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

CAUTION: Open an Service Request on My Oracle Support confer with Oracle before performing disaster recovery procedure

Before recovering any system, access My Oracle Support (<u>https://support.oracle.com</u>) and review any My Oracle Support Alerts that relate to this procedure.

My Oracle Support (<u>https://support.oracle.com</u>) 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.

See more information on My Oracle Support, see Appendix B

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

F79980-01

Copyright © 2016, 2019, 2021, 2022, 2023 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION	5
1.1 Purpose and Scope	5
1.2 References	5
1.3 Acronyms	5
1.4 Terminology	6
1.5 How to Use this Document	6
CHAPTER 2. GENERAL DESCRIPTION	7
2.1 Complete Site Outage (All Servers)	7
2.2 Partial Outage with One UDR Server Intact and Second UDR Server Failed	7
2.3 Partial Outage with Corrupt Database	7
CHAPTER 3. PROCEDURE OVERVIEW	8
3.1 Required Materials	8
3.2 Disaster Recovery Strategy	8
3.3 Procedure Preparation	9
CHAPTER 4. DISASTER RECOVERY PROCEDURE	11
4.1 Recovering and Restoring System Configuration	11
4.1.1 Recovery Scenario 1 (Complete Site Outage)	. 11
4.1.2 Recovery Scenario 2 (Partial Server Outage with One UDR Server Intact and Second UDR Server Failed)	.22
1.1.1 Recovery Scenario 3 (Database Recovery)	.31
CHAPTER 5. RESOLVING USER CREDENTIAL ISSUES AFTER DATABASE RESTORE	37
5.1 Keeping a Restored User (Resetting User Password)	37
5.2 Removing a Restored User	39
5.3 Restoring a Modified User	40
5.4 Restoring an Archive that Does Not Contain a Current User	41
APPENDIX A. ORACLE COMMUNICATIONS USER DATA REPOSITORY DATABASE BACKUP	46
APPENDIX B. MY ORACLE SUPPORT	50
APPENDIX C. LOCATE PRODUCT DOCUMENTATION ON THE ORACLE HELP CENTER SITE 51	

Oracle Communications User Data Repository Cloud Disaster Recovery Guide

List of Figures

gure 1. Determining Recovery Scenario9
--

List of Tables

Table 1. Terminology
Table 2: Recovery Scenarios9

List of Procedures

Procedure 1: Recovery Scenario 1—Complete Server Outage	12
Procedure 2: Recovery Scenario 2—Partial Outage One UDR Intact	22
Procedure 3: Recovery Scenario 3 (Case 1)—Database Recovery Backup Present	32
Procedure 4: Recovery Scenario 3 (Case 2)—Database Recovery Backup Not Present	34
Procedure 5: Keep Restored User (Resetting User Password)	37
Procedure 6: Remove the Restored User	39
Procedure 7: Restoring an Archive that does not Contain a Current User	41
Procedure 8: Restoring an Archive that does not Contain a Current User	46

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

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	Constains 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		

1.3 Acronyms

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 reinstall the software and/or hardware.	
Enablement	The business practice of providing support services (hardware, software, documentation, etc) that enable a 3 rd 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 ChannelCase 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:

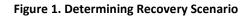
http://docs.oracle.com/en/industries/communications/user-data-repository/index.html

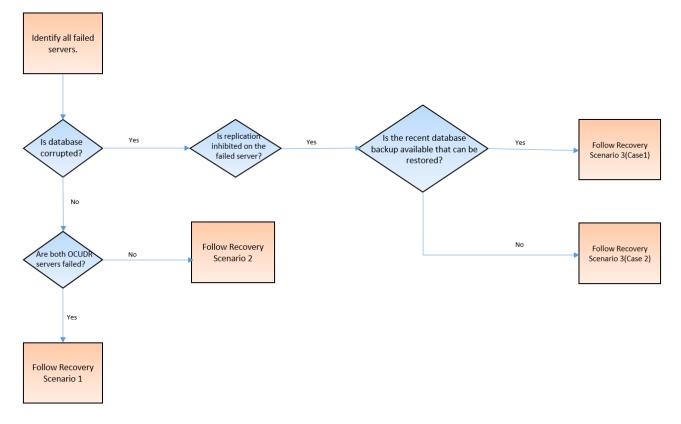
NOTE: For all disaster recovery scenarios, we assume that the UDR database backup was performed

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).





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.

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 intactDatabase gets corrupted on the server	Section Recovery Scenario 3 (Database Recovery)
3: Case 1	Server is intactDatabase gets corrupted on the server	Section Recovery Scenario 3: Case 1

Table 2: Recovery Scenarios

Oracle Communications User Data Repository Cloud Disaster Recovery Guide

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.

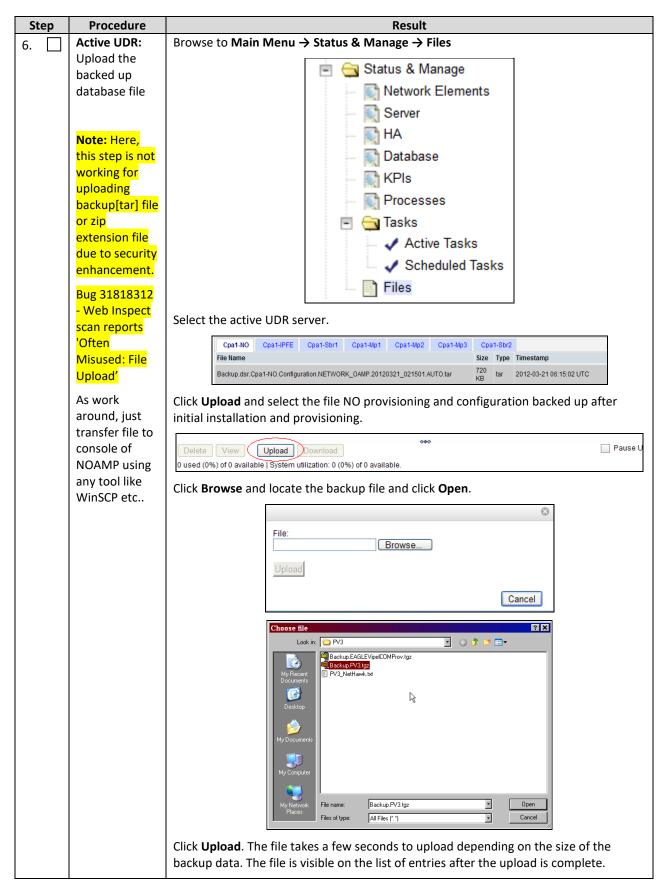
This procedure performs recovery if both UDR servers are failed

Check off ($\sqrt{}$) 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 (1 st NOAMP Only) NOTE: If Topology or nodeld 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: CORRECLEC Oracle System Login Fri Mar 20 12:29:52 2015 EDT Log In Username: guiadmin Password:		



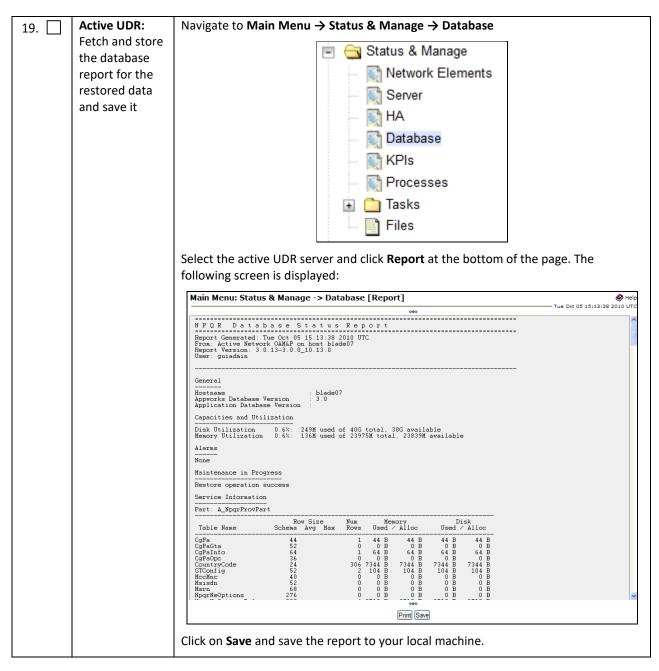
Step	Procedure	Result
Step 7.	Procedure Active UDR: Disable provisioning	Result Click on Main Menu → Status & Manage → Database Image: Status & Manage Image: Status & Manage Image: Status & Manage Image: Status & Manage </th
		The Warning Code 002 message may appear.

Step	Procedure	Result
8.	Active UDR:	Select the active UDR server and click Compare .
	Verify the archive contents and	Enable Provisioning Report Inhibit Replication Backup Compare Restore Man Audit Suspend Auto Audit
database compatibility		The following screen is displayed; select the restored database file that was uploaded as a part of Step 13 of this procedure.
		Database Compare
		Select archive to compare on server: blade02 Backup nogr blade02 Configuration NETWORK_OAMP 20100928_021502 AUTO tar Backup nogr blade02 Configuration NETWORK_OAMP 20100020 021501 AUTO tar Backup nogr blade02 Configuration NETWORK_OAMP 2010100_021501 AUTO tar Backup nogr blade02 Configuration NETWORK_OAMP 2010100_021501 AUTO tar Backup nogr blade02 Configuration NETWORK_OAMP 2010100_021502 AUTO tar Backup nogr blade02 Configuration NETWORK_OAMP 2010100_021501 AUTO tar Backup nogr blade02 Configuration NETWORK_DAMP 2010100_021501 AUTO tar Backup nogr blade02 Configuration NETWORK_DAMP 2010100_0100100 AUTO tar Backup nogr blade02 Configuration NETWORK_DAMP 2010100_0100100 AUTO AUTO AUTO AUTO AUTO AUTO AUTO AUTO
		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.
		The selected database came from blacke07 on 01/19/2011 at 13:43-47 EDT and contains the following comment: Addma Contains Product Contains Product Contains Product Contains Contain Contains Con
		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:	Navigate to Main Menu → Status & Manage → Database
	Restore the database	Select the active UDR server, and click Restore .
	ualabase	Select the back up provisioning and configuration file.
		Database Restore
		Select archive to Restore on server: blade02
		OBackup.npgr.blade02.configuration NETWORK_OAMP 20100928_021501 AUTO tar OBackup.npgr.blade02.configuration NETWORK_OAMP 20101003_021501 AUTO tar OBackup.npgr.blade02.configuration NETWORK_OAMP 20101001_021501 AUTO tar OBackup.npgr.blade02.configuration.NETWORK_OAMP 20101003_021502 AUTO tar OBackup.npgr.blade02.configuration.NETWORK_OAMP 20101005_021501 AUTO tar OBackup.npgr.blade02.configuration.NETWORK_OAMP 20101005_021501 AUTO tar
		Click OK . The following confirmation screen is displayed.
		NOTE: You get a database mismatch regarding the NodelDs 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.
		Database Restore Confirm
		Incompatible database selected
		 IMI Server Address A3118.120 has different node IDs in current topology and the selected backu p file. Current node ID: A3118.120, Selected backup file node ID: B2073.087 IMI Server Address C1157.241 has different node IDs in current topology and the selected backu p file. Current node ID: C1157.241, Selected backup file node ID: B2073.087 IMI Server Address B1787.161 has different node IDs in current topology and the selected backu p file. Current node ID: C1157.241, Selected backup file node ID: B2073.087
		Confirm archive "3bladeNPQR.blade07.Configuration.NETWORK_OAMP.20110119_184253.MAN.tar" to Restore on server: blade07
		Force Restore? Force restore on blade07, despite compare errors.
		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></primary_udr_vip_ip_address>
		Login as the guiadmin user:
		ORACLE
		Oracle System Login
		Enter your username and password to log in Username: guiadmin Password: ••••••• Champe password Log in Wetcome to the Oracle System Logn.
		Unauthorized access is prohibited. This Cracke system requires the use of Microsoft Internet Explorer 6.0, 9.0, or 10.0 with support for JavaScropt and coalies. Oracle and Java are registred refacements of Oracle Corporation and/or its attiliates. Other names may be trademarks of their respective owners.

Step	Procedure	Result
11.	Active UDR: Monitor and	Wait for approximately 5 to 10 minutes for the system to stabilize with the new topology:
	confirm database restoral	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:	Perform the following command:
	Restore /etc/hosts/ file of the active UDR	<pre>\$ sudo AppWorks AppWorks_AppWorks updateServerAliases <udr host="" name=""></udr></pre>
14.	Active UDR: Recover standby UDR	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]:
	(HA Deployments Only)	 Procedure 6 "Create Configuration for Remaining Servers", Step 8. Procedure 7 "Apply Configuration for Remaining Servers" for second UDR. NOTE: If Topology or nodeld alarms are persistent after the database restore, refer to the steps below.
15.	Active UDR:	Navigate to Main Menu → Status & Manage → Server,
	Restart UDR application on recovered UDR	Status & Manage Network Elements Server HA Database KPIs Tasks Files Select the recovered standby UDR server and click Restart.

Step	Procedure	Result
16.	Active UDR:	Navigate to Status & Manage → HA
	Set HA on standby UDR	 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 System Login Fit Mar 20 12:29:52 2015 EDT Log In</primary_udr_vip_ip_address>
		Enter your username and password to log in Username: guiadmin Password: Password: Change password Change password Log In Username: Wekome to the Oracle System Logn. 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 cookes. 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 hostname="" server=""></recovered>



20.	Active UDR:	Login to the	e active	UDR via S	SH terr	minal as	admus	r user.				
	Verify replication	Run the following command:										
	between	\$ sudo irepstat -m										
	servers	Output is ge	enerate	d:								
		Policy	0 ActS	tb [DbRe	plicat	ion]						
		*UDR-A (A2	2434.10	4) Ac	t/Act	Act	Gr	oups=1	Links=	=2		
		ΑΑ Το	PO UD	R-B A	ctive		0	0.10	1%R 0	.08%cpu	44.6/	s
		ΑΑ Το	P1 DR	-UDR-B A	ctive		0	0.10	1%R 0	.10%cpu	38.6/	s
		UDR-B (A24	134.105) Act	/Stb -	- Stb -	Gro	ups=1	Links=1	1		
		AA From	P0 *U	DR-A A	ctive		0	0.10	^0.07 ^s	%cpu 35	.7/s	
		DR-UDR-A ((A3629.	172)	Stb/St	b Ir	nSvc -	- Grou	ps=1 L:	inks=1		
		AA From	P0 DR	-UDR-B A	ctive		0	0.10	^0.07	%cpu 49	.9/s	
		DR-UDR-B ((A3629.	173)	Stb/Ac	t Ir	nSvc -	- Grou	ps=1 L:	inks=2		
		AA To	P0 DR	-UDR-A A	ctive		0	0.10	1%R 0	.08%cpu	31.3/	S
		AA From	P1 *U	DR-A A	ctive		0	0.10	^0.06	%cpu 47	.1/s	
21.	Active UDR: Verify the database states		the OAN ormal. erver R-OCUDR-B CUDR-A CUDR-B			Status Netv Serv HA Data NPIs Proc Tasl	& Man vork E ver abase s cesses ks s	age lement	S	SIG Repl Status NotApplicable	Repl Status Allowed Allowed Allowed	the Repl Audit Status NotApplicable NotApplicable NotApplicable

	1	1							
22.	Active UDR:	Click on M a	ain Menu	ı → Statu	s and Ma	anage → HA			
	Verify the HA			(internet)	🚔 Stat	tus & Manage			
	status			-		-			
					- Q1	Network Elem	ents		
					💽 :	Server			
						HA			
					1 A				
					🔍 I	Database			
					🔊 I	KPIs			
					- A				
						Processes			
					🛨 💼 1	Tasks			
						Files			
		Select the	row for a	ll of the s	ervers				
		Verify that	the HA R	ole is eith	ner Active	e 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	Enable pro	visioning oning Repo	by clickir	sti state st	age → Databas atus & Manag Network Eler Server HA Database KPIs Processes Tasks Files Provisioning a Backup Compare OK to enable p	e nents t the bottom		en. nd Auto Audit
						OK Cancel			

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
25.	Restore GUI usernames and passwords	Examine all active alarms and refer to the on-line help on how to address them. If needed contact My Oracle Support. 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 ($\sqrt{}$) 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

St	ер	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: <pre>http://<primary_udr_vip_ip_address></primary_udr_vip_ip_address></pre> Login as the guiadmin user:
		Cracle System Login Fit Mar 20 12:29:52 2015 EDT Ender your username and password to log in Username: guadminin Password: colspan="2">Change password Change password Log in Wetcome to the Oracle System Login. Username: guadminin Password: colspan="2">Change password Change password Change password Log in Divolme 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 cooles. Oracle and Java ar registered trademarks of Oracle Corporation andor its affinides. Citree names may be trademarks of their respective owners.
3.	Active UDR: Set failed server to standby	 1. Navigate to Main Menu → Status & Manage → HA Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Select Edit 3. Set the Max Allowed HA Role to Standby for the failed server. 4. Click Ok Øk Cancel
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

St	tep	Procedure	Result
5.		Active UDR:	Establish a GUI session on the UDR server by using the VIP IP address of the UDR
		Login	server. Open the web browser and enter a URL of:
			http:// <primary_udr_vip_ip_address></primary_udr_vip_ip_address>
			Login as the guiadmin user:
			ORACLE
			Oracle System Login
			Pri Mar 20 12:29:52 2015 EDT
			Log In Enter your username and pessword to log in Username: guadrum
			Password: •••••••
			Log In Weccene to the Oracle System Login.
			Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Exposer 8.0, 9.0, or 10.0 with support for JavaScript and cookes.
			Oracie and Jana are registered instemation of Oracie Corporation and/or its affiliates Other names may be inademarks of their respective owners.
6.		Active UDR:	Configure the standby UDR server by performing procedures from reference Oracle
		Recover standby UDR	<i>Communications User Data Repository</i> 12.5.1 <i>Cloud Installation and Configuration</i> <i>Guide,</i> E95212, <i>latest revision</i> [2]:
		standby ODK	
			 Procedure 6 "Create Configuration for Remaining Servers", Step 8. Procedure 7 "Apply Configuration for Remaining Servers" for UDR.
			NOTE: If Topology or nodeld alarms are persistent after the database restore, refer to
			the steps below.
7.		Active UDR:	Navigate to Main Menu → Status & Manage → Server,
		Restart UDR application on	🖃 😋 Status & Manage
		recovered UDR	Network Elements
			Server
			HA 🔂
			🔤 💽 Database
			🔤 💽 KPIs
			Processes
			🖃 🧰 Tasks
			Files
			Select the recovered standby UDR server and click Restart .
			Stop Restart Reboot NTP Sync Report
1			

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

67ms =? ntppeerA 0 6 0 - +0ns[+0ns] +/- Ons =? ntppeerB 0 6 0 - +0ns[+0ns] +/- Ons [root@NO-A admusr]# 2.Stop ntpd service: \$ sudo systemct1 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:</ntp>	10.	Recovered	1. Perform the following to retrieve the remote NTP server:
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. / 'x' = may be in error, '-' = too variable, '?' = unusable. / 'x' = may be in error, '-' = too variable, '?' = unusable. / xxxx [yyyy] +/- zzzz [1] II xxxx [yyyy] = measured offset,			\$ sudo chronyc -N 'sources -a -v'
<pre> Source mode '^' = server, '=' = peer, '#' = local clock. / Source state ''' = current best, '+' = combined, '-' = not combined, i / 'x' = may be in error, '~' = too variable, '?' = unusable. ii</pre>		Sync NTP	Example output:
<pre>/ 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, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, </pre>			[root@NO-A admusr]# chronyc -N 'sources -a -v'
<pre>/ 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, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, yyyy = measured offset, </pre>			
<pre>combined, / 'x' = may be in error, '-' = too variable, '?' = unusable. // xxxx [yyyy] +/- zzzz // Reachability register (octal) xxxx = adjusted offset, // Log2(Polling interval) yyyy = measured offset, // I zzzz = estimated error. // NS Name/IP address Stratum Poll Reach LastRx Last sample </pre>			
<pre>unusable. if unusable. if unusable.</pre>			
<pre>zzzz Reachability register (octal) xxxx = adjusted offset, Log2(Polling interval) yyyy = measured offset, \ \ zzzz = estimated error. \ \ \ zzzz = estimated error. \ \ \ \ MS Name/IP address Stratum Poll Reach LastRx Last sample</pre>			
<pre>offset, ii Log2(Polling interval) i yyyyy = measured offset, ii Log2(Polling interval) i yyyyy = measured offset, ii Log2(Polling interval) i yyyyy = measured offset, ii Lyyyy = measured</pre>			
<pre>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 systemct1 stop chronyd.service 3.Sync the date to the ntp remote server: \$ sudo systemct1 stop chronyd.service 3.Sync the date to the ntp remote server: \$ sudo systemct1 stop chronyd.service aserver </pre>			
<pre>error. </pre>			
MS Name/IP address Stratum Poll Reach LastRx Last sample			
<pre></pre>			
<pre>^* 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 systemct1 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:</ntp></pre>			MS Name/IP address Stratum Poll Reach LastRx Last sample
67ms =? ntppeerA 0 6 0 - +0ns[+0ns] +/- Ons =? ntppeerB 0 6 0 - +0ns[+0ns] +/- Ons [root@NO-A admusr]# 2.Stop ntpd service: \$ sudo systemct1 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:</ntp>			
Ons =? ntppeerB 0 6 0 - +Ons[+Ons] +/- Ons [root@NO-A admusr]# 2.Stop ntpd service: \$ sudo systemct1 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:</ntp>			
<pre>Ons [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:</ntp></pre>			
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:</ntp>			
<pre>\$ 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:</ntp></pre>			[root@NO-A admusr]#
<pre>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:</ntp></pre>			2. Stop ntpd service:
<pre>\$ sudo vi etc/chrony.conf Update NTP source as below # Specify time sources. server <ntp source=""> iburst peer ntppeerA iburst peer ntppeerB iburst Example:</ntp></pre>			<pre>\$ sudo systemctl stop chronyd.service</pre>
Update NTP source as below # Specify time sources. server <ntp source=""> iburst peer ntppeerA iburst peer ntppeerB iburst Example:</ntp>			
server <ntp source=""> iburst peer ntppeerA iburst peer ntppeerB iburst Example:</ntp>			
			server <ntp source=""> iburst peer ntppeerA iburst</ntp>
<pre># Specify time sources. server 10.250.32.10 iburst peer ntppeerA iburst peer ntppeerB iburst</pre>			Example: # Specify time sources. server 10.250.32.10 iburst peer ntppeerA iburst
NOTE: The remote server is the one gathered in sub step 1.			
4. Start the ntp service:			4. Start the ntp service:
<pre>\$ sudo systemctl start chronyd.service</pre>			<pre>\$ sudo systemctl start chronyd.service</pre>

Step	Procedure	Result
Step	Procedure Active UDR: Restart UDR application on recovered servers (HA deployments only)	 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 : 0.000038986 seconds Frequency : 91.246 ppm slow Residual freq : -0.001 ppm Skew : 0.276 ppm Root delay : 0.033020783 seconds Update interval : 64.7 seconds Leap status : Normal [root@NO-A admusr]# NOTE: For Non-HA sites SKIP this step Navigate to Main Menu → Status & Manage → Server Image: Status & Manage Image: KPIs
		🖬 🧰 Tasks
		Files
		Select the recovered server and click Restart .
		Stop Restart Reboot NTP Sync Report

Step	Procedure	Result					
12.	Active UDR:	Un-Inhibit (start) replication to the all C-Level (MP) servers					
	Start replication on all servers	Navigate to Status & Manage → Database					
		📄 😋 Status & Manage					
		Network Elements					
		- Server					
		- 💽 HA					
	Database						
		- 🟹 KPIs					
		- Nordenses					
	🖬 🧰 Tasks						
	Files						
		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 middle button shows Inhibit Replication, and not Allow Replication. 						
13.	Active UDR:	Establish an SSH session to the Active UDR, login as admusr.					
	Perform key exchange between the	Perform the following command to perform a keyexchange from the active UDR to each recovered server:					
	active-UDR and \$ keyexchange admusr@ <recovered hostname="" server=""></recovered>						
	recovered servers. NOTE: If an export server is configured, perform this step.						

Step	Procedure	Result
14.	Active UDR:	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: Main Menu: Status & Manage -> Database [Report]
		Hortmarke Database Version : Application Database Version : Capacities and Utilization Disk Utilization 0.6%: 249M used of 40G total, 38G available Memory Utilization 0.6%: 136M used of 23975M total, 23839M available Alarms None Maintenance in Progress Restore operation success Service Information Part: A_NpqrProvPart Table Name Schema Avg Max Rovs Used / Alloc CgPaCta 52 1 0 B 0 B 0 B 0 B CgPaCta 54 1 64 B 64 B 64 B 64 B 64 B 64 B 64 B CgPaChi 64 1 64 B
		Print Save
		Click on Save and save the report to your local machine.

Step	Procedure					Re	sult					
15.	Active UDR: Login to the active UDR via SSH terminal as admusr user.											
	Verify replication	Perform the	e follow	ing comm	and:							
	between	\$ sudo	ireps	tat -m								
	servers.	Output like	below i	s generat	ed:							
		Policy	0 ActS	tb [DbRe	plicat	ion] -						
		*UDR-A (A2	2434.10	4) Ac	t/Act	Act	Gi	roups=1	l Link:	s=2		
		AA To	PO UD	R-B A	ctive		0	0.10	0 1%R (0.06%cp	ou 65.4	l/s
		AA To	P1 DR	-UDR-B A	ctive		0	0.10	0 1%R (0.08%cp	ou 73.0)/s
		UDR-B (A24	134.105) Act	/Stb -	- Stb	Gro	oups=1	Links	=1		
		AA From	PO *U	DR-A A	ctive		0	0.14	4 ^0.0'	7%cpu 6	6.0/s	
		DR-UDR-A	(A3629.	172)	Stb/St	b I	nSvc -	Grou	ups=1 :	Links=1		
		AA From	P0 DR	-UDR-B A	ctive		0	0.10	0.0^	7%cpu 8	3.5/s	
		DR-UDR-B	(A3629.	173)	Stb/Ac	t I	nSvc -	Grou	ups=1 1	Links=2		
		AA To	P0 DR	-UDR-A A	ctive		0	0.10	0 1%R (0.08%cp	ou 72.8	8/s
		AA From	P1 *U	DR-A A	ctive		0	0.10	0.0^	6%cpu 7	3.2/s	
16. 🗌	Active UDR:	Click on Ma	in Men	u → Statu	is and	Manage	er → D	atabas	e			
	Verify the database states					Status						
						📄 Netv	work E	Elemen	ts			
						Sen						
						HA 🕤						
						Data	abase					
						KPI						
						A.		_				
						A.	cesse	5				
					- 🖻 🖡	🗋 Tasl						
						File:	s					
		Verify that	tha 041		Role i	aithar	active	orstan	dby for	r LIDR ai	nd that	the
		status is No			noie i.	, citilet	active	Ji Stall			ia triat	the
			-			Application						
		Network Element	Server	Role	OAM Max HA Role	Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
		Site2_NE_DR_NO		Network OAM&P	Spare	N/A	Normal	18387	Normal	NotApplicable		NotApplicable
			OCUDR-A OCUDR-B	Network OAM&P	Active Standby	N/A N/A	Normal	18387 18387	Normal	NotApplicable NotApplicable		NotApplicable NotApplicable
		Site2_NE_DR_NO		Network OAM&P	Spare	N/A	Normal	18387	Normal	NotApplicable		NotApplicable

Step	Procedure			Resu	t		
17.	Active UDR:	Click on Main Menu \rightarrow Status and Manage \rightarrow HA					
	Verify the HA	📄 😋 Status & Manage					
	status	Network Elements					
				Server			
				HA			
				Databas	e		
				KPIs			
			💓	Process	ses		
			🗈) Tasks			
			III	Files			
		Select the row for all of	the servers				
		Verify that the HA Role	is either acti	ive or star	idby.		
		OAM Max	Application Max				
		Hostname HA Role NO2 Active	Role Role	Mate Hostname List	Network Element	Server Role Network OAM&P	Active VIPs 10.240.70.132
		SO1 Standby SO2 Active	OOS Active	SO2 SO1	SO_10303 SO_10303	System OAM System OAM	10.240.70.133
		MP1 Standby	Active Active	MP2	SO_10303	MP	10.210.10.100
		MP2 Active IPFE Active	Active Active OOS Active	MP1	SO_10303 SO_10303	MP MP	
18.	Active UDR:	Login to the UDR VIP if not logged in.					
	Examine all	Navigate to Main Menu	u → Alarms a	& Events -	→ View Active		
	alarms	Γ		Alarms &			
		View Active					
					listory		
					-		
		View Trap Log					
		Examine all active alarms and refer to the on-line help on how to address them.					
		If needed contact My O	racle Suppo	rt.			
19.	Backup and	Perform Appendix A Or			User Data Repo	sitory Da	tabase Backup
	archive all the	to back up the configur	ation databa	ise.			
	databases from						
	the recovered						
	system						
		THIS PROCEDU	RE HAS BEEN		TED		

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 ($\sqrt{}$) 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:	Navigate to Main Menu → Status & Manage → HA						
т. <u>с</u>	Set failed servers to standby	Status & Manage Status & Manage Ketwork Elements HA Database KPIs Processes						
		Tasks						
		Select Edit						
		Set the Max Allowed HA Role to Standby for the failed servers.						
		Click Ok						
		Ok Cancel						
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						
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 ($\sqrt{}$) 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 Pre	sent
--	------

Step	Procedure	Result				
1.	Active UDR: Set failed	Navigate to Main Menu → Status & Manage → HA				
	servers to	🖃 😋 Status & Manage				
	standby	Network Elements				
		- Server				
		🟹 HA				
		— 💽 Database				
		- KPIs				
		- Norman Processes				
		🖬 🧰 Tasks				
		Files				
		Click Edit				
		Set the Max Allowed HA Role to Standby for the failed servers.				
		Click Ok				
		Ok Cancel				
2.	Server with	Establish an SSH session to the server in question. Login as admusr user.				
	DB Corruption:					
	Login					
3.	Server with	Run the following command to take the server out of service.				
	DB Corruption:	\$ sudo bash -1 \$ sudo prod clobbor				
	Take server	<pre>\$ sudo prod.clobber</pre>				
	out of service					

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 -1 \$ sudo prod.start
5.	Server with DB Corruption: Verify the server state	<pre>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</pre>
6.	Active UDR: Restart UDR application	Navigate to Main Menu → Status & Manage Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select each recovered server and click Restart. Stop Restart Reboot NTP Sync Report

Step	Procedure	Result						
7.	Active UDR:	Navigate to Status & Manage → HA						
	Set failed	🖃 😋 Status & Manage						
	servers to active	Network Elements						
	active							
		Server						
		🔊 HA						
		🔤 🏹 Database						
		🔤 💽 KPIs						
		- M Processes						
		🖃 🧰 Tasks						
		Files						
		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	Perform Appendix A Oracle Communications User Data Repository Database Backup to						
	archive all the	back up the configuration databases.						
	databases							
	from the recovered							
	system							
	system							
	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 ($\sqrt{}$) 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: Image: Concernent concernet concernent concernet concernet concernent</primary_udr_vip_ip_address>

Step	Procedure	Result
3.	After	Navigate to Administration → Access Control → Users
3.	Restoration: Reset User Passwords	 Main Menu Administration General Options Access Control Users Users Groups Sessions Certificate Management
		Authorized IPs
		SFTP Users
		Select the user
		Click Change Password
		Insert Edit Delete Report Change Password
		Enter a new password
		Enter the new password for guiadmin two times. New Password: Retype New Password: If Force password change on next login Continue
		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 ($\sqrt{}$) 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	Establish a GUI session on the UDR server by using the VIP IP address of the UDR	
	Restoration:	server. Open the web browser and enter a URL of:	
	Login to the active UDR	http:// <primary_udr_vip_ip_address></primary_udr_vip_ip_address>	
		Login as the guiadmin user:	
		Oracle System Login Fit Mar 20 12:29:52 2015 EDT Description of the Colspan Description of	

Step	Procedure	Result
5.	After	Navigate to Administration → Access Control → Users
	Restoration: Delete User	🖃 💻 Main Menu
		🖻 😋 Administration
		General Options
		🖃 🤤 Access Control
		- 🍦 Users
		- 🚰 Groups
		Sessions
		Certificate Management
		Authorized IPs
		SFTP Users
		Select the user
		Click Delete
		Insert Edit Delete Report Change Password
		Delete selected users?
		OK Cancel
		Click OK to confirm.
	<u> </u>	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 ($\sqrt{}$) 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.	2. D 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:
	Login to the	http:// <primary_udr_vip_ip_address></primary_udr_vip_ip_address>
	active UDR (before	Login as the guiadmin user:
	restoration)	ORACLE
		Oracle System Login
		Log In Enter your username and password to log in Username: guiadmin
		Password: Change password
		Welcome to the Oracle System Login.
		Unauthorized access is prohibiled. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookes.
		Oracie and Java are registered trademarks of Oracie Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Step	Procedure	Result	
3.	Before Restoration: Record user settings (Before	Navigate to Administration → Access Control → Users Main Menu Administration General Options	
	(Before Restoration)	 General Options Access Control Users Groups Sessions Certificate Management Authorized IPs SFTP 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: <a href="http://<Primary_UDR_VIP_IP_Address">http://<primary_udr_vip_ip_address< a=""> Login as the guiadmin user:</primary_udr_vip_ip_address<>	
		Oracle System Login Fit Mar 20 12: 29:52 2015 EDT	

5.	After	Navigate to Administration → Access Control → Users
5.	After Restoration: Recreate affected user	Navigate to Administration → Access Control → Users Main Menu Administration General Options Access Control Access Control Users Groups Sessions Certificate Management Authorized IPs SFTP Users
		Click Insert Click Insert Edit Delete Report Change Password Recreate the user using the data collected in Step 3.

Step	Procedure		Re	sult
			Username *	
			Group *	admin
			Authentication Options	Allow Remote AuthenticationAllow Local Authentication
			Access Options	Allow GUI AccessAllow MMI Access
			Access Allowed	Account Enabled
			Maximum Concurrent Logins	0
			Session Inactivity Limit	120
			Comment *	
		Click O ł		ly Cancel
6.	After Restoration: Repeat for Additional Users	Repeat	Step 5 to recreate additional users.	

Step	Procedure	Result
7.	After	Navigate to Administration → Access Control → Users
	Restoration: Reset the	🖃 💻 Main Menu
	Passwords	🖻 😋 Administration
		🔤 📺 General Options
		🖃 🤤 Access Control
		- 🌔 Users
		- 🎁 Groups
		- Dissions
		- 📄 Certificate Management
		Authorized IPs
		SFTP Users
		Select the user
		Click Change Password
		Insert Edit Delete Report Change Password
		Enter a new password
		Enter the new password for guiadmin two times.
		New Password:
		Retype New Password:
		Force password change on next login
		Continue
		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 ($\sqrt{}$) 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></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 cookes. Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.	

Step	Procedure	Result	
2.	Active UDR:	Navigate to Main Menu → Status & Manage → Database	
	Backup	📄 😋 Status & Manage	
	configuration data for the	Network Elements	
	system		
	-,	Server	
		— 🟹 HA	
		— 💽 Database	
		- 💽 KPIs	
		- Nordenses	
		Select the active UDR server and click Backup .	
		Disable Provisioning Report Inhibit Replication Backup Compare Restore Man Audit Suspend Auto Audit	
		Make sure that configuration is selected.	
		Field Value	
		Server: OCUDR-A	
		Select data for backup	
		Configuration	
		Archive Name * Backup.udr.OCUDR-A.Configuration.NETWORK_OAMP.20180419_015336.MAN	
		Comment	
		Ok Cancel	
		Enter a filename for the backup and click OK	

Step	Procedure	Result
3.	Active UDR:	Navigate to Main Menu → Status & Manage → Files
	Verify the backup file	📄 😋 Status & Manage
	existence.	Network Elements
		Server
		- 🛐 HA
		Database
		- KPIs
		- Structure Processes
		🕢 🛅 Tasks
		Files
		Main Menu: Status & Manage -> Files
		Filter* ▼ Tasks ▼
		OCUDR-A OCUDR-B DR-OCUDR-A DR-OCUDR-B
		File Name
		Backup.UDR.OCUDR-A.FullDBParts.NETWORK_OAMP.20180410_074209.UPG.tar
		Backup.UDR.OCUDR-A.FullRunEnv.NETWORK_OAMP.20180410_074209.UPG.tar
		backup/Backup.udr.OCUDR-A.Configuration.NETWORK_OAMP.20180410_021512.AUTO.tar
		backup/Backup.udr.OCUDR-A.Provisioning.NETWORK_OAMP.20180410_031512.AUTO.tar
		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 Delete View Upload Download Deploy ISO Validate ISO 1.1 GB used (5.93%) of 18.4 GB available System utilization: 1.1 GB (5.99%) of 18.4 GB available. Click OK to confirm the download. Click OK to confirm the download. Opening Backup.udr.OCUDR-A.Configuration.NETWORK_OAMP.20180 You have chosen to open: A.Configuration.NETWORK_OAMP.20180410_021512.AUTO.tar which is: tar File (2,8 MB) from: https://10.75.173.158 What should Firefox do with this file? 		
5.	Upload the	Transfer the backed up image saved in Step 4 to a secure location where the server		
	Image to Secure	backup files are fetched during a system disaster recovery.		
	Location			
	THIS PROCEDURE HAS BEEN COMPLETED			

Appendix B. My Oracle Support

My Oracle Support (<u>https://support.oracle.com</u>) 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 <u>http://www.oracle.com/us/support/contact/index.html</u>. 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, <u>http://docs.oracle.com</u>. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at <u>http://www.adobe.com</u>.

- 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.