

# Virtualized CUDB Virtual Machine Recovery

## 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

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Description	1
1.2	Target Groups	3
1.3	Revision Information	3
1.4	Typographic Conventions	4
<b>2</b>	<b>Reboot and Rebuild the VM</b>	<b>5</b>
2.1	Reboot the VM	5
2.2	Rebuild the VM	6
<b>3</b>	<b>Actions in the Case of Infrastructure Activities</b>	<b>8</b>
3.1	One Compute Host Affected	9
3.2	Multiple Compute Hosts Affected	9
3.3	Identify All Affected VMs	10
3.4	Recovery of Multiple VMs in Parallel	12
3.5	Prepare the VMs for Operation	15
	<b>Glossary</b>	<b>17</b>
	<b>Reference List</b>	<b>18</b>





# 1 Introduction

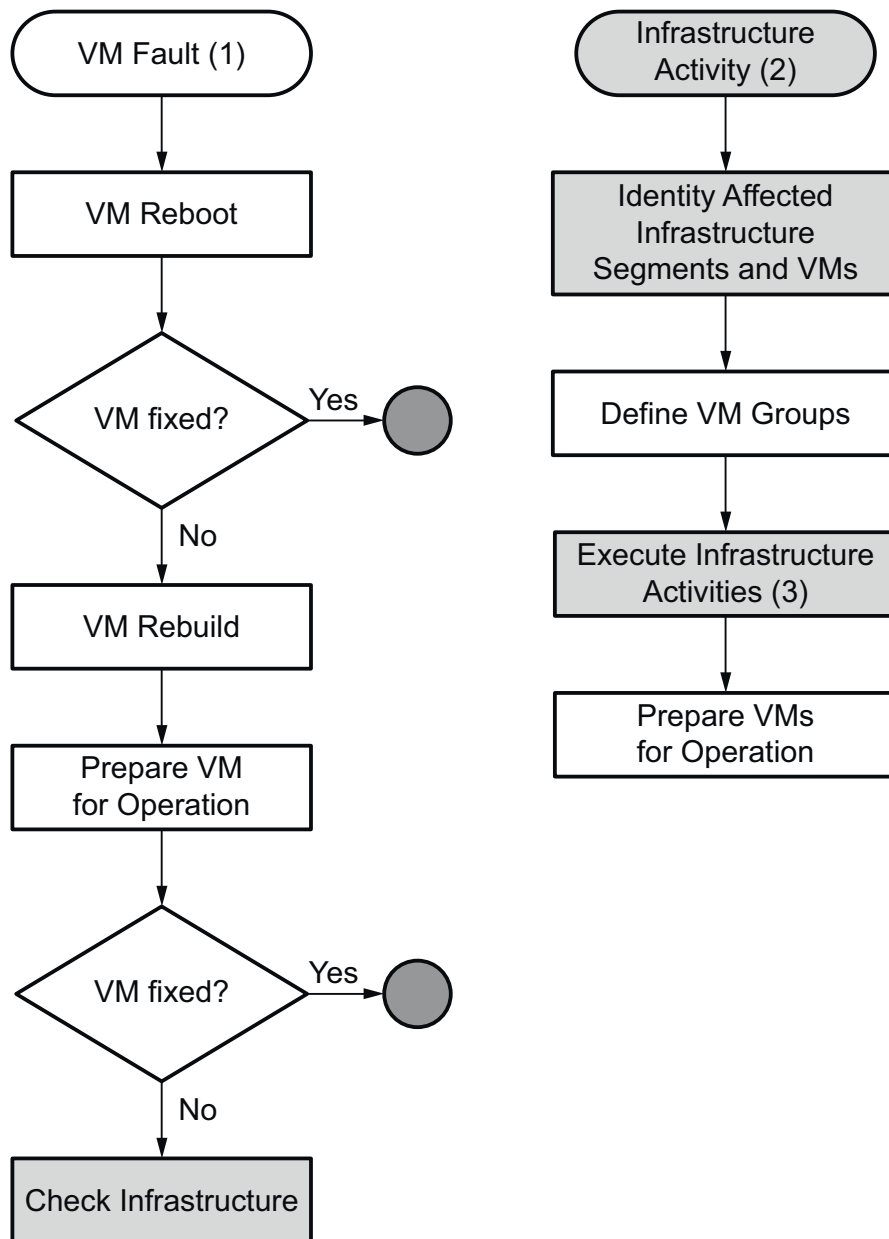
This document describes how to recover a Virtual Machine (VM) in an Ericsson Centralized User Data Base (CUDB) node deployed on a cloud infrastructure.

## 1.1 Description

This Operating Instruction (OPI) describes how to recover a VM in a virtualized CUDB node. Specifically, it describes the following procedures:

- Manually recovering the VM by means of rebooting or rebuilding it.
- Preparing the CUDB node and system to gracefully handle and recover from an infrastructure activity.

The major steps of the recovery procedures listed above are shown in [Figure 1](#).



(1) Where reboot is recommended in CUIDB procedures, or after other procedures have been exhausted.

(2) Triggered by VM faults, or other reasons.

(3) Aligned with VM grouping.


 Cloud Infrastructure Level

Figure 1 VM Recovery Procedures



## 1.2 Target Groups

This document is intended for system administrators operating CUDB systems. For some of the actions described in the document, cloud administration role is also required. The cloud administrator is the cloud service provider who delivers the cloud service and executes required actions on the cloud infrastructure.

## 1.3 Revision Information

### Rev. A

Initial release.

### Rev. B

Editorial changes only.

### Rev. C

Other than editorial changes the document has been revised as follows:

- [Rebuild the VM](#) on page 6: Added a note regarding restoring stored procedures after blade replacement.

### Rev. D

Other than editorial changes the document has been revised as follows:

- [Prepare SC VM](#) on page 15: Updated [Step 3 in Section 3.5.1](#) in the SC VM preparation procedure.
- [Prepare PLDB or DSG VM](#) on page 16: Removed obsolete step.

### Rev. E

Other than editorial changes the document has been revised as follows:

- [Rebuild the VM](#) on page 6: Updated description.

### Rev. F

Other than editorial changes the document has been revised as follows:

- **Preparations for PLDB or DSG VM Recovery:** Removed section.
- [Execute Parallel Recovery](#) on page 14: Removed former **Step 2**.
- Former section **Cloud Administration Actions After Infrastructure Maintenance:** Updated procedure.



- [Prepare PLDB or DSG VM](#) on page 16: Removed case from the list of applicable steps to prepare the recovered PLDB or DSG VM for operation.

### Rev. G

Other than editorial changes the document has been revised as follows:

- [Identify All Affected VMs](#) on page 10: Added attention.

### Rev. H

Other than editorial changes the document has been revised as follows:

- [Description](#) on page 1: Updated [Figure 1](#) and the description of the document.
- [Rebuild the VM](#) on page 6: Updated procedure, and removed description and `cudbPrepareStore --pl` command.
- [Actions in the Case of Infrastructure Activities](#) on page 8: Updated title, description, and the structure of the section by moving the steps of preparing the CUDB node and system to recover from maintenance activity to [Multiple Compute Hosts Affected](#) on page 9, and added Attention, procedure and Do.
- [One Compute Host Affected](#) on page 9: Added section.
- [Multiple Compute Hosts Affected](#) on page 9: Added section.
- [Identify All Affected VMs](#) on page 10: Removed description, added procedure, and updated Attention.
- [VM Groups](#) on page 13: Updated Do, note, description, and procedure.
- Former section **Cloud Administration Actions After Infrastructure Maintenance**: Removed section.
- [Prepare the VMs for Operation](#) on page 15: Removed Do, added note.
- [Prepare SC VM](#) on page 15: Updated procedure and description.
- [Prepare PLDB or DSG VM](#) on page 16: Added description, removed procedure.

## 1.4 Typographic Conventions

Typographic Conventions can be found in the following document:

- [Typographic Conventions](#)



## 2 Reboot and Rebuild the VM

If a VM is having issues and all applicable CUDB recovery procedures outlined in [CUDB Troubleshooting Guide](#) have been performed, but the VM still did not recover, it can be rebooted from the cloud infrastructure (see [Reboot the VM](#) on page 5). If rebooting does not solve the issue, or if the VM must be reinstalled, the VM can also be rebuilt (see [Rebuild the VM](#) on page 6).

### 2.1 Reboot the VM

Perform the following steps to reboot the VM from the cloud infrastructure.

---

---

#### Attention!

Any custom data not saved in the `/local` or `/local2` folders will be lost after rebooting.

---

---

#### Steps

In case of using Cloud Execution Environment (CEE), follow the below steps to reboot the VM:

1. Login to the Atlas Dashboard.
2. Select the appropriate project in the **Current Project** field, then select **Project** in the **View** field.
3. Choose the **Instances** category.
4. Identify the VM to reboot.
5. In the **Actions** column of the identified VM, select the action **Soft Reboot Instance** to use graceful shutdown, or the action **Hard Reboot Instance** to use non-graceful shutdown. Refer to the "Openstack End User Guide" or the "Atlas Dashboard End User Guide" documents of the CEE Customer Product Information (CPI) for more details.
6. While the reboot process is ongoing, the **Status** column of the instance will show REBOOT. Once it becomes ACTIVE, the processes in the VM will begin to start up.
7. If the issue still persists after the VM has fully started up, rebuild the VM by performing the steps of [Rebuild the VM](#) on page 6.

#### After This Task

Refer to the "Atlas Dashboard End User Guide" document in the CEE documentation for more information on how to reboot VMs if using CEE. In case



of using a different cloud solution, refer to the solution-specific documentation for more information.

## 2.2 Rebuild the VM

VMs are rebuilt during node installation to ensure the automatic recovery of System Controllers (SCs), or when any VM is reinstalled.

---

---

### Attention!

All data on the VM will be lost when it is about to be reinstalled.

---

---

#### Steps

In case of using CEE, follow the steps below to rebuild the affected VM:

1. Login to the Atlas Dashboard.
2. Select the appropriate project in the **Current Project** field, then select **Project** in the **View** field.
3. Choose the **Instances** category.
4. Identify the VM to rebuild.
5. In the **Actions** column of the identified VM, select the action **Rebuild Instance**.
6. In the **Rebuild Instance** window, choose the **Payload** image option from the **Select Image** drop-down box to allow the VM to boot from network.
7. Once the image is chosen, select **Rebuild**.
8. While the rebuild process is ongoing, the **Status** column of the instance will show REBUILD. Once it becomes ACTIVE, the processes in the VM will begin to start up.
9. Depending on the type of the VM, perform the applicable steps below to prepare the recovered VM for operation:
  - If the rebuilt VM is an SC, wait until the synchronization between the SCs is completed. Use the following command to check the synchronization status:

```
cat /proc/drbd
```



**Note:** Once the synchronization is finished, any custom `crontab` jobs and their definitions (or similar tasks) which are not deployed by default in CUDB or scheduled with data or software backup scripts will be lost. If necessary, redeploy them after the procedure is completed.

- If the rebuilt VM belongs to a Data Store Unit Group (DSG), and replication issues are detected after all the processes in the VM started up, perform a combined unit data backup and restore as described in the *Performing Combined Unit Data Backup and Restore* section of CUDB Backup and Restore Procedures.

### After This Task

**Note:** After finishing the rebuild procedure, the stored procedures are not restored so it is recommended to recreate them with the following command: `cudbManageStore -p -o restorestoredprocedures`

Refer to the Atlas Dashboard End User Guide document in the CEE documentation for more information on how to rebuild VMs if using CEE. In case of using a different cloud solution, refer to the solution-specific documentation for more information.



## 3 Actions in the Case of Infrastructure Activities

This section describes how to prepare the CUDB node and system to gracefully handle and recover from both planned and unplanned activities on the infrastructure level.

In general, upon infrastructure activities including compute host shutdown/reboot, VMs evacuate automatically on remaining functional host(s) in their failure domain. Same behavior is expected in the case of a sudden compute host failure. To check if the VM is evacuated, on the cloud infrastructure, check actions/events under VM information. For more information about failure domains, refer to the *Infrastructure Availability for CUDB Systems Deployed on a Cloud Infrastructure* section of CUDB High Availability. For more information about the VM evacuation infrastructure related requirements, refer to the Other Requirements section of CUDB Virtual Infrastructure Requirements.

---

---

### Attention!

If VM's failure domain does not have spare resources configured as described in the *Infrastructure Availability for CUDB Systems Deployed on a Cloud Infrastructure* section of CUDB High Availability, or VM is previously shutdown/powered off (when using CEE), VM evacuation is not possible and VM will not be available until previously used host affected with infrastructure activity becomes available. In systems deployed on CEE cloud infrastructure, VM Evacuation Failed alarm is expected to be raised. Check with the cloud administrator if the mentioned alarm is raised and cloud infrastructure documentation for alarm Operating Instruction.

---

---

For more information on how to check if compute host is running out of resources or if it is underperforming, refer to the documentation provided by the cloud infrastructure. For example, if the infrastructure is the CEE, refer to the CEE Troubleshooting Guideline in the Cloud Execution Environment CPI.

---

---

### Do!

In case compute host is underperforming because of hardware faults for example, shut down the affected VM(s) until the compute host is recovered or replaced.

---

---

When using CEE, if underlying compute host is underperforming, perform the following steps to shut down the affected VM:



### Steps

1. Login to the **Atlas Dashboard**.
2. Select the appropriate project in the **Current Project** field, then select **Project** in the **View** field.
3. Choose the **Instances** category.
4. Identify the VM to shut down.
5. In the **Actions** column of the identified VM, select the action "Shut Off Instance".

### Results

Depending on the type of infrastructure activity, if the activity will result, or has already resulted, in shutdown or reboot of:

- One compute host, perform the steps in [One Compute Host Affected](#) on page 9.
- Multiple compute hosts, perform the steps in [Multiple Compute Hosts Affected](#) on page 9.

## 3.1 One Compute Host Affected

If the infrastructure activity results in a compute host shut down or reboot, no manual activities are needed to prepare the VMs.

To recover evacuated VM(s), perform the following steps:

### Steps

1. Identify all affected VMs, if they are not known already (see [Identify All Affected VMs](#) on page 10).
2. Prepare the evacuated VMs for operation (see [Prepare the VMs for Operation](#) on page 15).

## 3.2 Multiple Compute Hosts Affected

If the infrastructure activity results in multiple compute host shutdown or reboot, it must be ensured that those activities are executed in order that **Cloud administration related security** infrastructure requirement is respected. During this process, VMs will evacuate automatically on remaining functional host(s) in their failure domain. Refer to the Other Requirements section of CUDB Virtual Infrastructure Requirements for more information about that requirement.

Perform the following steps to recover VM groups:



## Steps

1. Identify the VM groups and prepare the system for parallel recovery (see [Recovery of Multiple VMs in Parallel](#) on page 12).
2. Prepare the evacuated VMs for operation (see [Prepare the VMs for Operation](#) on page 15).

## 3.3 Identify All Affected VMs

To identify the VMs that will be or have already been affected by the infrastructure activity, either do the following:

- Perform the steps described in [Cloud Administration Actions to Identify Infrastructure Position](#) on page 11 if VMs are already known and infrastructure segment has yet to be identified.
- Perform the steps described in [Cloud Administration Actions to Identify Affected VMs](#) on page 12 if infrastructure segment is known and affected VMs have yet to be identified.

---

### Attention!

If the identified VM to be recovered belongs to a DSG replica, that DSG replica will result in a degraded state. If a DSG master replica is degraded due to hardware or software failure, the system selects a new master for the DSG provided that at least one other slave replica of the DSG is available, not degraded and with a replication delay below than 3 seconds; otherwise smooth mastership change will not happen until the previous conditions are met. Therefore, if the master remains in the degraded replica, the infrastructure activity or VM recovery must be performed in low traffic periods if possible. If not, repair the other replica so the smooth mastership change occurs and the mastership is removed from the degraded one. Note also that if Automatic Mastership Change (AMC) is disabled, mastership will not be returned to preferred location until AMC is enabled or mastership change is done manually.

---

### 3.3.1 Identify Affected Infrastructure Segment

If the infrastructure segment has not yet been identified, it can be identified by the infrastructure position of the faulty VMs. To do so, provide the VM instance name(s), the VM instance Universally Unique Identifier(s) (UUIDs), or both to the cloud administrator. This information can be gathered as follows:

- The **instance name** can be obtained from the cloud infrastructure.
- The **instance UUID** can be obtained either from the CUDB system, if an alarm was raised for that VM (from the alarm description), or from the cloud infrastructure.



In case of using CEE, identify the instance name, the instance UUID, or both as described below:

- ☐ The **instance name** of the VM can be obtained from the **Instances** page of the Atlas Dashboard. Its format is <tenant>\_<nameOfFailingVirtualMachine> . For example, the SC\_2\_1 VM instance name of the CUDB\_VNF01 tenant would be CUDB\_VNF01\_SC\_2\_1.
- ☐ The **instance UUID** of the VM can be obtained from the Atlas Dashboard by choosing the instance name identified above, and checking the ID value under the **Information** section of the **Overview** tab.

Once one or both of the above data is available, contact the cloud administrator, and provide them the VM instance name(s), instance UUID(s), or both.

### 3.3.2 Cloud Administration Actions to Identify Infrastructure Position

After obtaining the VM(s) instance name, instance UUID, or both (as described in [Identify Affected Infrastructure Segment](#) on page 10), cloud administrators must identify the infrastructure position. Depending on the user interface used, perform the applicable procedure described in [Identifying the VM Infrastructure Position in the Case of Using Atlas Dashboard GUI](#) on page 11 or [Identifying the VM Infrastructure Position in the Case of Using OpenStack Command Line Tools](#) on page 12.

**Note:** In the case of using a cloud solution other than CEE, refer to the solution-specific documentation for more information on how to identify the infrastructure position.

#### 3.3.2.1 Identifying the VM Infrastructure Position in the Case of Using Atlas Dashboard GUI

In the case of using the Atlas Dashboard GUI, identify the VM infrastructure position with the following steps:

##### Steps

1. Login to the Atlas Dashboard.
2. Choose the **Instances** category, and search for the instance using the provided instance name.
3. Look for the compute host name, which is located left to the name of the provided instance name in the **Host** column. Ignore the .domain.tld suffix.



### 3.3.2.2 Identifying the VM Infrastructure Position in the Case of Using OpenStack Command Line Tools

In the case of using OpenStack command line tools, perform the following steps in a Cloud Infrastructure Controller (CIC):

#### Steps

1. Execute the below command to show the details of the specific VM:  

```
nova show <instance_UUID>
```
2. Check the command output for the infrastructure position. The information is stated under the OS-EXT-SRV-ATTR:host field. Ignore the .domain.tld suffix.

### 3.3.3 Cloud Administration Actions to Identify Affected VMs

The cloud administrator can identify the affected VMs on the cloud infrastructure level from the cloud infrastructure segment. To do so, identify which VMs the infrastructure segment hosts.

In case of using CEE, follow the steps below to identify the VMs hosted by the specific infrastructure segment:

**Note:** In case of using a cloud solution other than CEE, refer to the solution-specific documentation for more information on how to identify the affected VMs.

#### Steps

1. Login to the Atlas Dashboard.
2. Choose the **Compute Environment** category, and search for the identified compute host.
3. Choose the identified compute host to see the related details.
4. Check the instances running on the selected compute host. This information can be found under the **Instances** view of the opened compute host details.
5. Provide the instance names to the requesting tenants.

## 3.4 Recovery of Multiple VMs in Parallel

This section describes how to recover multiple VMs in parallel on a virtualized CUDB node.



### 3.4.1

#### VM Groups

Because of the virtualized CUDB node infrastructure deployment on host aggregates, multiple VMs can be affected by an infrastructure activities. An affected infrastructure segment (that is, "compute host") can host either one SC, or one or several payload VMs for one CUDB node.

---

#### Do!

Because of the deployment rules described in the *Virtual Deployment Considerations* section of *CUDB Deployment Guide*, VMs of another virtualized CUDB node can be hosted on the same infrastructure segment, and can therefore also be affected. Take special care while identifying the affected VMs, and execute the recovery steps of [Execute Parallel Recovery](#) on page 14 on all affected virtualized CUDB nodes.

---

In the CUDB system, VMs are categorized into three distinct groups: SC, PLDB, and DSG. These groups can be further divided into groups of even-numbered and odd-numbered VMs. Considering the deployment of a typical virtualized CUDB node and the applied failure domains, the affected infrastructure segment is likely to host one of the following groups of VMs:

- SC\_2\_1
- SC\_2\_2
- Odd-numbered PLDB and odd-numbered DSG VMs.
- Even-numbered PLDB and even-numbered DSG VMs.

**Note:** The type of VMs in the last two groups can vary depending on the infrastructure availability during the deployment, but the redundancy over the infrastructure must be satisfied because of the applied failure domains. This means the following:

- The same infrastructure segment cannot host both VMs of the same DSG.
- The PLDB VMs must be evenly distributed. In other words, the majority of the PLDB VMs cannot be hosted by one infrastructure segment.

In case of a failure in multiple infrastructure segments (that is, more than one group of VMs of the above four groups must be recovered), consider the following rules for recovery:

- Do not execute recovery in parallel for different VM groups. Instead, recover one VM group at a time, with the priority as listed above.



- If the affected VMs belong to the same group, they can be recovered in parallel. To do so, perform the recovery in the following order, skipping any group, which has no faulty VMs:
  1. SC\_2\_1
  2. SC\_2\_2
  3. Continue with the parallel recovery of the odd-numbered PLDB and DSG VMs.
  4. Then, continue with the parallel recovery of the even-numbered PLDB and DSG VMs.

### 3.4.2 Execute Parallel Recovery

---

---

#### Do!

During VM recovery, always follow the order of groups exactly as listed in [VM Groups](#) on page 13. Deviations from the defined order can result in a major node outage.

---

---

Perform the following steps to recover multiple VMs belonging either to the same or a different VM group:

#### Steps

1. Identify all affected VMs inside the node to group them. Follow the steps of [Identify All Affected VMs](#) on page 10 to do so.

**Note:** To ensure that the traffic handling capacity is enough during the recovery procedure, the number of VMs to replace in parallel should not exceed the configured value of the `redundancyLevel` attribute of the `CudbLdapAccess` class (refer to the "Class `CudbLdapAccess`" section of [CUDB Node Configuration Data Model Description](#)). If this condition cannot be fulfilled (that is, the amount of VMs to recover is larger than the value of the `redundancyLevel` attribute), then it is recommended to perform the recovery only for the same number of VMs in parallel at a single time as the value of the `redundancyLevel` attribute. However, if recovery is performed during a low traffic period or in a maintenance window (when the degraded traffic handling capacity could still be enough), recovery may be executed in parallel for more VMs, than the value of the `redundancyLevel` attribute.
2. In case of recovering SC group(s) or PLDB group(s), force the applications to move their primary connections to another CUDB node. This applies in case primary connections are established, or if the SC or PLDB VMs are affected.



3. Execute the recovery of the VMs exactly in the order as specified in [VM Groups](#) on page 13, skipping any group which has no affected VMs.
4. If all recoveries have been finished, and more VMs were recovered than the value of the `redundancyLevel` attribute, then perform a rolling restart of the LDAP Front Ends (FEs) with the `cudbLdapFeRestart` command.

## 3.5 Prepare the VMs for Operation

This section describes how to prepare the VMs for operation after the infrastructure activities have been performed.

- Note:** In case the VM was shut down due to underperforming host as specified in [Actions in the Case of Infrastructure Activities](#) on page 8, it must be powered on before taking any further actions.
- Note:** If the VM did not join the cluster automatically after the infrastructure activity has been performed, refer to the Release Notes to check if any manual action is needed for the recovery of the network connectivity of the VMs. Some actions can involve cloud administration.

### 3.5.1 Prepare SC VM

- Note:** When recovering the SC, the SAF, LOTC Disk Replication Consistency Failed alarm might appear. At the same time, if the evacuation is taking more than 20 minutes to complete, then the SAF, LOTC Disk Replication Communication Failed alarm might also appear. These alarms can be expected during the VM recovery procedure on the SC, and should be automatically cleared when all recovery steps are executed. Refer to the corresponding alarm OPI for more information on these alarms.

If the VM to recover is an SC, then perform the following steps once the infrastructure activity has been finished:

#### Steps

1. Login to the other SC with the following command:  

```
ssh root@<CUDB_Node_OAM_VIP_Address>
```

Refer to for more information on the default root password.
2. During the first boot, the new SC also synchronizes its replicated disk storage system with another SC. This process can take up to one hour, depending on the disk storage system size and network bandwidth. Use the following command to check the synchronization status:  

```
cat /proc/drbd
```



3. On the recovered SC, restore the `crontab` jobs and their definitions, or similar tasks that are not deployed by default in CUDB or scheduled with data or software backup scripts. Edit cron configuration according to the cron configuration on the other SC.

### 3.5.2 Prepare PLDB or DSG VM

In case replication is not recovered automatically, refer to CUDB Backup and Restore Procedures.



## 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 Troubleshooting Guide
2. CUDB Backup and Restore Procedures
3. CUDB High Availability
4. CUDB Virtual Infrastructure Requirements
5. CUDB Virtual Infrastructure Requirements
6. CUDB Deployment Guide
7. CUDB Node Configuration Data Model Description
8. CUDB Users and Passwords 3/00651-HDA 104 03/10
9. CUDB Node Commands and Parameters
10. CUDB System Administrator Guide
11. SAF, LOTC Disk Replication Consistency Failed
12. SAF, LOTC Disk Replication Communication Failed
13. CUDB Glossary of Terms and Acronyms

### Other Ericsson Documents

1. CEE Troubleshooting Guideline