2_1 Major 2 Ethernet Bonding Bonding degraded on bond0 (link down on eth4)	Run the <b>cluster alarm -a -l</b> command to check which alarms are in the system. If no reason is found for the alarms, contact the next level of support.

## 4.12 Alarm

Table 12 shows ALARM faults in different scenarios.

Table 12 Alarm

Fault	Example Printout	Action
There are active alarms.	[ERROR] ALARM: There are active alarms (Severity: Critical)  Timestamp First : Mon Nov 28 05:15:05 GMT 2016	Run the <b>factivealarms</b> command to see all active alarms. (1)



Fault	Example Printout	Action
	Timestamp Last : Mon Nov 28 05:15:05 GMT 2016  Active Description : Root Login Failed @172.17.17.10	

(1) For more information on alarms, refer to CUDB Node Fault Management Configuration Guide.

## 4.13 Log

Table 13 shows LOG faults in different scenarios.

Table 13 Log

Fault	Example Printout	Action
Potentially harmful situation.	[ERROR] LOG: New printouts with EMERG level (Severity: Warning) > May 12 07:48:35 SC_2_1 clsupervisor[16467] : Monitoring : EMERG - main: Failed to read configuration	This is generic error message that can refer to any component. Refer to CUDB Node Logging Events for troubleshooting information. If the cause cannot be determined, contact the next level of support.
Error conditions.	[ERROR] LOG: New printouts with ERROR level (Severity: Warning)  > May 11 13:08:56 SC_2_1 clsupervisor[13154] : Monitoring : INFO - N8D0-cl_control: testSQLNodeConnections failed for node 49 a1 on host 10.22.8.3 port 15000, user root with error: ErrCode: 2003 Err message: Can't connect to MySQL server on '10.22.8.3' (111) SQLState: HY000	This is generic error message that can refer to any component. Refer to CUDB Node Logging Events for troubleshooting information. If the cause cannot be determined, contact the next level of support.
Component or subcomponent is unusable.	[ERROR] LOG: New printouts with WARNING level (Severity: Warning)  > May 11 13:08:57 SC_2_1 clsupervisor[13154] : Monitoring : WARNING - N8D0-cl_control: Clean stop procedure for Mysql server	This is generic error message that can refer to any component. Refer to CUDB Node Logging Events for troubleshooting information. If the cause cannot be determined, contact the next level of support.



Fault	Example Printout	Action
	with ndb node id 49 failed on 10.22.8.3 with error: ErrCode: 2003 Err message: Can't connect to MySQL server on '10.22.8.3' (111) SQLState: HY000. Killing the server.	



## 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. Preventive Maintenance, Logchecker Found Error(s)
2. CUDB Node Preventive Maintenance
3. CUDB Troubleshooting Guide
4. CUDB Node Commands and Parameters
5. Server Platform, Blade Replacement
6. CUDB LDAP Interwork Description
7. CUDB LDAP Data Access
8. Data Collection Guideline for CUDB
9. CUDB Node Fault Management Configuration Guide
10. CUDB Node Logging Events
11. CUDB Glossary of Terms and Acronyms