Oracle® Communications

Disaster Recovery

Diameter Signal Routing
User Data Repository
Cloud Disaster Recovery Guide for
Release 14.0.0.0.0

F79980-01

April 2023

ORACLE®

Diamter Signal Routing User Data Repository (DB Only) Cloud Disaster Recovery Guide for Release 14.0.0.0.0

F79980-01

TABLE OF CONTENTS

List of Figures

List of Tables

List of Procedures

Chapter 1.   Introduction

1.1 Purpose and Scope

This document describes disaster recovery procedures used during disaster scenarios of the cloud based Oracle Communications User Data Repository 14.0.0.0.0 product.

This document is a guide to describe procedures used to perform disaster recovery for Oracle Communications User Data Repository Cloud deployments. This includes recovery of partial or a complete loss of one or more Oracle Communications User Data Repository virtual servers (Primary or DR). The audience for this document includes Oracle customers as well as the following internal groups: Software Development, Quality Assurance, Product Verification, Information Development, and Consulting Services including NPx. This document provides step-by-step instructions to perform disaster recovery for Oracle Communications User Data Repository 14.0.0.0.0 Performing this procedure also involves referring to and performing procedures in existing support documents found in the reference section.

This document is intended for Customer Service team on the fielded Oracle Communications User Data Repository 14.0.0.0.0 systems.

1.2 References

[1] Oracle Communications User Data Repository 12.5.1 Disaster Recovery Guide, E83400, latest revision
[2] Oracle Communications User Data Repository 12.5.1 Cloud Installation and Configuration Guide, E95212, latest revision

1.3 Acronyms

Acronym	Meaning
BIOS	Basic Input Output System
CD	Compact Disk
DR	Disaster Recovery
FRU	Field Replaceable Unit
IMI	Internal Management Interface
ISL	Inter-Switch-Link
NE	Network Element
NOAMP	Network Operations, Administration, Maintenance and Provisioning
ISO	Contains software images
OVA	Open Virtualization Archive
NAPD	Network Architecture Planning Diagram
TAC	Technical Assistance Centers
TPD	Tekelec Platform Distribution (Linux OS)
UDR	User Data Repository
VIP	Virtual IP
VM	Virtual Machine
XMI	External Management Interface

1.4 Terminology

Table 1. Terminology

Term	Definition
Base hardware	Base hardware includes all hardware components (bare metal) and electrical wiring to allow a server to power on.
Base software	Base software includes installing the operating system for the server: Tekelec Platform Distribution (TPD).
Failed server	A failed server in disaster recovery context refers to a server that has suffered partial or complete software and/or hardware failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-install the software and/or hardware.
Enablement	The business practice of providing support services (hardware, software, documentation, etc) that enable a 3rd party entity to install, configuration, and maintain Oracle products for Oracle customers.
Software Centric	The business practice of delivering an Oracle software product, while relying on the customer to procure the requisite hardware components. Oracle provides the hardware specifications, but does not provide the hardware, and is not responsible for hardware installation, configuration, or maintenance.

1.5 How to Use this Document

When using this document, understanding the following helps to ensure that you understand the intent of the manual:

- Before beginning a procedure, completely read the instructional text (it displays immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.
- Before performing of a STEP in a procedure, completely read the left and right columns including any STEP specific WARNINGS and/or NOTES.

If a procedural STEP fails to perform successfully, stop and contact My Oracle Support.

Chapter 2.   General Description

Disaster recovery procedures falls into five basic categories. It is primarily dependent on the state of the UDR servers:

Recovery of the site from a total outage	All UDR servers failed
Recovery of one or more servers with at least one UDR server intact	1 or more UDR servers intact
Recovery of one or more servers with corrupt database	• Case 1: No Replication Channel • Case 2: Replication Channel Available

2.1 Complete Site Outage (All Servers)

This is the worst case scenario where all the servers in the site have suffered complete software failure. The servers are recovered using OVA images then restoring database backups to the active UDR servers.

NOTE: UDR servers originally installed by ISO instead of OVA are recovered using ISO.

Database backups are taken from offsite backup storage locations (assuming these were performed and stored offsite before the outage). If backup files are not available, the only option is to rebuild the network from scratch. The network data must be reconstructed from whatever sources are available, including entering all data manually.

2.2 Partial Outage with One UDR Server Intact and Second UDR Server Failed

This case assumes that at least one UDR servers intact. Other servers have failed and are recovered using OVA images. Database is restored on the UDR server and replication recovers the database of the remaining servers.

2.3 Partial Outage with Corrupt Database

Case 1

Database is corrupted, replication channel is inhibited (either manually or because of comcol upgrade barrier) and database backup is available.

Case 2

Database is corrupted but replication channel is available.

Chapter 3. Procedure Overview

This section lists the materials required to perform disaster recovery procedures and a general overview (disaster recovery strategy) of the procedure.

3.1 Required Materials

The following items are needed for disaster recovery:

1. A hardcopy of this document (E71445-01) and hardcopies of all documents in the reference list

2. Hardcopy of all NAPD performed at the initial installation and network configuration of this site. If the NAPD cannot be found, escalate this issue in My Oracle Support until the NAPD documents can be located.

3. Oracle Communications User Data Repository recent backup files: electronic backup file (preferred) or hardcopy of all Oracle Communications User Data Repository configuration and provisioning data.

4. Latest Network Element report: Electronic file or hardcopy of Network Element report.

5. The network element XML file used for the VMs initial configuration.

The software media referenced here may be acquired online from the Oracle e-Delivery service at `edelivery.oracle.com`

This document and others referenced here can be acquired online from the Oracle Document Repository at the followin URL:

http://docs.oracle.com/en/industries/communications/user-data-repository/index.html

NOTE: For all disaster recovery scenarios, we assume that the UDR database backup was performed

3.2 Disaster Recovery Strategy

Disaster recovery procedure is performed as part of a disaster recovery strategy with the basic steps listed below:

1. Evaluate failure conditions in the network and determine that normal operations cannot continue without disaster recovery procedures. This means the failure conditions in the network match one of the failure scenarios described in section Chapter 2.

2. Read and review the content in this document.

3. Gather required materials in section 3.1 **Required Materials**

4. From the failure conditions, determine the Recovery Scenario and procedure to follow using Figure 1. Determining Recovery Scenario.

5. Perform the appropriate recovery procedures (listed in section Chapter 4).

Figure 1. Determining Recovery Scenario
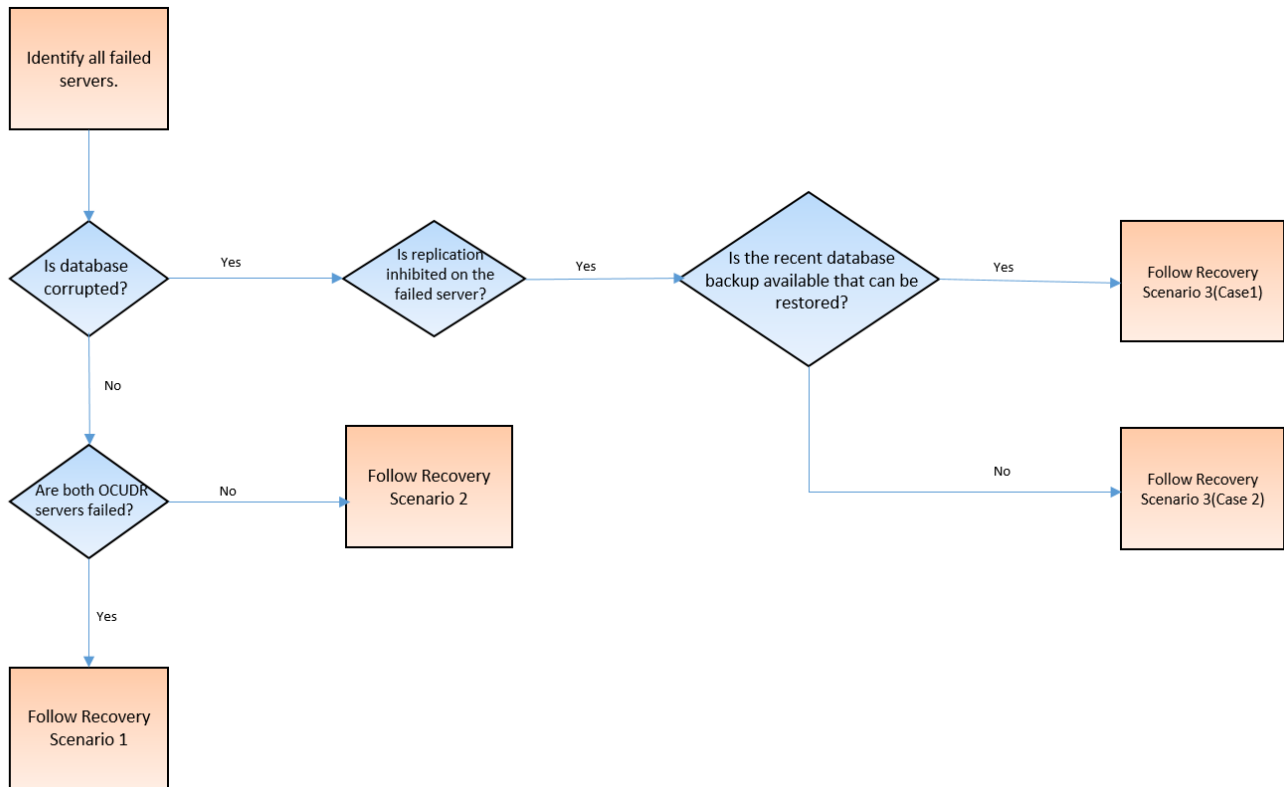
3.3 Procedure Preparation

Disaster recovery procedure is dependent on the failure conditions in the network. The severity of the failure determines the recovery scenario for the network. Use Table 2: Recovery Scenarios below to evaluate the correct recovery scenario and follow the procedures listed to restore operations.

NOTE: A failed server in disaster recovery context refers to a server that has suffered partial or complete software failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-deploy base software.

Table 2: Recovery Scenarios

Recovery Scenario	Failure Condition	Section
1	All UDR servers failed.	Section Recovery Scenario 1 (Complete Site Outage)
2	At least 1 UDR server is intact and available.	Section Recovery Scenario 2 (Partial Server Outage with One UDR Server Intact and Second UDR Server Failed)
3	• Server is intact • Database gets corrupted on the server	Section Recovery Scenario 3 (Database Recovery)
3: Case 1	• Server is intact • Database gets corrupted on the server	Section Recovery Scenario 3: Case 1

Recovery Scenario	Failure Condition	Section
	• Replication is inhibited (either manually or because of comcol upgrade barrier)	
3: Case 2	• Server is intact • Database gets corrupted on the server • Replication is occurring to the server with corrupted database	Section Recovery Scenario 3: Case 2

Chapter 4.   Disaster Recovery Procedure

Call the CAS main number at 1-800-223-1711 (toll-free in the United States), or call the Oracle Support hotline for your local country from the list at **http://www.oracle.com/us/support/contact/index.html** before performing this procedure to ensure that the proper recovery planning is performed.

Before disaster recovery, you must evaluate the outage scenario. This check ensures that the correct procedures are used for the recovery.

**** WARNING *****

**** WARNING *****

NOTE: Disaster recovery is an exercise that requires collaboration of multiple groups and is expected to be coordinated by the TAC prime. Based on TAC's assessment of Disaster, it may be necessary to deviate from the documented process.

4.1 Recovering and Restoring System Configuration

Disaster recovery requires configuring the system as it was before the disaster and restoration of operational information. There are 7 distinct procedures to select from depending on the type of recovery needed. Only one of these should be followed (not all).

4.1.1   Recovery Scenario 1 (Complete Site Outage)

For a complete server outage, UDR servers are recovered using recovery procedures for software and then performing a database restore to the active UDR server. All other servers are recovered using recovery procedures for software.

Database replication from the active UDR server recovers the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to perform the procedure. The actual detailed steps are in Procedure 1. The major activities are summarized as follows:

Recover Base software for all VMs:

- Recover the virtual machines hosting the UDRs
- Recover the active UDR server by recovering the UDRs base software
- Recover the UDR database
- Reconfigure the application

Recover the standby UDR server by recovering base software, for a Non-HA deployment this can be skipped.

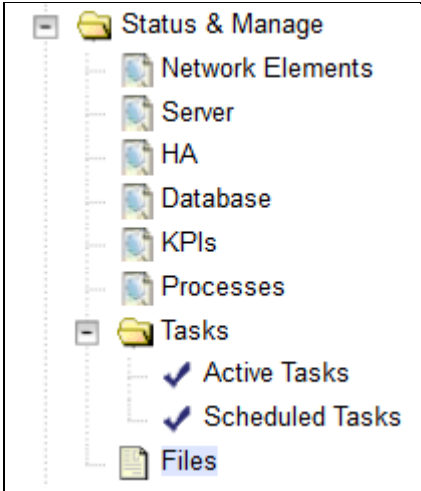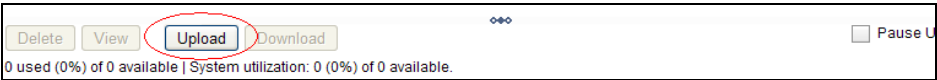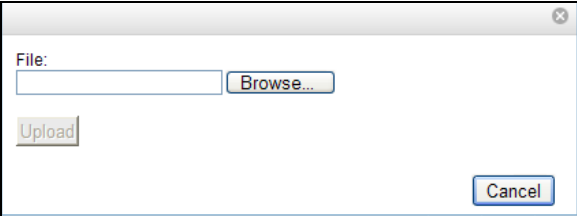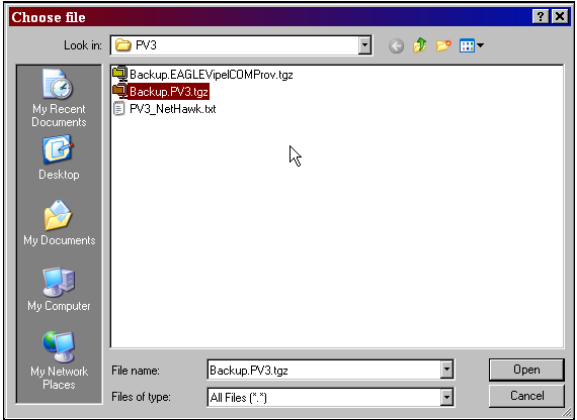- Reconfigure the Oracle Communications User Data Repository application
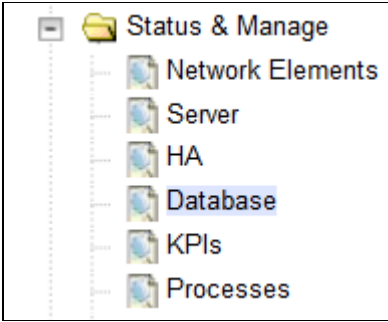
Restart process and re-enable provisioning replication

NOTE: Any other applications DR recovery actions (PCRF, etc) may occur in parallel. These actions can be worked simultaneously; doing so allows faster recovery of the complete solution.
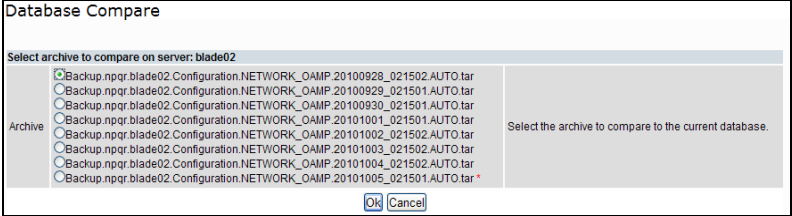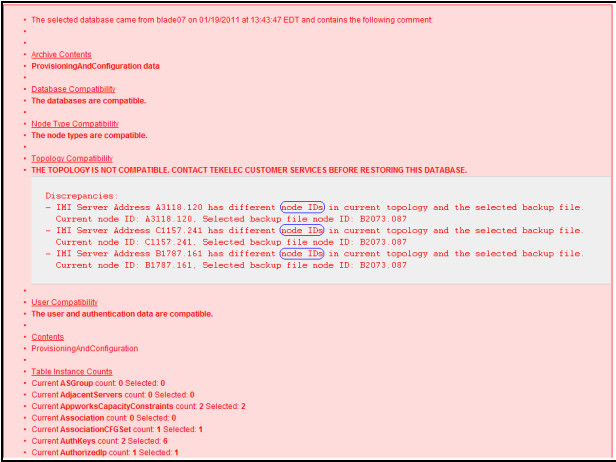
This procedure performs recovery if both UDR servers are failed

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

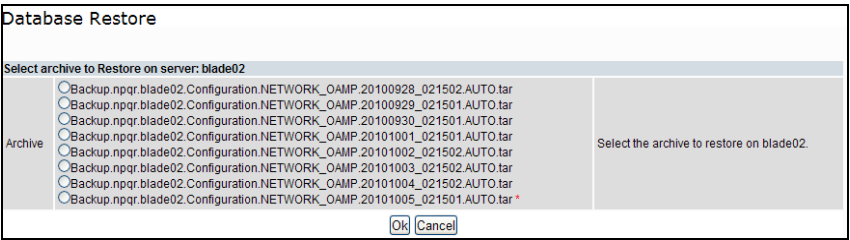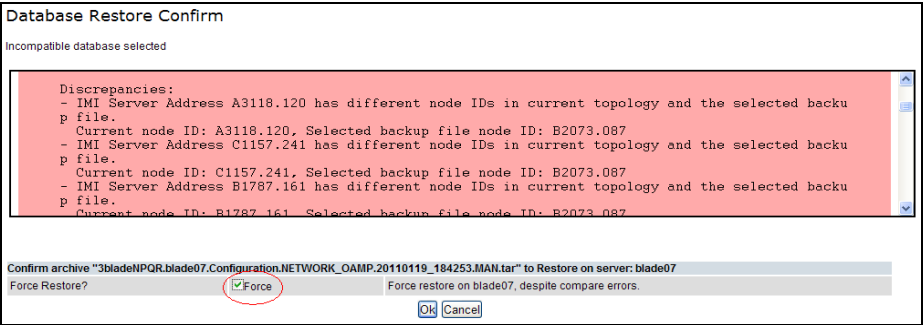If this procedure fails, contact **My Oracle Support**, and ask for assistance.

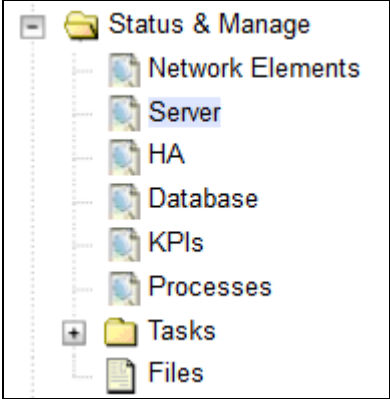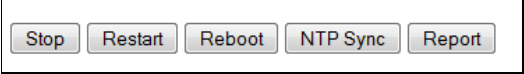**Procedure 1: Recovery Scenario 1—Complete Server Outage**

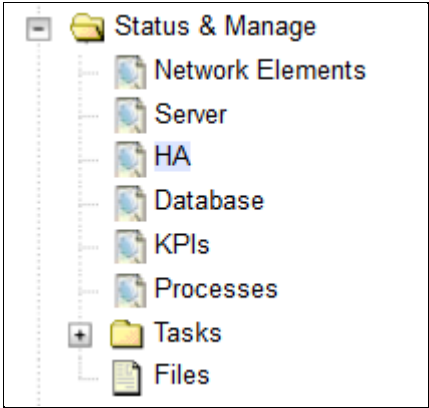| Step	Procedure	Result
1. ☐	Gather Required Materials	Gather the documents and required materials listed in Section **Required** Materials
2. ☐	Recover the failed software	Perform these procedures from reference *Oracle Communications User Data Repository 12.5.1 Cloud Installation and Configuration Guide,* E95212, *latest revision* [2]: Procedure 2: Deploy Oracle Communications User Data Repository Virtual Machines on VMware
3. ☐	Obtain latest database backup and network configuration data.	Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. From required materials list in 3.1 Required Materials; use site survey documents and Network Element report (if available), to determine network configuration data.
4. ☐	Perform UDR installation procedure for the first UDR	Configure the First UDR server by performing procedures from reference *Oracle Communications User Data Repository 12.5.1 Cloud Installation and Configuration Guide,* E95212, *latest revision* [2]: Procedure 5: Configure UDR-A Server (1st NOAMP Only) **NOTE:** If Topology or nodeId alarms are persistent after the database restore, refer to the steps below.
5. ☐	**Active UDR:** Login	Login to the UDR GUI as the guiadmin user:

Step	Procedure	Result
6. ☐	**Active UDR:** Upload the backed up database file **Note:** Here, this step is not working for uploading backup[tar] file or zip extension file due to security enhancement. Bug 31818312 - Web Inspect scan reports 'Often Misused: File Upload' As work around, just transfer file to console of NOAMP using any tool like WinSCP etc..	Browse to **Main Menu → Status & Manage → Files** Select the active UDR server. Click **Upload** and select the file NO provisioning and configuration backed up after initial installation and provisioning. Click **Browse** and locate the backup file and click **Open**. Click **Upload**. The file takes a few seconds to upload depending on the size of the backup data. The file is visible on the list of entries after the upload is complete.

Step	Procedure	Result
7. ☐	**Active UDR:** Disable provisioning	Click on **Main Menu → Status & Manage → Database** Disable Provisioning by clicking **Disable Provisioning** at the bottom of the screen. A confirmation window opens, press **OK** to disable Provisioning. The `Warning Code 002` message may appear.

Step	Procedure	Result
8. ☐	**Active UDR:** Verify the archive contents and database compatibility	Select the active UDR server and click **Compare**. The following screen is displayed; select the restored database file that was uploaded as a part of Step 13 of this procedure. Verify that the output window matches the screen below. **NOTE:** You get a database mismatch regarding the NodeIDs of the VMs. That is expected. If that is the only mismatch, proceed, otherwise stop and contact My Oracle Support. **NOTE:** Archive contents and database compatibilities must be the following: • Archive contents: Configuration data • Database compatibility: The databases are compatible. **NOTE:** The following is expected output for topology compatibility check since we are restoring from existing backed up data base to database with just one UDR: **Topology Compatibility** The topology should be compatible minus the NODEID. **NOTE:** We are trying to restore a backed up database onto an empty UDR database. This is an expected text in Topology Compatibility. If the verification is successful, click **BACK** and continue to the next step in this procedure.

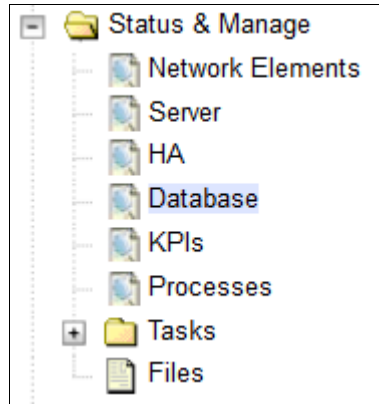| Step	Procedure	Result
9. ☐	**Active UDR:** Restore the database	Navigate to **Main Menu → Status & Manage → Database** Select the active UDR server, and click **Restore**. Select the back up provisioning and configuration file. Click **OK**. The following confirmation screen is displayed. **NOTE:** You get a database mismatch regarding the NodeIDs of the servers. That is expected. If that is the only mismatch, proceed, otherwise stop and contact My Oracle Support. Select **Force** and click **OK** to proceed with the DB restore. **NOTE:** After the restore has started, you are logged out of XMI NO GUI since the restored topology is old data.
10. ☐	**Active UDR:** Login	Establish a GUI session on the UDR server by using the VIP IP address of the UDR server. Open the web browser and enter a URL of: `http://<Primary_UDR_VIP_IP_Address>` Login as the guiadmin user:

Step	Procedure	Result
11. ☐	**Active UDR:** Monitor and confirm database restoral	Wait for approximately 5 to 10 minutes for the system to stabilize with the new topology: Monitor the Info tab for Succes. This indicates that the backup is complete and the system is stabilized. Following alarms must be ignored for UDR until all the servers are configured: Alarms with Type Column as REPL , COLL, HA (with mate UDR), DB (about Provisioning Manually Disabled) **NOTE:** Do not pay attention to alarms until all the servers in the system are completely restored. **NOTE:** The configuration and maintenance information is in the same state it was backed up during initial backup.
12. ☐	**Active UDR:** Login	Login to the recovered active UDR via SSH terminal as admusr user.
13. ☐	**Active UDR:** Restore /etc/hosts/ file of the active UDR	Perform the following command: `$ sudo AppWorks AppWorks_AppWorks updateServerAliases <UDR Host Name>`
14. ☐	**Active UDR:** Recover standby UDR **(HA Deployments Only)**	Configure the second UDR server by performing procedures from reference *Oracle Communications User Data Repository 12.5.1 Cloud Installation and Configuration Guide,* E95212, *latest revision* [2]: • Procedure 6 "Create Configuration for Remaining Servers", Step 8. • Procedure 7 "Apply Configuration for Remaining Servers" for second UDR. **NOTE:** If Topology or nodeId alarms are persistent after the database restore, refer to the steps below.
15. ☐	**Active UDR:** Restart UDR application on recovered UDR	Navigate to **Main Menu → Status & Manage → Server**, Select the recovered standby UDR server and click **Restart**.

Step	Procedure	Result
16. ☐	**Active UDR:** Set HA on standby UDR	Navigate to **Status & Manage → HA** Status & Manage — Network Elements — Server — HA — Database — KPIs — Processes + Tasks — Files Click **Edit** at the bottom of the screen. Select the standby UDR server, set it to Active. Click **OK.**
17. ☐	**Active UDR:** Login	Establish a GUI session on the UDR server by using the VIP IP address of the UDR server. Open the web browser and enter a URL of: `http://<Primary_UDR_VIP_IP_Address>` Login as the guiadmin user: **ORACLE** Oracle System Login Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: •••••• ☐ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
18. ☐	**Active UDR:** Perform key exchange between the active-UDR and recovered servers.	Establish an SSH session to the active UDR, login as admusr. Run the following command to perform a keyexchange from the active UDR to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>`

19. ☐	**Active UDR:** Fetch and store the database report for the restored data and save it	Navigate to **Main Menu → Status & Manage → Database** Select the active UDR server and click **Report** at the bottom of the page. The following screen is displayed: Click on **Save** and save the report to your local machine.

| 20. ☐ | **Active UDR:** Verify replication between servers | Login to the active UDR via SSH terminal as admusr user. |

Run the following command:

```
$ sudo irepstat -m
```

Output is generated:

```
-- Policy 0 ActStb [DbReplication] ------------------------------------
*UDR-A (A2434.104) -- Act/Act -- Act -- Groups=1 Links=2
  AA To     P0 UDR-B     Active          0   0.10 1%R 0.08%cpu 44.6/s
  AA To     P1 DR-UDR-B Active           0   0.10 1%R 0.10%cpu 38.6/s
UDR-B (A2434.105) -- Act/Stb -- Stb -- Groups=1 Links=1
  AA From  P0 *UDR-A   Active           0   0.10 ^0.07%cpu 35.7/s
DR-UDR-A (A3629.172) -- Stb/Stb -- InSvc -- Groups=1 Links=1
  AA From  P0 DR-UDR-B Active           0   0.10 ^0.07%cpu 49.9/s
DR-UDR-B (A3629.173) -- Stb/Act -- InSvc -- Groups=1 Links=2
  AA To     P0 DR-UDR-A Active          0   0.10 1%R 0.08%cpu 31.3/s
  AA From  P1 *UDR-A   Active           0   0.10 ^0.06%cpu 47.1/s
```

| 21. ☐ | **Active UDR:** Verify the database states | Click on **Main Menu → Status and Manager → Database** |

Verify that the OAM Max HA Role is either active or standby for UDR, and that the status is Normal.

Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
Site2_NE_DR_NO	DR-OCUDR-B	Network OAM&P	Spare	N/A	Normal	18387	Normal	NotApplicable	Allowed	NotApplicable
Site1_NE_NO	OCUDR-A	Network OAM&P	Active	N/A	Normal	18387	Normal	NotApplicable	Allowed	NotApplicable
Site1_NE_NO	OCUDR-B	Network OAM&P	Standby	N/A	Normal	18387	Normal	NotApplicable	Allowed	NotApplicable
Site2_NE_DR_NO	DR-OCUDR-A	Network OAM&P	Spare	N/A	Normal	18387	Normal	NotApplicable	Allowed	NotApplicable

22. ☐	**Active UDR:** Verify the HA status	Click on **Main Menu → Status and Manage → HA**

Select the row for all of the servers

Verify that the HA Role is either Active or Standby.

Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role	Active VIPs
OCUDR-A	Active	N/A	Active	OCUDR-B	Site1_NE_NO	Network OAM&P	10.10.1.121
OCUDR-B	Standby	N/A	Active	OCUDR-A	Site1_NE_NO	Network OAM&P	
DR-OCUDR-A	Spare	N/A	Active	DR-OCUDR-B	Site2_NE_DR_NO	Network OAM&P	
DR-OCUDR-B	Spare	N/A	Active	DR-OCUDR-A	Site2_NE_DR_NO	Network OAM&P	10.10.1.28

23. ☐	**Active UDR:** Enable provisioning	Click on **Main Menu → Status & Manage → Database**

Enable provisioning by clicking **Enable Provisioning** at the bottom of the screen.

A confirmation window displays, click **OK** to enable provisioning.

Enable provisioning.
Are you sure?

OK   Cancel

Step	Procedure	Result

24. ☐	**Active UDR:** Examine all alarms	Login to the UDR VIP if not logged in. Navigate to **Main Menu → Alarms & Events → View Active**
		
		 Alarms & Events
		    View Active
		    View History
		    View Trap Log
		
		 Examine all active alarms and refer to the on-line help on how to address them.
		
		 If needed contact My Oracle Support.

25. ☐	Restore GUI usernames and passwords	If applicable, perform the steps in Chapter 5 to recover the user and group information restored.
26. ☐	Backup and archive all the databases from the recovered system	Perform Appendix A Oracle Communications User Data Repository Database Backup to back up the configuration databases.
	THIS PROCEDURE HAS BEEN COMPLETED	

4.1.2 Recovery Scenario 2 (Partial Server Outage with One UDR Server Intact and Second UDR Server Failed)

For a partial server outage with an UDR server intact and available; second UDR server is recovered using recovery procedures for software. Second server is recovered using recovery procedures for software. Database replication from the active UDR server recovers the database on second server. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to perform the procedure. The actual steps are in Procedure 2. The major activities are summarized as follows:

Recover Standby UDR server (if needed) by recovering software and the database.
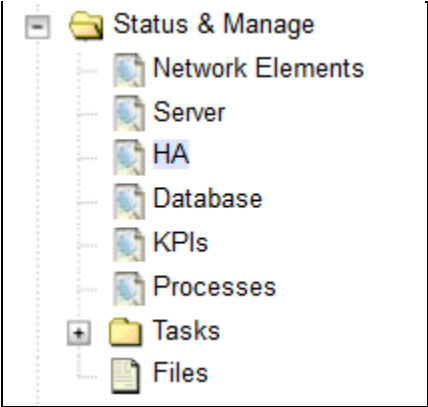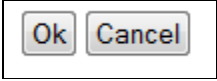
- Recover the software.
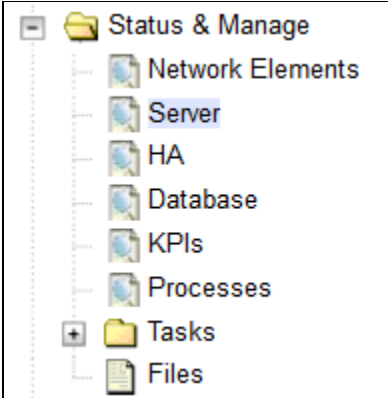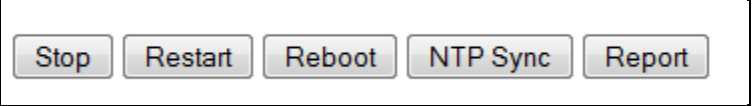
This procedure performs recovery if at least 1 UDR server is available but second server in a site have failed. This includes any UDR server .

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support, and ask for assistance.

Procedure 2: Recovery Scenario 2—Partial Outage One UDR Intact
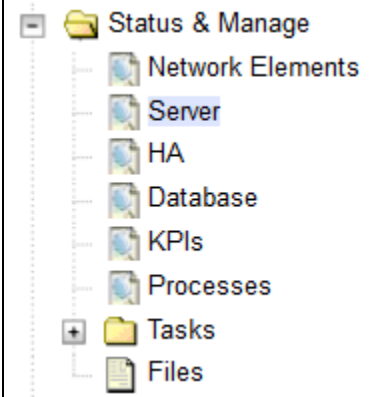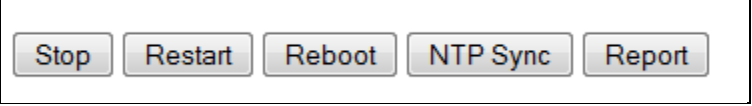
Step	Procedure	Result
1. ☐	Gather required materials	Gather the documents and required materials listed in **Required** Materials

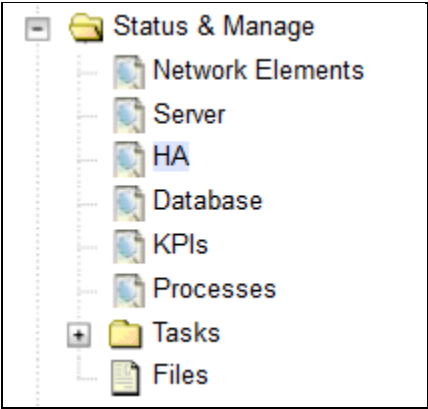| Step	Procedure	Result
2. ☐	**Active UDR:** Login	Establish a GUI session on the UDR server by using the VIP IP address of the UDR server. Open the web browser and enter a URL of: `http://<Primary_UDR_VIP_IP_Address>` Login as the guiadmin user:
3. ☐	**Active UDR:** Set failed server to standby	1. Navigate to **Main Menu → Status & Manage → HA** 2. Select **Edit** 3. Set the Max Allowed HA Role to **Standby** for the failed server. 4. Click **Ok**
4. ☐	**Create VMs** Recover the failed software	Perform the following procedures from reference *Oracle Communications User Data Repository 12.5.1 Cloud Installation and Configuration Guide,* E95212, *latest revision* [2]: Procedure 2: Deploy Oracle Communications User Data Repository Virtual Machines on VMware

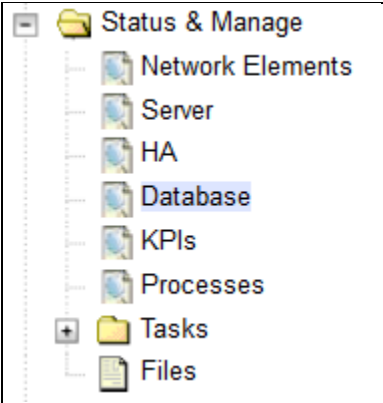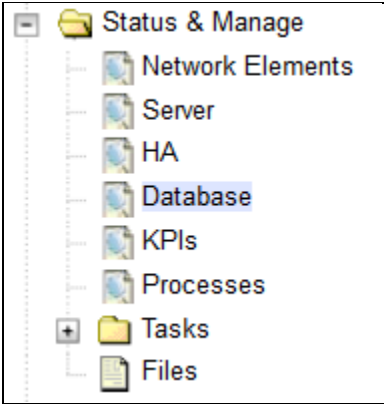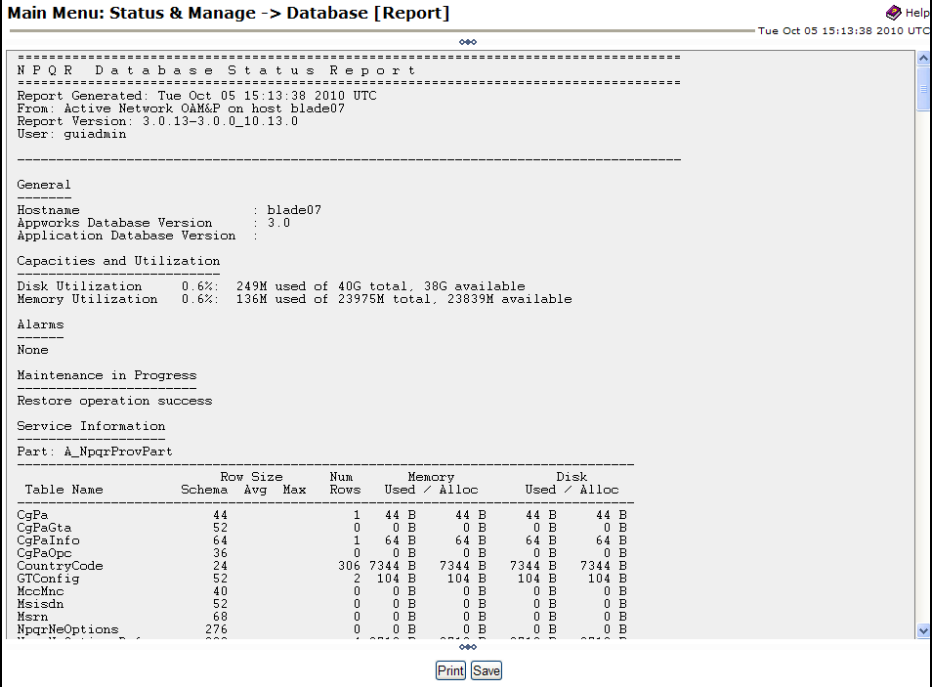| Step	Procedure	Result
5. ☐	**Active UDR:** Login	Establish a GUI session on the UDR server by using the VIP IP address of the UDR server. Open the web browser and enter a URL of: `http://<Primary_UDR_VIP_IP_Address>` Login as the guiadmin user:
6. ☐	**Active UDR:** Recover standby UDR	Configure the standby UDR server by performing procedures from reference *Oracle Communications User Data Repository 12.5.1 Cloud Installation and Configuration Guide,* E95212, *latest revision* [2]: • Procedure 6 "Create Configuration for Remaining Servers", Step 8. • Procedure 7 "Apply Configuration for Remaining Servers" for UDR. **NOTE:** If Topology or nodeId alarms are persistent after the database restore, refer to the steps below.
7. ☐	**Active UDR:** Restart UDR application on recovered UDR	Navigate to **Main Menu → Status & Manage → Serve**r, Select the recovered standby UDR server and click **Restart**.

Step	Procedure	Result
8. ☐	**Active UDR:** Set HA on recovered UDR	Navigate to **Status & Manage → HA** Click **Edit** at the bottom of the screen Select the standby UDR server, set it to Active Click **OK**
9. ☐	**Recovered Servers:** Login	Establish an SSH to the recovered XMI address for the server

| 10. ☐ | **Recovered Servers:** Sync NTP | 1. Perform the following to retrieve the remote NTP server:

```
$ sudo chronyc -N 'sources -a -v'
```
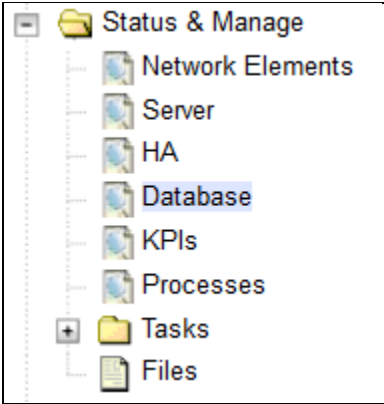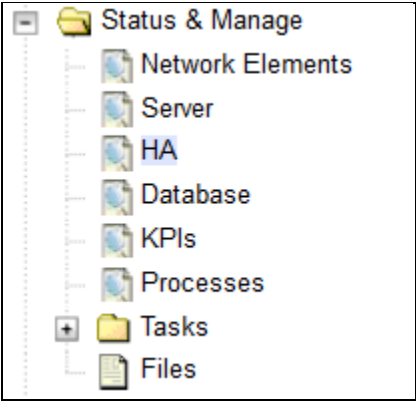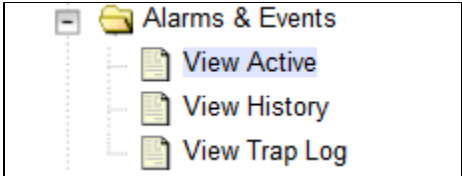
Example output:

```
[root@NO-A admusr]# chronyc -N 'sources -a -v'


  .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
 / .- Source state '*' = current best, '+' = combined, '-' = not
combined,
| /              'x' = may be in error, '~' = too variable, '?' =
unusable.
||                                                  .- xxxx [ yyyy ] +/-
zzzz
||      Reachability register (octal) -.          |  xxxx = adjusted
offset,
||      Log2(Polling interval) --.      |          |  yyyy = measured
offset,
||                                \      |          |  zzzz = estimated
error.
||                                |      |          \
MS Name/IP address          Stratum Poll Reach LastRx Last sample
===============================================================================
======
^* 10.250.32.10               3    8    377    113    +49us[  +87us] +/-
67ms
=? ntppeerA                   0    6    0      -      +0ns[   +0ns] +/-
0ns
=? ntppeerB                   0    6    0      -      +0ns[   +0ns] +/-
0ns
[root@NO-A admusr]#
```

2. Stop ntpd service:

```
$ sudo systemctl stop chronyd.service
```

3. Sync the date to the ntp remote server:

```
$ sudo vi etc/chrony.conf
Update NTP source as below

# Specify time sources.
server <NTP Source> iburst
peer ntppeerA iburst
peer ntppeerB iburst

Example:
# Specify time sources.
server 10.250.32.10 iburst
peer ntppeerA iburst
peer ntppeerB iburst
```

NOTE: The remote server is the one gathered in sub step 1.

4. Start the ntp service:

```
$ sudo systemctl start chronyd.service
```
|

Step	Procedure	Result
		5. Verify NTP: ```$ sudo chronyc tracking``` Example: [root@NO-A admusr]# chronyc tracking Reference ID : 0AFA200A (10.250.32.10) Stratum : 4 Ref time (UTC) : Wed Mar 29 10:32:31 2023 System time : 0.000004655 seconds fast of NTP time Last offset : -0.000008532 seconds RMS offset : 0.000038986 seconds Frequency : 91.246 ppm slow Residual freq : -0.001 ppm Skew : 0.276 ppm Root delay : 0.033020783 seconds Root dispersion : 0.048987720 seconds Update interval : 64.7 seconds Leap status : Normal [root@NO-A admusr]#
11. ☐	**Active UDR:** Restart UDR application on recovered servers *(HA deployments only)*	**NOTE:** For Non-HA sites SKIP this step Navigate to **Main Menu → Status & Manage → Server** Select the recovered server and click **Restart**.

Step	Procedure	Result
12. ☐	**Active UDR:** Start replication on all servers	Un-Inhibit (start) replication to the all C-Level (MP) servers Navigate to **Status & Manage → Database** If the Repl Status is set to Inhibited, click **Allow Replication** in this order: • Active UDRP server • Standby UDRP server Verify that replication on all servers is allowed. Select each server and verify that the middle button shows Inhibit Replication, and not Allow Replication.
13. ☐	**Active UDR:** Perform key exchange between the active-UDR and recovered servers.	Establish an SSH session to the Active UDR, login as admusr. Perform the following command to perform a keyexchange from the active UDR to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>` **NOTE:** If an export server is configured, perform this step.

Step	Procedure	Result
14. ☐	**Active UDR:** Fetch and store the database report for the restored data and save it	Navigate to **Main Menu → Status & Manage → Database** Select the active UDR server and click **Report** at the bottom of the page. The following screen is displayed: Click on **Save** and save the report to your local machine.

Step	Procedure	Result

15. ☐	**Active UDR:** Verify replication between servers.	Login to the active UDR via SSH terminal as admusr user. Perform the following command:
		
		 `$ sudo irepstat -m`
		
		 Output like below is generated:
		
		 ``` -- Policy 0 ActStb [DbReplication] ------------------------------------ *UDR-A (A2434.104) -- Act/Act -- Act -- Groups=1 Links=2 AA To P0 UDR-B Active 0 0.10 1%R 0.06%cpu 65.4/s AA To P1 DR-UDR-B Active 0 0.10 1%R 0.08%cpu 73.0/s UDR-B (A2434.105) -- Act/Stb -- Stb -- Groups=1 Links=1 AA From P0 *UDR-A Active 0 0.14 ^0.07%cpu 66.0/s DR-UDR-A (A3629.172) -- Stb/Stb -- InSvc -- Groups=1 Links=1 AA From P0 DR-UDR-B Active 0 0.10 ^0.07%cpu 83.5/s DR-UDR-B (A3629.173) -- Stb/Act -- InSvc -- Groups=1 Links=2 AA To P0 DR-UDR-A Active 0 0.10 1%R 0.08%cpu 72.8/s AA From P1 *UDR-A Active 0 0.10 ^0.06%cpu 73.2/s ```

16. ☐	**Active UDR:** Verify the database states	Click on **Main Menu → Status and Manager → Database** Verify that the OAM Max HA Role is either active or standby for UDR and that the status is Normal.

Database status table:

Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
Site2_NE_DR_NO	DR-OCUDR-B	Network OAM&P	Spare	N/A	Normal	18387	Normal	NotApplicable	Allowed	NotApplicable
Site1_NE_NO	OCUDR-A	Network OAM&P	Active	N/A	Normal	18387	Normal	NotApplicable	Allowed	NotApplicable
Site1_NE_NO	OCUDR-B	Network OAM&P	Standby	N/A	Normal	18387	Normal	NotApplicable	Allowed	NotApplicable
Site2_NE_DR_NO	DR-OCUDR-A	Network OAM&P	Spare	N/A	Normal	18387	Normal	NotApplicable	Allowed	NotApplicable

Step	Procedure	Result
17. ☐	**Active UDR:** Verify the HA status	Click on **Main Menu → Status and Manage → HA** Select the row for all of the servers Verify that the HA Role is either active or standby.
18. ☐	**Active UDR:** Examine all alarms	Login to the UDR VIP if not logged in. Navigate to **Main Menu → Alarms & Events → View Active** Examine all active alarms and refer to the on-line help on how to address them. If needed contact My Oracle Support.
19. ☐	Backup and archive all the databases from the recovered system	Perform Appendix A Oracle Communications User Data Repository Database Backup to back up the configuration database.
	THIS PROCEDURE HAS BEEN COMPLETED	

For step 17, the HA status table:

Hostname	OAM Max HA Role	Application Max HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role	Active VIPs
NO2	Active	OOS	Active	NO1	NO_10303	Network OAM&P	10.240.70.132
SO1	Standby	OOS	Active	SO2	SO_10303	System OAM	
SO2	Active	OOS	Active	SO1	SO_10303	System OAM	10.240.70.133
MP1	Standby	Active	Active	MP2	SO_10303	MP	
MP2	Active	Active	Active	MP1	SO_10303	MP	
IPFE	Active	OOS	Active		SO_10303	MP	

1.1.1 Recovery Scenario 3 (Database Recovery)

The following sections deal with recovering from database corruption, whether a backup is present or not.

1.1.1.1 Recovery Scenario 3: Case 1
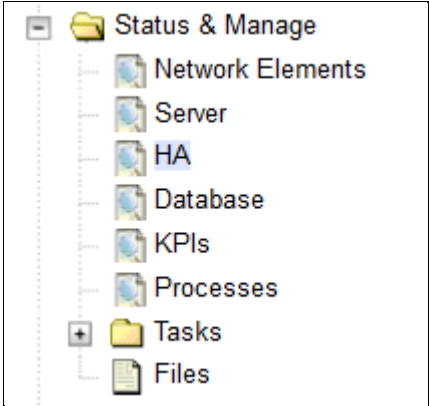
For a partial outage with

- Server having a corrupted database
- Replication channel from parent is inhibited because of upgrade activity or
- Server is in a different release then that of its active parent because of upgrade activity.
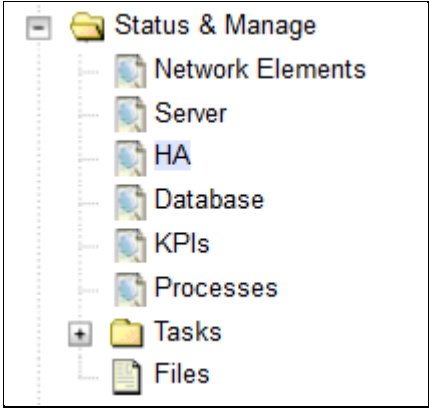
- Verify that the Server Runtime backup files, performed at the start of the upgrade, are present in `/var/TKLC/db/filemgmt` area in the following format

    o Backup.UDR.HPC02-NO2.FullDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2
    o Backup.UDR.HPC02-NO2.FullRunEnv.NETWORK_OAMP.20140524_223507.UPG.tar.bz2

NOTE: During recovery, the corrupted database is replaced by the sever runtime backup. Any configuration performed after taking the backup is not visible post recovery.

This procedure performs recovery if database is corrupted in the system

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact **My Oracle Support**, and ask for assistance.

Procedure 3: Recovery Scenario 3 (Case 1)—Database Recovery Backup Present

Step	Procedure	Result
1. ☐	**Active UDR:** Set failed servers to standby	Navigate to **Main Menu → Status & Manage → HA** Select **Edit** Set the Max Allowed HA Role to **Standby** for the failed servers. Click **Ok**
2. ☐	**Server with DB Corruption:** Login	Establish an SSH session to the server in question. Login as admusr user.
3. ☐	**Server with DB Corruption:** Change runlevel to 3	Run the following command to bring the system to runlevel 3. `$ sudo init 3`
4. ☐	**Server with DB Corruption:** Recover system	Run the following command and follow the instructions appearing the console prompt `$ sudo /usr/TKLC/appworks/sbin/backout_restore`

Step	Procedure	Result
5. ☐	**Server with DB Corruption:** Change runlevel to 4	Perform the following command to bring the system back to runlevel 4. `$ sudo init 4`
6. ☐	**Server with DB Corruption:** Verify the server	Perform the following command to verify if the processes are up and running `$ sudo pm.getprocs`
7. ☐	**Active UDR:** Set failed servers to active	Navigate to **Status & Manage → HA** Click **Edit** at the bottom of the screen For each failed server whose Max Allowed HA Role is set to Standby, set it to Active Click **OK**
8. ☐	Backup and archive all the databases from the recovered system	Perform Appendix A Oracle Communications User Data Repository Database Backup to back up the configuration databases:
THIS PROCEDURE HAS BEEN COMPLETED		

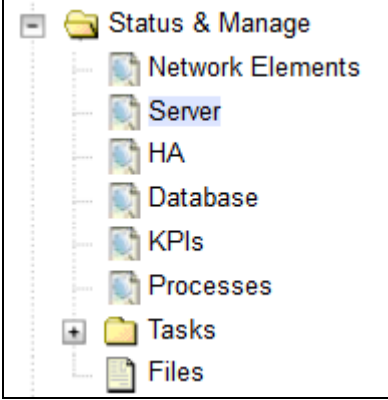### 4.1.2.1   Recovery Scenario 3: Case 2

For a partial outage with

- Server having a corrupted database
- Replication channel is available or
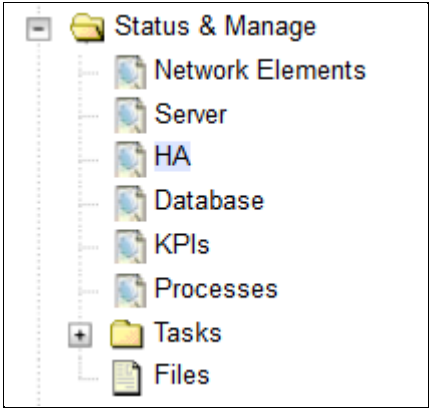- Server has the same release as that of its active parent

This procedure performs recovery if database got corrupted in the system and system is in the state to get replicated

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support, and ask for assistance.

Procedure 4: Recovery Scenario 3 (Case 2)—Database Recovery Backup Not Present

Step	Procedure	Result
1. ☐	**Active UDR:** Set failed servers to standby	Navigate to **Main Menu → Status & Manage → HA** Click **Edit** Set the Max Allowed HA Role to Standby for the failed servers. Click **Ok**
2. ☐	**Server with DB Corruption:** Login	Establish an SSH session to the server in question. Login as admusr user.

3. ☐	**Server with DB Corruption:** Take server out of service	Run the following command to take the server out of service.
		
		```$ sudo bash –l```
		```$ sudo prod.clobber```

Step	Procedure	Result

4. ☐	**Server with DB Corruption:** Take server to DbUp state and start the aplication	Perform the following commands to take the server to Dbup and start the Oracle Communications User Data Repository application:
		
		```$ sudo bash -l```
		```$ sudo prod.start```

5. ☐	**Server with DB Corruption:** Verify the server state	Perform the following commands to verify the processes are up and running:
		
		```$ sudo pm.getprocs```
		
		Perform the following command to verify if replication channels are up and running:
		
		```$ sudo irepstat```
		
		Perform the following command to verify if merging channels are up and running:
		
		```$ sudo inetmstat```

6. ☐	**Active UDR:** Restart UDR application	Navigate to **Main Menu → Status & Manage → Server** Select each recovered server and click **Restart**.

Step	Procedure	Result
7. ☐	**Active UDR:** Set failed servers to active	Navigate to **Status & Manage → HA** Click **Edit** at the bottom of the screen For each failed server whose Max Allowed HA Role is set to Standby, set it to Active Press **OK**
8. ☐	Backup and archive all the databases from the recovered system	Perform Appendix A Oracle Communications User Data Repository Database Backup to back up the configuration databases.
		THIS PROCEDURE HAS BEEN COMPLETED

Chapter 5.   Resolving User Credential Issues after Database Restore

User incompatibilities may introduce security holes or prevent access to the network by administrators. User incompatibilities are not dangerous to the database, however. Review each user difference carefully to ensure that the restoration does not impact security or accessibility.

5.1 Keeping a Restored User (Resetting User Password)

User accounts kept across a restore operation have their passwords reset. This procedure guides you through that process.
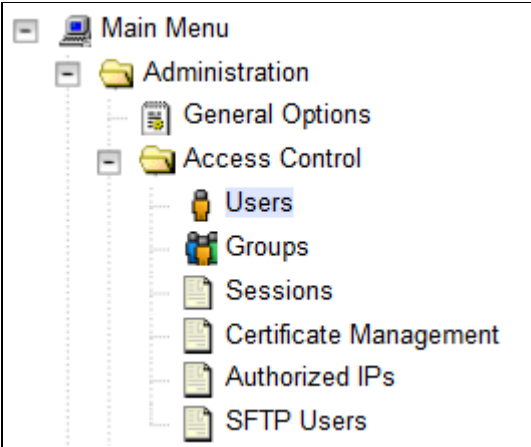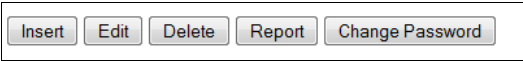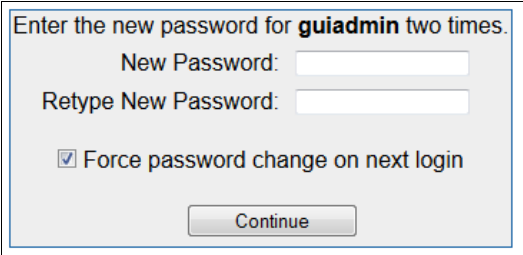
Perform this procedure to keep users that are restored by system restoration.

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact **My Oracle Support**, and ask for assistance.

Procedure 5: Keep Restored User (Resetting User Password)

Step	Procedure	Result
1. ☐	**Before Restoration:** Notify Affected Users (Before Restoration)	Contact each user that is affected before the restoration and notify them that you are resetting their password during this maintenance operation.
2. ☐	**After Restoration:** Login to the active UDR (before restoration)	Establish a GUI session on the UDR server by using the VIP IP address of the UDR server. Open the web browser and enter a URL of: `http://<Primary_UDR_VIP_IP_Address>` Login as the guiadmin user:

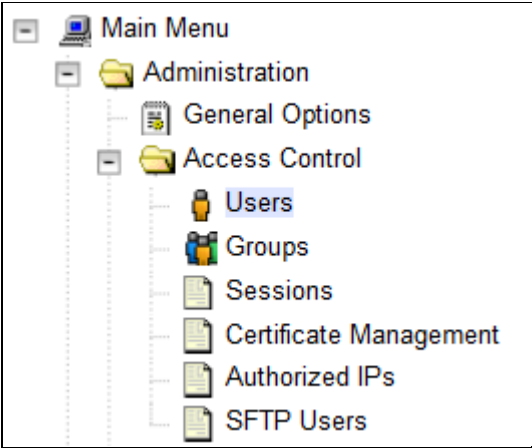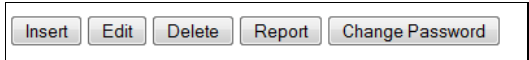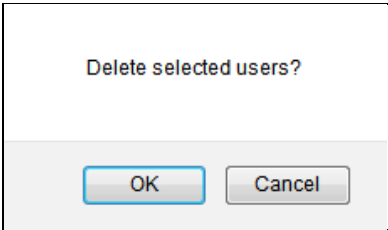| Step	Procedure	Result
3. ☐	**After Restoration:** Reset User Passwords	Navigate to **Administration → Access Control → Users** Select the user Click **Change Password** Enter a new password Click **Continue**
		THIS PROCEDURE HAS BEEN COMPLETED

5.2 Removing a Restored User

Perform this procedure to remove users that are restored by system restoration

Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact **My Oracle Support**, and ask for assistance.

Procedure 6: Remove the Restored User

Step	Procedure	Result
4. ☐	**After Restoration:** Login to the active UDR	Establish a GUI session on the UDR server by using the VIP IP address of the UDR server. Open the web browser and enter a URL of: `http://<Primary_UDR_VIP_IP_Address>` Login as the guiadmin user:

Step	Procedure	Result
5. ☐	**After Restoration:** Delete User	Navigate to **Administration → Access Control → Users** Select the user Click **Delete** Click **OK** to confirm.
	THIS PROCEDURE HAS BEEN COMPLETED	

5.3 Restoring a Modified User

These users have had a password change before the creation of the backup and archive file. They are reverted by system restoration of that file.

The password for testuse differs between the selected backup file and the current database.

Before Restoration:

Verify that you have access to a user with administrator permissions that is not affected.

Contact each user that is affected and notify them that you are resetting their password during this maintenance operation.

After Restoration:

Log in and reset the passwords for all users in this category. See the steps in Section 5.1 (Keeping a Restored User) for resetting passwords for a user.

5.4 Restoring an Archive that Does Not Contain a Current User

These users have been created after the backup operation. They are deleted by a system restoration of that file.

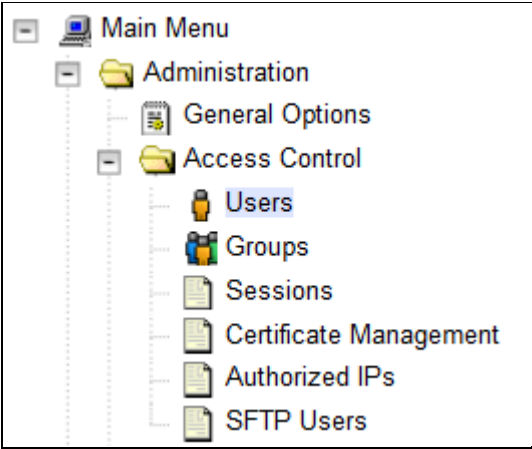If the users are not needed, do not perform any additional steps. The user is permanently removed.

Perform this procedure to remove users that are restored by system restoration
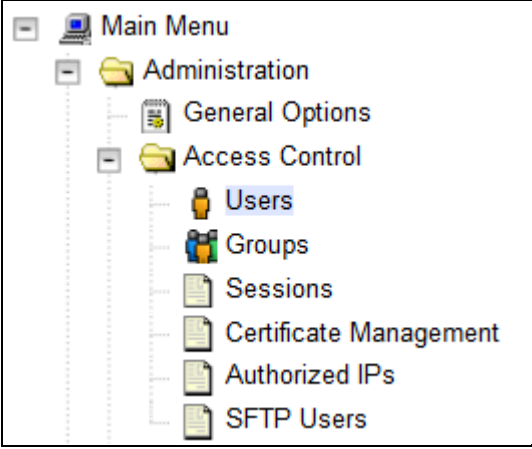
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

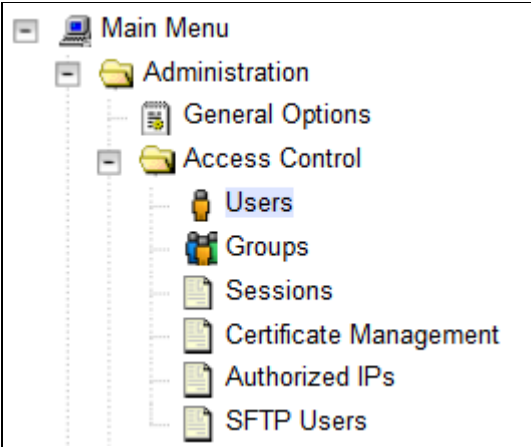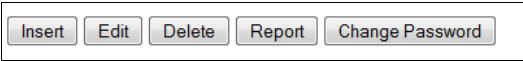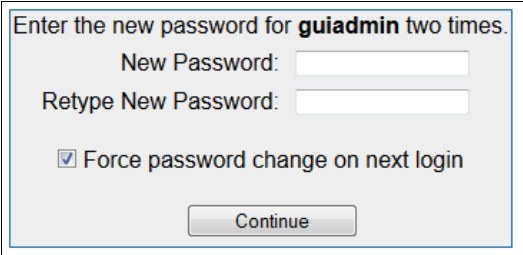If this procedure fails, contact **My Oracle Support**, and ask for assistance.

Procedure 7: Restoring an Archive that does not Contain a Current User

Step	Procedure	Result
1. ☐	**Before Restoration:** Notify Affected Users (Before Restoration)	Contact each user that is affected before the restoration and notify them that you are resetting their password during this maintenance operation.
2. ☐	**Before Restoration:** Login to the active UDR (before restoration)	Establish a GUI session on the UDR server by using the VIP IP address of the UDR server. Open the web browser and enter a URL of: `http://<Primary_UDR_VIP_IP_Address>` Login as the guiadmin user:

Step	Procedure	Result
3. ☐	**Before Restoration:** Record user settings *(Before Restoration)*	Navigate to **Administration → Access Control → Users** Under each affected user, record the following: • Username • Account status • Remote auth • Local auth • Concurrent logins allowed • Inactivity limit • Comment • Groups
4. ☐	**After Restoration:** Login	Establish a GUI session on the UDR server by using the VIP IP address of the UDR server. Open the web browser and enter a URL of: `http://<Primary_UDR_VIP_IP_Address>` Login as the guiadmin user:

5.	☐	**After Restoration:** Recreate affected user	Navigate to **Administration → Access Control → Users** Click **Insert** Recreate the user using the data collected in Step 3.

Step	Procedure	Result
		  Click **Ok**
6. ☐	**After Restoration:** Repeat for Additional Users	Repeat Step 5 to recreate additional users.

Step	Procedure	Result
7. ☐	**After Restoration:** Reset the Passwords	Navigate to **Administration → Access Control → Users** Select the user Click **Change Password** Enter a new password Click **Continue**
		THIS PROCEDURE HAS BEEN COMPLETED

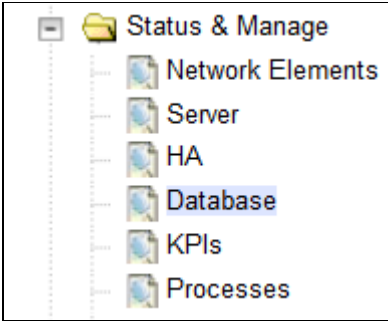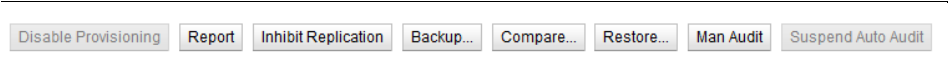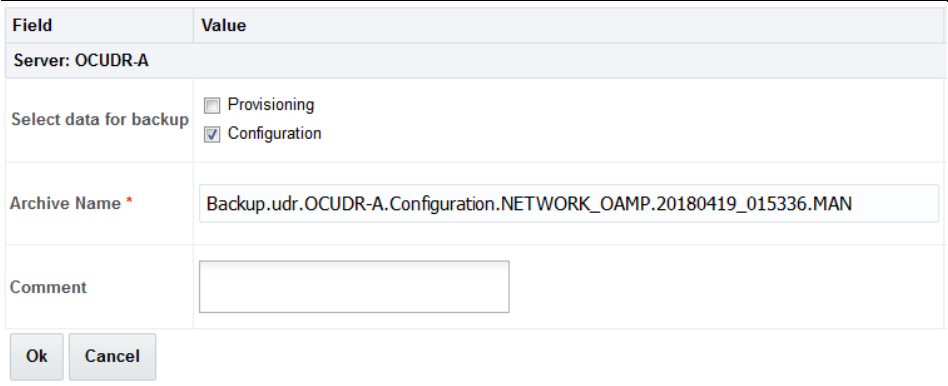## Appendix A. Oracle Communications User Data Repository Database Backup

The intent of this procedure is to back up the provision and configuration information from an UDR server after the disaster recovery is complete
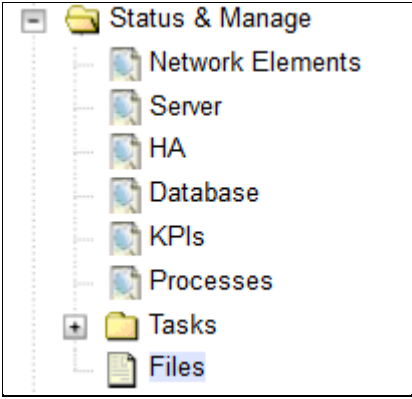
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.
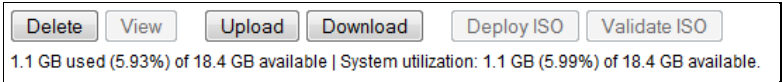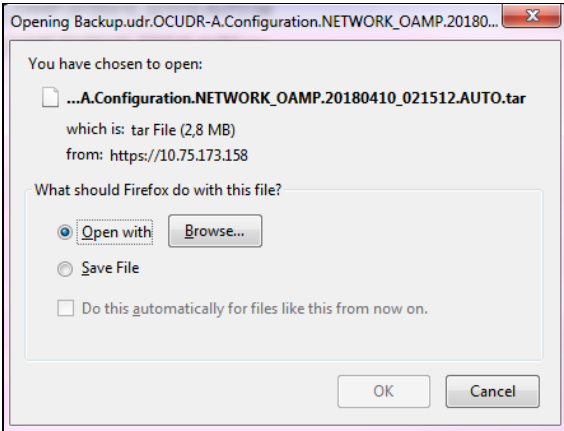
If this procedure fails, contact **My Oracle Support**, and ask for assistance.

Procedure 8: Restoring an Archive that does not Contain a Current User

Step	Procedure	Result
1. ☐	**Active UDR:** Login	Establish a GUI session on the active UDR server by using the VIP IP address of the UDR server. Open the web browser and enter a URL of: `http://<Primary_UDR_VIP_IP_Address>` Login as the guiadmin user:

Step	Procedure	Result
2. ☐	**Active UDR:** Backup configuration data for the system	Navigate to **Main Menu → Status & Manage → Database** Select the active UDR server and click **Backup**. Make sure that configuration is selected. Enter a filename for the backup and click **OK**

Step	Procedure	Result
3. ☐	**Active UDR:** Verify the backup file existence.	Navigate to **Main Menu → Status & Manage → Files** Select the active UDR tab. The files on this server are displayed. Verify the existence of the backup file.

Step	Procedure	Result
4. x	**Active UDR:** Download the file to a local machine.	From the previous step, select the backup file. Click **Download** Click **OK** to confirm the download.
5. ☐	Upload the Image to Secure Location	Transfer the backed up image saved in Step 4 to a secure location where the server backup files are fetched during a system disaster recovery.
		THIS PROCEDURE HAS BEEN COMPLETED

Appendix B. My Oracle Support

My Oracle Support (**https://support.oracle.com**) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at **http://www.oracle.com/us/support/contact/index.html**. When calling, make the selections in sequence on the Support telephone menu:

6. Select **2** for New Service Request

7. Select **3** for Hardware, Networking and Solaris Operating system support

8. Select one of the following options:

    o   For Technical issues such as creating a Service Request (SR), Select **1**
    o   For Non-technical issues such as registration or assistance with My Oracle Support, Select **2**

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Appendix C. Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, **http://docs.oracle.com**. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at **http://www.adobe.com**.

1. Access the Oracle Help Center site at **http://docs.oracle.com**

2. Click **Industries**.

3. Under the Oracle Communications subheading, click **Oracle Communications documentation**.

4. The Communications Documentation page displays. Most products covered by these documentation sets appear under the headings Network Session Delivery and Control Infrastructure or Platforms.

5. Click on your Product and then the Release Number.

6. A list of the documentation set for the selected product and release displays.

7. To download a file to your location, right-click **PDF**, select **Save target as** (or similar command based on your browser), and save to a local folder.