Oracle® Communications

Diameter Signaling Router DSR 3-Tier Disaster Recovery Guide

Release 5.0/6.0/7.0/7.1

E57520 Revision 02

August 2015



Oracle Communications Diameter Signaling Router DSR 3-tier Disaster Recovery Procedure, Release 5.0/6.0/7.0/7.1

Copyright © 2015 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, 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 on 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. 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.



MOS (<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 MOS 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*.

|--|

Table of Contents	3
List of Procedures	1
List of Tables	5
List of Figures	5
1.0 Introduction	5
1.1 Purpose and Scope	5
1.2 References	3
1.3 Acronyms	7
1.4 Terminology	3
1.5 Optional Features)
2.0 General Description)
2.1 Complete Server Outage (All Servers)1	I
2.2 Partial server outage with one NOAM server intact and both SOAMs failed	I
2.3 Partial server outage with both NOAM servers failed and one SOAM server intact	I
2.4 Partial server outage with NOAM and one SOAM server intact1	I
2.5 Partial Service outage with corrupt database1	I
3.0 Procedure Overview	2
3.1 Required Materials12	2
3.1.1 Release Document Matrix13	3
3.2 Disaster Recovery Strategy14	1
4.0 Procedure Preparation	3
5.0 Disaster Recovery Procedure	7
5.1 Recovering and Restoring System Configuration19)
5.1.1 Recovery Scenario 1 (Complete Server Outage)19)
5.1.2 Recovery Scenario 2 (Partial Server Outage with one NOAM server intact and both SOAMs failed)	1
5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact)	5
5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)	5
5.1.5 Recovery Scenario 5 (Both NOAM servers failed with DR-NOAM available)	2
5.1.6 Recovery Scenario 6 (Database Recovery)118	3
6.0 Resolving User Credential Issues after Database Restore	1
6.1 Restoring a Deleted User	1
6.2 Keeping a Restored user12	5

6.3 Removing a Restored User	. 127
6.4 Restoring a Modified User	. 129
6.5 Restoring an Archive that does not contain a Current User	. 130
7.0 IDIH Disaster Recovery	. 133
Appendix A. DSR Database Backup	. 138
Appendix B. Recovering/Replacing Failed 3 rd Party Components (Switches, OAs)	. 142
Appendix C. Switching DR NOAM Site to Primary	. 147
Appendix D. Returning a Recovered Site to Primary	. 151
Appendix E. Inhibit A and B Level Replication on C-Level Servers	. 157
Appendix F. Un-Inhibit A and B Level Replication on C-Level Servers	. 159
Appendix G. Workarounds for Issues not fixed in this Release	. 161
Appendix H. My Oracle Support (MOS)	. 163

List of Procedures

Procedure 1: Recovery Scenario 1	21
Procedure 2: Recovery Scenario 2	52
Procedure 3: Recovery Scenario 3	76
Procedure 4: Recovery Scenario 4	96
Procedure 5: Recovery Scenario 5	
Procedure 6: Recovery Scenario 6 (Case 1)	
Procedure 7: Recovery Scenario 6 (Case 2)	
Procedure 8: Keep Restored User	
Procedure 9: Remove the Restored User	
Procedure 10: Restoring an Archive that does not Contain a Current User	
Procedure 11: IDIH Disaster Recovery Preparation	
Procedure 12: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)	
Procedure 13: Restoring an Archive that does not Contain a Current User	
Procedure 14: Recovering a Failed Aggregation Switch (Cisco 4948E/4948E-F)	
Procedure 15: Recovering a Failed Enclosure Switch (Cisco 3020)	
Procedure 16: Recovering a Failed Enclosure Switch (HP 6120XG)	144
Procedure 17: Recovering a Failed Enclosure Switch (HP 6125XLG, HP 6125G)	145
Procedure 18: Recovering a Failed Enclosure OA	146
Procedure 19: Switching a DR NOAM Site to Primary	147
Procedure 20: Returning a Recovered Site to Primary	

Procedure 21: Inhibit A and B Level Replication on C-Level Servers	. 157
Procedure 22: Un-Inhibit A and B Level Replication on C-Level Servers	. 159

List of Tables

Table 1 Acronyms	7
Table 2 Terminology	8
Table 3 Optional Features	9
Table 4: DSR Base Hardware Installation Reference Table	13
Table 5: DSR Software Installation/Configuration Reference Table	13
Table 6: DSR PMAC Disaster Recovery Reference Table	13
Table 7: Platform Configuration Reference Table	13
Table 8 IDIH Disaster Recovery Reference Table	13
Table 9 IDIH Installation Reference Table	13
Table 10. Recovery Scenarios	16

List of Figures

1.0 Introduction

1.1 Purpose and Scope

This document is a guide to describe procedures used to execute disaster recovery for DSR 5.0/6.0/7.0/7.1 (3-tier deployments). This includes recovery of partial or a complete loss of one or more DSR servers. The audience for this document includes GPS groups such as Software Engineering, Product Verification, Documentation, and Customer Service including Software Operations and First Office Application. This document can also be executed by Oracle customers, as long as Oracle Customer Service personnel are involved and/or consulted. This document provides step-by-step instructions to execute disaster recovery for DSR 5.0/6.0/7.0/7.1. Executing this procedure also involves referring to and executing procedures in existing support documents.

Note that components dependent on DSR might need to be recovered as well, for example SDS, IDIH, and PMAC. As of DSR 7.1, IDIH content is included in this document (**Section 7.0**). For DSR 5.0, 6.0, and 7.0, please refer to **Table 8** IDIH Disaster Recovery Reference Table. For SDS, please refer to [7] for 5.x/6.x/7.0, [23] for SDS 7.1

1.2 References

- [1] TPD Initial Product Manufacture, E54521-01
- [2] DSR 5.x Base Hardware and Software Installation, 909-2282-001
- [3] DSR 6.0/7.0 Hardware and Software Installation, E57789
- [4] Platform 6.7/7.0 Configuration Procedure Reference, E54386
- [5] DSR 5.x/6.x Software Installation and Configuration Procedure Part 2/2, E52510
- [6] PM&C 5.x Disaster Recovery Guide, 909-2283-001
- [7] SDS 5.x/6.x/7.x Disaster Recovery Guide, 909-2308-001
- [8] IDIH 6.0/7.0 Installation/Upgrade Guide, E56571
- [9] DSR 3.0/4.x/5.x 2-tier Disaster Recovery, 909-2225-001
- [10]Policy DRA Activation, E58662
- [11] CPA Feature Activation Procedure, E58663
- [12] DSR Mediation Feature Activation Procedure, E58661
- [13] DSR FABR Feature Activation Procedure, E58664
- [14] DSR RBAR Feature Activation Procedure, E58665
- [15] DSR MAP-Diameter IWF Feature Activation Procedure, E58666
- [16] DSR 7.0 PCA Work Instruction, E58667
- [17] DSR 7.0/7.1 Software Installation and Configuration Procedure Part 2/2, E58954
- [18] Integrated Diameter Intelligence Hub 7.0 Disaster Recovery Procedure, E56375
- [19] DSR GLA Feature Activation Procedure, E58659
- [20] DSR 7.1 Hardware and Software Installation, E53488
- [21] PM&C 5.7/6.0 Disaster Recovery Guide, E54388
- [22] DSR 5.0/6.0 PDRA Configuration Work Instruction, WI006808
- [23] SDS 7.1 Disaster Recovery Guide. E59145
- [24] IDIH 5.x Installation/Upgrade Procedure, 909-2232-002
- [25] DSR 7.1 PCA Activation and Configuration, E63560
- [26] IDIH 6.0/7.0 Disaster Recovery Guide, E56375

1.3 Acronyms

Table 1 Acronyms

Acronym	Definition	
BIOS	Basic Input Output System	
CD	Compact Disk	
DVD	Digital Versatile Disc	
EBIPA	Enclosure Bay IP Addressing	
FRU	Field Replaceable Unit	
HP c-Class	HP blade server offering	
iLO	Integrated Lights Out manager	
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform	
MSA	Modular Smart Array	
NB	NetBackup	
OA	DA HP Onboard Administrator	
OS	Operating System (e.g. TPD)	
RMS	Rack Mounted Server	
PMAC	Platform Management & Configuration	
SAN	Storage Area Network	
SFTP	Secure File Transfer Protocol	
SNMP	Simple Network Management Protocol	
TPD	Tekelec Platform Distribution	
TVOE	Tekelec Virtual Operating Environment	
VM	Virtual Machine	
VSP	Virtual Serial Port	
IPFE	IP Front End	
PCA	Policy and Charging Application	
IDIH	Integrated Diameter Intelligence Hub	
SDS	Subscriber Database Server	

1.4 Terminology

Table 2 Terminology

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 server's operating system: Oracle 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.
Software Centric	The business practice of delivering an Oracle software product, while relying upon the customer to procure the requisite hardware components. Oracle provides the hardware specifications, but does not provide the hardware or hardware firmware, and is not responsible for hardware installation, configuration, or maintenance.
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.

1.5 Optional Features

Further configuration and/or installation steps will need to be taken for optional features that may be present in this deployment. Please refer to these documents for disaster recovery steps needed for their components

Table 3 Optional Features

Feature	Document
Diameter Mediation	DSR Meta Administration Feature Activation Procedure,
	E58661
Charging Proxy Application (CPA)	DSR CPA Feature Activation Procedure, E58663
Full Address Based Resolution (FABR)	DSR FABR Feature Activation Procedure, E58664
Range Based Address Resolution	DSR RBAR Feature Activation Procedure, E58665
(RBAR)	
Map-Diameter Interworking (MAP-IWF) –	DSR MAP-Diameter IWF Feature Activation Procedure,
DSR 6.0+	E58666
Policy and Charging Application (PCA)	 DSR 7.0 PCA Activation and Configuration
	Procedure, E58667
	DSR 5.0/6.0 PDRA Activation and Configuration Work
	Instruction, WI006808
	 DSR 7.1 PCA Activation and Configuration
	Procedure, E63560

2.0 General Description

The DSR disaster recovery procedure falls into five basic categories. It is primarily dependent on the state of the NOAM servers and SOAM servers:

Recovery of the entire network from a total outage	All NOAM servers failedAll SOAM servers failed
Recovery of one or more servers with at least one NOAM server intact	 1 or more NOAM servers intact 1 or more SOAM or MP servers failed
Recovery of the NOAM pair with one or more SOAM servers intact	All NOAM servers failed1 or more SOAM servers intact
Recovery of one or more server with at least one NOAM and one SOAM server intact.	 1 or more NOAM servers intact 1 or more SOAM servers intact 1 SOAM or 1 or more MP servers failed
Recovery of one or more server with corrupt databases that cannot be restored via replication from the active parent node.	

Note: For Disaster Recovery of the PMAC Server, refer to **Table 6**: DSR PMAC Disaster Recovery Reference Table.

Note: Aggregation switches, OA or 6120/6125/3020 switches refer to **Appendix B**. Recovering/Replacing Failed 3rd Party Components (Switches, OAs).

Note: As of DSR 7.1, IDIH content is included in this document (**Section 7.0**). For DSR 5.0, 6.0, and 7.0, please refer to **Table 8** IDIH Disaster Recovery Reference Table.

2.1 Complete Server Outage (All Servers)

This is the worst case scenario where all the servers in the network have suffered complete software and/or hardware failure. The servers are recovered using base recovery of hardware and software and then restoring database backups to the active NOAM and SOAM servers.

Database backups will be taken from customer offsite backup storage locations (assuming these were performed and stored offsite prior to the outage). If no backup files are available, the only option is to rebuild the entire network from scratch. The network data must be reconstructed from whatever sources are available, including entering all data manually.

2.2 Partial server outage with one NOAM server intact and both SOAMs failed

This case assumes that at least one NOAM servers intact. All SOAM servers have failed and are recovered using base recovery of hardware and software. Database is restored on the SOAM server and replication will recover the database of the remaining servers.

2.3 Partial server outage with both NOAM servers failed and one SOAM server intact

If both NOAM servers have suffered complete software and/or hardware failure (where DR-NOAMs are not present), but at least one SOAM server is available. Database is restored on the NOAM and replication will recover the database of the remaining servers.

2.4 Partial server outage with NOAM and one SOAM server intact

The simplest case of disaster recovery is with at least one NOAM and at least one SOAM servers intact. All servers are recovered using base recovery of hardware and software. Database replication from the active NOAM and SOAM servers will recover the database to all servers. (**Note:** this includes failures of any disaster recovery Network NOAM servers)

2.5 Partial Service 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 active

3.0 Procedure Overview

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

3.1 Required Materials

The following items are needed for disaster recovery:

- 1. A hardcopy of this document (E57520-02) and hardcopies of all documents in the reference list
- Hardcopy of all NAPD performed at the initial installation and network configuration of this customer's site. If the NAPD cannot be found, escalate this issue within My Oracle Support (MOS) until the NAPD documents can be located.
- 3. DSR recent backup files: electronic backup file (preferred) or hardcopy of all DSR configuration and provisioning data.
- 4. Latest Network Element report: Electronic file or hardcopy of Network Element report.
- 5. Oracle Tekelec Platform Distribution (TPD) Media (64 bits).
- 6. Platform Management & Configuration (PMAC) ISO or SW.
- 7. DSR 5.0/6.0/7.0/7.1 CD-ROM (or ISO image file on USB Flash) of the target release.
- 8. TVOE Platform Media (64 bits)
- 9. The xml configuration files used to configure the switches, available on the PMAC Server (or PMAC backup)
- 10. The switch backup files taken after the switch is configured, available on the PMAC Server (or PMAC backup)
- 11. The network element XML file used for the blades initial configuration.
- 12. The HP firmware upgrade pack (Or customer provided firmware)
- 13. NetBackup Files if they exist. This may require the assistance of the customer's NetBackup administrator.
- 14. PMAC and TVOE backups (If available)

Note: For all Disaster Recovery scenarios, we assume that the NOAM Database backup and the SOAM database backup were performed around the same time, and that no synchronization issues exist among them.

<u>SUDO</u>

DSR 6.0+ introduced a new non-root user **'admusr'**, as a non-root user, many commands (when run as admusr) now require the use of 'sudo'.

3.1.1 Release Document Matrix

Table 4: DSR Base Hardware Installation Reference Table

DSR Release	Reference
DSR 5.0	[2]
DSR 6.0	[3]
DSR 7.0	[3]
DSR 7.1	[20]

Table 5: DSR Software Installation/Configuration Reference Table

DSR Release	Reference
DSR 5.0	[5]
DSR 6.0	[5]
DSR 7.0	[17]
DSR 7.1	[17]

Table 6: DSR PMAC Disaster Recovery Reference Table

DSR Release	Reference
DSR 5.0	[6]
DSR 6.0	[21]
DSR 7.0	[21]
DSR 7.1	[21]

Table 7: Platform Configuration Reference Table

DSR Release	Reference
DSR 5.0	[2]
DSR 6.0	[4]
DSR 7.0	[4]
DSR 7.1	[4]

Table 8 IDIH Disaster Recovery Reference Table

IDIH Release	Reference
IDIH 6.0	[26]
IDIH 7.0	[26]

Table 9 IDIH Installation Reference Table

IDIH Release	Reference
IDIH 6.0	[8]
IDIH 7.0	[8]
IDIH 7.1	[17]

3.2 Disaster Recovery Strategy

Disaster recovery procedure execution 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 2.0**.
- 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 and **Table 10.** Recovery Scenarios.
- 5. Execute appropriate recovery procedures (listed in Table 10. Recovery Scenarios).





4.0 Procedure Preparation

Disaster recovery procedure execution is dependent on the failure conditions in the network. The severity of the failure determines the recovery scenario for the network. Use **Table 10.** Recovery Scenarios below to evaluate the correct recovery scenario and follow the procedure(s) listed to restore operations.

Note: 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.

Recovery Scenario	Failure Condition	Section
1	 All NOAM servers failed. All SOAM servers failed. MP servers may or may not be failed. 	Section 5.1.1 Recovery Scenario 1 (Complete Server Outage)
2	 At least 1 NOAM server is intact and available. All SOAM servers failed. MP servers may or may not be failed. 	Section 0
3	 All NOAM servers failed. At least 1 SOAM server out of Active, StandBy, Spare is intact and available. MP servers may or may not be failed. 	Section 5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact)
4	 At least 1 NOAM server is intact and available. At least 1 SOAM server out of Active, StandBy, Spare is intact and available. 1 or more MP servers have failed. 	Section 5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)

Table 10. Recovery Scenarios

5	 Both NOAM servers failed. DR NOAM is Available SOAM servers may or may not be failed. MP servers may or may not be failed. 	Section 5.1.5 Recovery Scenario 5 (Both NOAM servers failed with DR-NOAM available)
6	 Server is intact Database gets corrupted on the server Latest Database backup of the corrupt server is present Replication is inhibited (either manually or because of comcol upgrade barrier) 	Section 5.1.6 Recovery Scenario 6 (Database Recovery)
6: Case 1	 Server is intact Database gets corrupted on the server Replication is occurring to the server with corrupted database 	Section 5.1.6.1 Recovery Scenario 6: Case 1
6: Case 2	 Server is intact Database gets corrupted on the server Latest Database backup of the corrupt server is NOT present Replication is inhibited (either manually or because of comcol upgrade barrier) 	Section 5.1.6.2 Recovery Scenario 6: Case 2

5.0 Disaster Recovery Procedure

Call Appendix H. My Oracle Support (MOS) prior to executing this procedure to ensure that the proper recovery planning is performed.

Before disaster recovery, users must properly evaluate the outage scenario. This check ensures that the correct procedures are executed 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.

Recovering Base Hardware:

- 1. Hardware Recovery will be executed by the appropriate HW vender.
- 2. Base Hardware Replacement must be controlled by engineer familiar with DSR Application

5.1 Recovering and Restoring System Configuration

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

5.1.1 Recovery Scenario 1 (Complete Server Outage)

For a complete server outage, NOAM servers are recovered using recovery procedures of base hardware and software and then executing a database restore to the active NOAM server. All other servers are recovered using recovery procedures of base hardware and software.

Database replication from the active NOAM server will recover 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 execute the procedure. The actual detailed steps are in **Procedure 1**. The major activities are summarized as follows:

Note: Use the release document matrix from **Section 3.1.1** Release Document Matrixto determine which document is referenced for the applicable DSR release.

Recover Base Hardware and Software for all Blades:

- Recover the base hardware. (By replacing the hardware and executing hardware configuration procedures) Reference **Table 4**: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference.
- Recover the Virtual Machines hosting the NOAMs and SOAMs. Reference **Table 5** for the applicable DSR software installation and configuration reference.

Recover the Active NOAM server by recovering its' NOAM VM Image:

- Recover the NOAM database
- Reconfigure the application

Recover the **Standby NOAM** server by recovering base hardware/software and/or VM image:

• Reconfigure the DSR Application

Recover all SOAM and MP servers by recovering base hardware and software:

- Recover the SOAM database
- Reconfigure the DSR Application
- Reconfigure the signaling interface and routes on the MPs, the DSR software will automatically reconfigure the signaling interface from the recovered database.
- Reference **Table 5** for the applicable DSR software installation/configuration guide if any existing routes need to be altered.

Restart process and re-enable provisioning replication

Note: Any other applications DR recovery actions (SDS and IDIH) may occur in parallel. These actions can/should be worked simultaneously; doing so would allow faster recovery of the complete solution (i.e. stale DB on DP servers will not receive updates until SDS-SOAM servers are recovered. Refer to **Table 8** IDIH Disaster Recovery Reference Table for IDIH 5.0/6.0/7.0 disaster recovery and **Section 7.0** for 7.1

S T F	This procedure performs recovery if both NOAM servers are failed and all SOAM servers are failed. This procedure also caters the C-Level Sever failure		
Р #	Check off (√) each step number.	n step as it is completed. Boxes have been provided for this purpose under each	
	If this procedure fa	ails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.	
1	Workarounds	Refer to Appendix G . Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.	
2	Gather Required Materials	r Gather the documents and required materials listed in Section 3.1 Required red Materials ials	
3	RMS NOAM Failure	If the failed server is a rack mount server based NOAM, execute this step; otherwise skip to the next step .	
		1. HW vendor to replace the failed equipment	
		2. Execute the "iLO Configuration Procedure" appendix from [3]	
		3. Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6 : DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference.	
		4. Confirm necessary software images are present on the PMAC.	
		 If the failed NOAM is co-hosted with the PMAC on the first rack mount server, execute procedure "Continue TVOE Configuration on First RMS Server" - Refer to Table 5 for the applicable DSR software installation/configuration guide reference. 	
		 If the failed NOAM is NOT co-hosted with the PMAC on the first rack mount server, execute procedure "Configure TVOE on Additional RMS Servers(s)" - Refer to Table 5 for the applicable DSR software installation/configuration guide reference. 	

4	HP-Class Blade	If the failed server is an HP C-Class Blade, execute this step; otherwise skip to	
	Fallure	the next step.	
		1. HW vendor to replace the failed equipment	
		 Execute procedure "Confirm/Update blade Server BIOS Settings" – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 	
		 Execute procedure "Configure Blade Server iLO Password for Administrator Account" – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 	
		 Perform any needed firmware upgrades – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 	
		 For NOAM/SOAM servers, execute procedure "IPM Servers Using PM&C Application" - Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 	
5	Configure TVOE on Server Blades	For NOAMs on TVOE server Blades and SOAMs, execute procedure "Configure TVOE on Server Blades" - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.	
6	Create VMs	For NOAMs, execute procedure <i>"Create NOAM Guest VMs"</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.	
		For SOAMs, execute procedure <i>"Create SOAM Guest VMs"</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.	
7	IPM Failed Guest/Servers	IPM the failed guests/servers by executing procedure <i>"IPM Blades and VMs"</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.	
8	Install DSR application on Failed Guests/Servers	Install the DSR application on the failed guests/server by executing procedure <i>"Install Application Software on Blades"</i> - Refer to Table 5 for the applicable DSR software installation and configuration reference.	
9	Repeat for Remaining Failed Servers	If necessary, repeat steps 1-7 for all remaining failed servers.	
10	Install NetBackup Client (Optional)	If NetBackup is used execute procedure <i>"Install NetBackup Client (Optional)"</i> - Refer to Table 5 for the applicable DSR software installation and configuration reference.	

11	Obtain Latest Database Backup and Network Configuration	Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. From required materials list in Section 3.1 Required Materials; use site survey documents and Network Element report (if available), to determine
	Dala.	network configuration data.
12	Execute DSR	Verify the networking data for Network Elements
	Procedure for the First NOAM	Note: Use the backup copy of network configuration data and site surveys (Step 2)
		Configure the first NOAM server by executing procedure "Configure the First NOAM NE and Server" - Refer to Table 5 for the applicable DSR software installation and configuration reference.
		Configure the NOAM server group by executing procedure <i>"Configure the NOAM Server Group"</i> - Refer to Table 5 for the applicable DSR software installation and configuration reference
13	NOAM GUI: Login	Login to the NOAM GUI as the <i>guiadmin</i> user:
		Oracle System Login ————————————————————————————————————
		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.
		Other names may be trademarks of their respective owners.

14	NOAM GUI:	Browse to Main Menu->Status & Manage->Files
	Upload the	
	Backed up	📋 🚔 Status & Manage
	Database File	🔤 💽 Network Elements
		Server 💽 Server
		💽 HA
		📑 Database
		📑 KPIs
		📑 Processes
		🔁 🧰 Tasks
		👘 📲 Files
		Select the Active NOAM server. The following screen will appear:
		File Name Size Type Timestamp
		Backup.dsr.Cpa1-N0.Configuration.NETWORK_OAMP.20120321_021501.AUTO.tar KB tar 2012-03-21 06:15:02 UTC
		Click on Upload as shown below and select the file "NO Provisioning and
		Configuration:" file backed up after initial installation and provisioning.
		Delete View Upload Download Pause U
		0 used (0%) of 0 available System utilization: 0 (0%) of 0 available.
		Click on Browse and locate the backup file and click on Open as shown below
		File:
		Browse
		Upload
		Cancel
		Look in: PV3
		Backup EAGLEV pelCOMProv.tgz
		My Recent F 73, NetHawk.bt
		Cocuments Revealed Re
		Desktop
		My Documents
		My Computer
		My Network File name: Backup.PV31gz
		Click on the Unload button. The file will take a few seconds to unload
		depending on the size of the backup data. The file will be visible on the list of
		entries after the upload is complete.

15	NOAM GUI:	Click on Main Menu->Status & Manage->Database
	Disable Provisioning	 Status & Manage Network Elements Server Replication Collection HA Database KPIs Processes
		Files Disable Provisioning by clicking on Disable Provisioning button at the bottom of the screen as shown below. Disable Provisioning Report Inhibit/Allow Backup Compare Restore A confirmation window will appear, press OK to disable Provisioning.
		Message from webpage Image: Disable provisioning. Are you sure? Image: OK Cancel The message <i>"Warning Code 002"</i> will appear.

16 NOAM GUI:	Select the Active NOAM server and click on the Compare.
Archive	Enable Provisioning Report Inhibit Replication Backup Compare Restore Man Audit Suspend Auto Audit
Contents and Database Compatibility	The following screen is displayed; click the button for 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.ngr.blade02 Configuration NETWORK_OAMP.20100928_021502.AUTO tar
	Clascup noprobade02 continguration NETWORK_OAMP 20100920 201501 AUTO tar Clascup noprobade02 continguration NETWORK_OAMP 20100100 201501 AUTO tar Clascup noprobade02 contiguration NETWORK_OAMP 20101001 021501 AUTO tar Clascup noprobade02 contiguration NETWORK_OAMP 20101002 021502 AUTO tar Clascup noprobade02 contiguration NETWORK_OAMP 20101003 021502 AUTO tar Clascup noprobade02 contiguration NETWORK_OAMP 20101003 021502 AUTO tar Clascup noprobade02 contiguration NETWORK_OAMP 20101004 021502 AUTO tar Clascup noprobade02 contiguration NETWORK_OAMP 20101004 021502 AUTO tar Clascup noprobade02 contiguration NETWORK_OAMP 20101004 021502 AUTO tar
	Old Cancel
	Verify that the output window matches the screen below.
	Note: You will get a database mismatch regarding the NodeIDs of the blades. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix H. My Oracle Support (MOS) and ask for assistance.
	The selected database came from blade07 on 01/192011 at 13.43.47 EDT and contains the following comment:
	Acative Contents ProvisioningAnaConfiguration data
	Stational Contrastition Ter distances are compatible. Station Time Contrastition Station Time Contrastition Termonithme
	Statistics Consultation Total Commentation The TOPOLOGYTS HOT COMPATIBLE. CONTACT TERELEC CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE.
	Discrepancies: - IHI Server Address A318 120 has different <u>foode IDB</u> in current topology and the selected backup file. Current node ID: A318 120. Selected backup file node ID: B2073.007 - IHI Server Address C157 241 has different <u>food</u> . TDB in current topology and the selected backup file. Current node ID: C1157 241. Selected backup file node ID: B2073.007 - IHI Server Address B107 161 has different <u>food</u> . TDB in current topology and the selected backup file. Current node ID: B1707.161, Selected backup file node ID: B2073.007
	User Compatibility The user and authentication data are compatible. Contents Contents
	ProvisionnyAndConfiguration ProvisionnyAndConfiguration ProvisionnyAndConfiguration Control Additionation Configuration Control Additionationation Configuration Control Additionationation Configuration Control Additionationation Configuration Control Additionationation Control Additionationation Control Additionationation Control Additionationation Control Additionationation Control Additionation Control Additionation Control Additionationation Control Additionationation Control Additionationation Control Additionationation Control Additionationation Control Additionationation Control Additionation Control Additionationation Control Additionation
	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 NOAM:
	Topology Compatibility THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.
	Note: We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility.
	If the verification is successful, Click BACK button and continue to next step in this procedure.
Page 26	E57520-02

17	ACTIVE NOAM: Restore the	Click on Main Menu->Status & Manage->Database
	Database	Select the Active NOAM server, and click on Restore as shown below.
		The following screen will be displayed. Select the proper back up provisioning and configuration file.
		Select archive to Restore on server: blade02
		Archive Backup npgrblade02.configuration NETWORK_OAMP.20100320_021501.AUTO.tar Backup npgrblade02.configuration NETWORK_OAMP.2010030_021501.AUTO.tar Backup npgrblade02.configuration NETWORK_OAMP.20101002_021502.AUTO.tar Backup npgrblade02.configuration NETWORK_OAMP.20101002_021502.AUTO.tar Backup npgrblade02.configuration NETWORK_OAMP.20101003_021502.AUTO.tar Backup npgrblade02.configuration NETWORK_OAMP.20101003_021502.AUTO.tar Backup npgrblade02.configuration NETWORK_OAMP.20101003_021502.AUTO.tar Backup npgrblade02.configuration NETWORK_OAMP.20101005_021501.AUTO.tar
		Ok Cancel
		Click OK Button. The following confirmation screen will be displayed.
		If you get an error that the NodelDs do not match. That is expected. If no other errors beside the NodelDs are displayed, select the Force checkbox as shown above and Click OK to proceed with the DB restore.
		Database Restore Confirm
		Incompatible database selected
		Discrepancies: - 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: B1787.161 Selected backup file node ID: B2073.087 - Wirent node ID: B1787.161 Selected backup file node ID: B2073.087
		Confirm archive "3bladeNPQR.blade07.configuration.NETWORK_OAMP.20110119_184253.MAN.Lar" to Restore on server: blade07 Force Restore? Force restore on blade07, despite compare errors. In the sectore of the sectore o

18	NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: <pre>http://<primary_noam_vip_ip_address></primary_noam_vip_ip_address></pre> Login as the guiadmin user:
		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.
19	NOAM VIP GUI: Monitor and Confirm database restoral	 Wait for 5-10 minutes for the System to stabilize with the new topology: Monitor the Info tab for "Success". This will indicate that the backup is complete and the system is stabilized. Following alarms must be ignored for NOAM and MP Servers until all the Servers are configured: Alarms with Type Column as "REPL", "COLL", "HA" (with mate NOAM), "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 will be in the same state it was backed up during initial backup.
20	ACTIVE NOAM: Login	Login to the recovered Active NOAM via SSH terminal as root (5.0) or admusr(6.0+) user.

	ACTIVE NOAM:	IF DSR 7.1, SKIP THIS STEP
21	Restore	,
	/etc/hosts/ File	Execute the following command:
	of the Active	
	NOAM (DSR	<pre>\$ sudo AppWorks AppWorks_AppWorks updateServerAliases</pre>
	5.0/6.0/7.0	<noam host="" name=""></noam>
	ONLY)	
22	NOAM VIP GUI:	Install the second NOAM server by executing procedure "Configure the Second
	Recover	NOAM Server", steps 1, 4, 5, 6 - Refer to Table 5 for the applicable DSR
	Standby NOAM	software installation and configuration reference.
		Note: Execute step 7 if Netbackup is used.
		If NetBackup is used, execute procedure <i>"Install NetBackup Client"</i> - Refer to Table 5 for the applicable DSR software installation and configuration reference.
		Note: If Topology or nodeld alarms are persistent after the database restore, refer to Appendix G . Workarounds for Issues not fixed in this Release
23	NOAM VIP GUI:	Navigate to Main Menu->Status & Manage->Server,
25	Restart DSR	🚊 🚔 Status & Manage
	application	 Status & Manage Network Elements Server HA Database M Processes Tasks Files
		Select the recovered standby NOAM server and click on Restart .
		Stop Restart Reboot NTP Sync Report

24	NOAM VIP GUI:	Navigate to Status & Manage -> HA
	Set HA on Standby NOAM	Select the standby NOAM server, set it to Active Press OK
25	NOAM VIP GUI: Stop Replication to the C-Level Servers of this Site.	Inhibit Replication to the working C Level Servers which belong to the same site as of the failed SOAM servers, as the recovery of Active SOAM will cause the database wipeout in the C level servers because of the replication Execute Appendix E. Inhibit A and B Level Replication on C-Level Servers
26	NOAM VIP GUI: Recover Active SOAM Server	Install the SOAM servers by executing procedure <i>"Configure the SOAM Servers"</i> , steps 1-3, and 5-8 Refer to Table 5 for the applicable DSR software installation and configuration reference.
		Note: If you are using Netbackup, also execute step 11.

	NOAM VIP GUI	Navigate to Main Menu->Status & Manage->Files
27	Linload the	
	backed up	Select the Active SOAM server. The following screen will appear. Click on
	SOAM	Upload as shown below and select the file "SO Provisioning and Configuration:"
	Database file	file backed up after initial installation and provisioning.
		Delete View Upload Download Pause U
		0 used (0%) of 0 available System utilization: 0 (0%) of 0 available.
		Click on Browse and Locate the backup file and click on Open as shown below.
		8
		File:
		Browse
		Upload
		Cancel
		Lookin: PV3 V © P
		Backup EAGLEV/pelCOMProv.tgz
		My Recent Documente
		Desktop
		My Documents
		My Computer
		Nu Malmath File name Rackup FV3 Inz
		Places Files of type: All Files (".") Cancel
		Click on the Upload button. The file will take a few seconds to upload
		depending on the size of the backup data. The file will be visible on the list of
		entries after the upload is complete.

28	Recovered SOAM GUI: Login	Establish a GUI session on the recovered SOAM server. Open the web browser and enter a URL of: http:// <recovered_soam_ip_address> Login as the <i>guiadmin</i> user:</recovered_soam_ip_address>
		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.

29	Recovered	Click on Main Menu->Status & Manage->Database
	Verify the	Select the Active SOAM server and click on the Compare.
	Contents and	Enable Provisioning Report Inhibit Replication Backup Compare Restore Man Audit Suspend Auto Audit
	Database Compatibility	The following screen is displayed; click the button for 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 Claackup.nogr.blade02.configuration.NETWORK_OAMP.20100928_021502.AUT0.tar
		Clackup nopt blade02 configuration NETWORK_OAMP 20100929_021501 AUTO tar Backup nopt blade02 configuration NETWORK_OAMP 20100930_021501 AUTO tar Clackup nopt blade02 configuration NETWORK_OAMP 20101000_021502 AUTO tar Backup nopt blade02 configuration NETWORK_OAMP 20101003_021502 AUTO tar
		CBackup.npqr.blade02.Configuration.NETWORK_OAMP.20101005_021501.AUTO.tar*
		Verify that the output window matches the screen below.
		Note: You will get a database mismatch regarding the NodeIDs of the blades.
		That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix H. My Oracle Support (MOS)
		The selected database care from blase(07 on 0118/2011 at 13.43.47 EDT and contains the following comment:
		Pointenangenacionale autoritaria Pointenana Companhiana The distatases are compatible. The distatases are compatible.
		Hode Tops Compatibility Top code processor Top code procesor Top code processor Top code processor Top code proc
		THE TOPCOOPY SHOT COMPARELE CONTACT TRELECONTONER NEWCES BUYOR HIS CONTACT HIS CALAMAKE. Discreptancies: - Hill Server Address A3118.120 has different foode IDB in current topology and the selected backup file.
		Current node ID A110 120. Selected backup file mode ID E007.007 - BH Server Address (157:241 has different (<u>obce BB</u>) in current topology and the selected backup file. Current node ID C157:244. Selected backup file node ID E0073.007 - BH Server Address B107:161 has different (<u>obce BB</u>) in current topology and the selected backup file. Current node ID. B1787:161. Selected backup file node ID: E0073.007
		Usar Compatibility The user and suffering compatible. The user and suffering compatible. Order details
		Provisions/endConfiguration Table Institute Configuration Control Addressort 0
		Current AdjacentServers count: 0 Elektica: 0 Current AdjacentServers count: 0 Elektica: 0 Current Association count: 0 Elektica: 0 Current Association Count: 0 Elektica: 0 Current Association Count: 0 Elektica: 0
		Current Authorizedity count, 1 Selecter, 1
		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 SOAM:
		Topology Compatibility THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.
		Note: We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility.
		If the verification is successful, Click BACK button and continue to next step in this procedure.
Page	33	E57520-02

	D	I I I I I I I I I I I I I I I I I I I
30	Recovered SOAM GUI:	Select the Active SOAM server, and click on Restore as shown below.
	Restore the	
	Database	The following screen will be displayed. Select the proper back up provisioning
		and configuration file.
		Database Restore
		Select archive to Restore on server: blade02
		Archive Backup ngrct biade02. Configuration NETWORK_OAMP.20100928_021502 AUTO.tar Backup ngrct biade02. Configuration NETWORK_OAMP.20100930_021501 AUTO.tar Backup ngrct biade02. Configuration NETWORK_OAMP.20101001_021501 AUTO.tar Backup ngrct biade02. Configuration NETWORK_OAMP.20101001_021501 AUTO.tar Backup ngrct biade02. Configuration NETWORK_OAMP.20101003_021502 AUTO.tar Backup ngrct biade02. Configuration NETWORK_OAMP.20101003_021502 AUTO.tar Backup ngrct biade02. Configuration NETWORK_OAMP.20101004_021502 AUTO.tar Backup ngrct biade02. Configuration NETWORK_OAMP.20101004_021502 AUTO.tar Backup ngrct biade02. Configuration NETWORK_OAMP.20101004_021502 AUTO.tar
		Ok] (Cancel
		Click OK Button. The following confirmation screen will be displayed.
		If you get an error that the NodelDs do not match. That is expected. If no other errors beside the NodelDs are displayed, select the Force checkbox as shown above and Click OK to proceed with the DB restore.
		Database Restore Confirm
		Discrepancies: - 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: B1787.161 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, despile compare errors.
		Ok Cancel
		Note: After the restore has started, the user will be logged out of XMI SOAM GUI since the restored Topology is old data.
31	Recovered	Wait for 5-10 minutes for the System to stabilize with the new topology:
	Monitor and	Monitor the Info tab for " Success " This will indicate that the backup is
	Confirm	complete and the system is stabilized.
	database restoral	Note: Do not pay attention to alarms until all the servers in the system are completely restored.
		Note: The Configuration and Maintenance information will be in the same state it was backed up during initial backup.

32	NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: <pre>http://<primary_noam_vip_ip_address></primary_noam_vip_ip_address></pre> Login as the guiadmin user:
		Oracle System Login
		Log In
		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.
33	NOAM VIP GUI:	Recover the remaining SOAM servers (standby , spare) by repeating the following stops for each SOAM server:
	Remaining	1 Install the remaining SOAM earliers by even ting reference Dreadure
	SOAM Servers	<i>"Configure the SOAM Servers"</i> , steps 1-3, and 5-8 Refer to Table 5 for the applicable DSR software installation and configuration reference.
		Note: Execute step 11 as well if Netbackup is used.
		 If you are using Netbackup, execute procedure "Install Netbackup Client" - Refer to Table 5 for the applicable DSR software installation and configuration reference.

34	NOAM VIP GUI: Restart DSR application	Navigate to Main Menu->Status & Manage->Server, Status & Manage Network Elements Server HA Database KPIs Processes Tasks				
		Select the recovered standby SOAM server and click on Restart . Stop Restart Reboot NTP Sync Report				
35	NOAM VIP GUI: Set HA on Standby SOAM	Navigate to Status & Manage Status & Manage Network Elements Server Database KPIs Processes Tasks Files Click on Edit at the bottom of the screen Select the standby SOAM server, set it to Active Press OK				
36	NOAM VIP GUI: Start Replication	Un-Inhibit (<i>Start</i>) Replication to the working C-Level Servers which belong to the same site as of the failed SOAM servers.				
----	--	--	--	--	--	--
	Level Servers	Execute Appendix F. Un-Inhibit A and B Level Replication on C-Level Servers				
		If the <i>"Repl Status"</i> is set to "Inhibited", click on the Allow Replication button as shown below using the following order, otherwise if none of the servers are inhibited, skip this step and continue with the next step:				
		 Active NOAM Server Standby NOAM Server Active SOAM Server Standby SOAM Server Spare SOAM Server (<i>if applicable</i>) Active DR NOAM Server 				
		 Standby DR NOAM Server MP/IPFE Servers (if MPs are configured as Active/Standby, start with the Active MP, otherwise the order of the MPs does not matter) SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare) 				
		Verify that the replication on all the working servers is allowed. This can be done by clicking on each server and checking that the button below shows "Inhibit Replication", and NOT "Allow Replication".				
		Disable Provisioning Report (Allow Replication) Backup Compare Restore				
37	NOAM VIP GUI: Recover the C- Level Server (DA-MP, SBRs, IPEE SS7-MP)	Execute procedure <i>"Configure MP Blades Servers"</i> , Steps 1, 5, 6, 7, 8, and 9 Refer to Table 5 for the applicable DSR software installation and configuration reference.				
	IFFE, 337-WF)	Note: Also execute step 10 and 11 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.				
		Note: – DSR 5.0/6.0/7.0 ONLY : If this server is an IPFE server, ensure ipfeNetUpdate.sh from procedure <i>"IP Front End (IPFE) Configuration (Optional)"</i> from [17] has been executed.				
		Repeat this step for any remaining failed MP servers.				

38	NOAM VIP GUI:	Navigate to Main Menu->Status & Manage->Server
	Application on recovered C- Level Servers.	Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered C-Level servers and click on Restart.

20	NOAM VIP GUI:	Un-Inhibit (Start) Replication to the ALL C-Level Servers
39	Start replication	
	on all C-Level Servers	Navigate to Status & Manage -> Database
		💼 🚍 Status & Manage
		🔤 💽 Network Elements
		💽 Server
		💽 HA
		👘 💽 Database
		💽 KPIs
		🔤 🔤 Processes
		🖬 🧰 Tasks
		Files
		If the <i>"Repl Status"</i> is set to "Inhibited", click on the Allow Replication button as
		shown below using the following order:
		Active NOAM Server
		Standby NOAM Server
		Active SOAM Server
		Standby SOAM Server
		Spare SOAM Server (if applicable)
		Active DR NOAM Server Standby DP NOAM Server
		MP/IPEE Servers (if MPs are configured as Active/Standby, start with
		the Active MP, otherwise the order of the MPs does not matter)
		Verifie the table continue on all concerns in allowed. This can be done her allowed
		on each server and checking that the button below shows "Inhibit Replication"
		and NOT "Allow Replication".
		••••
		Disable Provisioning Report (Allow Replication) Backup Compare Restore

40	NOAM VIP GUI:	Navigate to Status & Manage -> HA
	Set HA on all C-	🚔 🗖 Ctatus 8. Manago
	Level Servers	
		🔤 💽 Network Elements
		🚽 🔤 Server
		🖌 🖉 🕂 🤯 HA
		🖉 🖬 Database
		KPIs
		🔚 🛄 Files
		Click on Edit at the bottom of the screen
		For each server whose Max Allowed HA Role is set to Standby, set it to Active
		Brood OK
41	ACTIVE NOAM:	Establish an SSH session to the Active NOAM, login as admusr.
-	Perform key	
	exchange	Execute the following command to perform a keyexchange from the active
	active-NOAM	NOAM to each recovered server.
	and recovered	<pre>\$ keyexchange admusr@<recovered hostname="" server=""></recovered></pre>
	servers.	
		Note: If an export server is configured, perform this step.
42	ACTIVE NUAM:	Establish an SSH session to the active NUAM, login as admusr.
	Optional	Refer to section
	Features	1.5 Optional Featuresto activate any features that were previously activated.



44	ACTIVE NOAM: Verify	Login to the Active NOAM via SSH terminal as <i>root(5.0) or admusr(6.0+)</i> user. Execute the following command:								
	Replication	¢ auda inanatat m								
	Between	Ş sudo irepstat -m								
	Gervers.									
		Output like below shall be generated:								
		Policy 0 ActStb [DbReplication]								
		Oahu-DAMP-1 Active								
		BC From Oahu-SOAM-2 Active 0 0.50 ^0.15%cpu 25B/s A=me								
		CC To Oahu-DAMP-2 Active 0 0.10 0.14%cpu 25B/s A=me								
		Oahu-DAMP-2 Stby								
		BC From Oahu-SOAM-2 Active 0 0.50 ^0.11%cpu 31B/s A=C3642.212								
		CC From Oahu-DAMP-1 Active 0 0.10 ^0.14 1.16%cpu 31B/s A=C3642.212								
		Oahu-IPFE-1 Active								
		BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 24B/s A=C3642.212								
		Oahu-IPFE-2 Active								
		BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 28B/s A=C3642.212								
		Oahu-NOAM-1 Stby								
		AA From Oahu-NOAM-2 Active 0 0.25 ^0.03%cpu 23B/s								
		Oahu-NOAM-2 Active								
		AA To Oahu-NOAM-1 Active 0 0.25 1%R 0.04%cpu 61B/s								
		AB To Oahu-SOAM-2 Active 0 0.50 1%R 0.05%cpu 75B/s								
		Oahu-SOAM-1 Stby								
		BB From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 27B/s								
		Danu-SOAM-2 Active								
		AB From Oanu-NOAM-2 Active 0 0.50 %0.03%cpu 24B/s								
		BE TO CANU-SCAN-I ACCIVE 0 0.50 16K 0.046 CPU 52B/S								
		BC To $Oabu=SS7MP=2$ Active $0 = 0.50$ 1%R 0.04 %cpu 21B/S								
		irepstat (40 lines) (h)elp (m)erged								

45	NOAM VIP GUI:	Click on Main Menu->Status and Manager->Database											
	Verify the	📩 💼 Chatus & Manago											
	Database states	📮 🦐 Status & Manage											
		💽 N	🔤 🔤 Network Elements										
		Server											
		💓 H	A										
		🚮 🖸	ataba	ise									
			DIe										
			P15										
		💽 P	roces	ses									
		Verify that the	"OAM	Max	HA Ro	ole" is eith	her "A	ctive"	or "S	tandb	v" for		М
		and SOAM an	d "Anr	licatio	n May		" for	MPs	is "Ac	tive" a	and th	at the	
		status is "Norr	nal" as	show	n helc		101		0 / 10				,
				01101									
							Application				SIG Reni	Roni	Rent Audit
		Network Element Se	rver		Role	HA Role	Max HA Role	Status	DB Level	Status	Status	Status	Status
		NO_10303 NO	02		Network OAM8	P Active	008	Normal	0	Normal	NotApplica	bl Allowed	AutoInProg
		SO_10303 PS SO_10303 MF	BR 22		MP MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg
		SO_10303 SC	~)1		System OAM	Standby	005	Normal	0	Normal	NotApplica	bl Allowed	AutoInProg
l		NO_10303 NO	D1		Network OAM8	P Standby	00S	Normal	0	Normal	NotApplica	bl Allowed	AutoInProg
		SO_10303 IPI SO 10303 SO	-E)2		MP System OAM	Active	005	Normal	0	Normal	Normal	Allowed bl Allowed	AutoInProg
		-											-
10	NOAM VIP GUI:	Click on Main Menu->Status and Manage->HA											
46	Verify the HA	č											
	Status	💼 🚔 Stat	us & N	lanad	ie								
		🔤 🦉 Server											
		💓 D	ataba	se									
		🔤 K	PIs										
		- E 🔤 🔤 P	roces	ses									
		Select the row	for all	of the	eserve	ers							
		Verify that the	"HA F	lole" is	s eithe	r "Active"	or "S	Standt	<i>эу″</i> .				
				8									
		Hostname	OAM Max HA Role	Max HA	Allowed HA	Mate Hostname Li	st Netwo	rk Element		Server Ro	le .	Active VIPs	
		NO2	Active	OOS	Active	NO1	NO_10	303		Network O	AM&P	10.240.70.13	2
		SO1	Standby	OOS	Active	SO2	SO_10	303		System O/	AM		
		SO2 MP1	Active	OOS Active	Active	SO1 MP2	SO_10	303 303		System O/	AM	10.240.70.13	3
		MP2	Active	Active	Active	MP1	SO_10	303		MP			
		IPFE	Active	005	Active		SO_10	303		MP			

47	NOAM GUI:	Click on Main Menu->Status & Manage->Database
47	Enable	
	Provisioning	🚊 🚖 Status & Manage
		🔤 📑 Network Elements
		🔤 🎆 Server
		Replication
		Collection
		HA HA
		Database
		KPIs
		Processes
		Eles
		Enable Provisioning by clicking on Enable Provisioning button at the bottom of the screen as shown below.
		Enable Provisioning Report Inhibit/Allow Replication Backup Compare Restore Man Audit Suspend Auto Audit
		A confirmation window will appear, press OK to enable Provisioning.
		Enable provisioning. Are you sure?
		OK Cancel
	1	





	SOAM VIP GUI:	Navigate to Main Menu->Diameter->Maintenance->Connections
52	Enable	
	Connections if needed	Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups Applications DA-MPs Select each connection and click on the Enable button. Alternatively you can enable all the connections by selecting the EnableAll button. Image: Imable Disable Imable Disable Imable Disable Imable Note: If a Disaster Recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution
53	SOAM VIP GUI:	Navigate to Main Menu -> Diameter -> Maintenance -> Applications
	Enable Optional Features	Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups Applications DA-MPs Select the optional feature application configured in step 42. Click the Enable button. Enable Disable Pause updates

54	SOAM VIP GUI:	Navigate to Main Menu->Transport Manager -> Maintenance -> Transport
	Re-enable Transports if Needed (Applicable	 Transport Manager Configuration Maintenance
	ONLY for DSR 6.0+)	Transport
		Select each transport and click on the Enable button
		Enable Disable Block
		Verify that the Operational Status for each transport is Up.
55	Re-enable	Navigate to Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users
	application if needed (Applicable ONLY for DSR	SS//Sigtran Configuration Configuration Cocal SCCP Users Remote Signaling Points Remote MTP3 Users
	6.0+)	Links
		Click on the Enable button corresponding to MAPIWF Application Name.
		Enable Disable
		Verify that the SSN Status is Enabled.
56	SOAM VIP GUI: Re-enable links if needed (Applicable ONLY for DSR 6.0+)	Navigate to Main Menu->SS7/Sigtran->Maintenance->Links
		Click on Enable button for each link.
		Enable Disable Verify that the Operational Status for each link is Up.

57	Active NOAM:	If recovering a DSR 5.0/6.0 system and POLICY AND CHARGING DRA
	Scope Data (If	application is activated then execute this step.
	POLICY AND CHARGING	Note: If recovering a DSR 7.0+ system, DO NOT execute this step
	DRA is activated):	Login to the Active NOAM VIP via SSH terminal as <i>root(5.0) or admusr(6.0+)</i> user.
	5.0/0.0 Only	Execute the following steps:
		Go to Appworks bin directory:
		<pre>\$ sudo cd /usr/TKLC/appworks/bin/</pre>
		Execute the PCRF sync script in "reportonly" mode to check whether PCRF data syncing is required or not. This is a read-only mode that does not modify the database:
		<pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -reportonly</pre>
		If the Report Summary shows one or more PCRFs "need to be synced", then repeat the script execution again but using the "sync" option instead of "reportonly" in order to sync the database.
		The "sync" option will modify the database:
		<pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -sync</pre>
		Re-execute the PCRF sync script in "reportonly" mode to verify all PCRF data is in sync. Examine the Report Summary output of the script. Verify the number of "PCRF record(s) processed in "total" is equal to the number of "PCRF record(s) already in sync":
		<pre>\$ sudo./syncPcrfReferencesAfterRestore.sh -reportonly</pre>
	SOAM VIP GUI:	Navigate to Main Menu->Alarms & Events->View Active
58	Examine All	
	Alarms	 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 peeded contact Appendix H. My Oracle Support (MOS)

59	NOAM VIP GUI: Examine All Alarms	Login to the NOAM VIP if not already 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 Appendix H. My Oracle Support (MOS).				
60	Restore GUI Usernames and Passwords	If applicable, Execute steps in Section 6.0 to recover the user and group information restored.				
61	Backup and Archive All the Databases from the Recovered System	Execute Appendix A . DSR Database Backup to back up the Configuration databases:				

5.1.2 Recovery Scenario 2 (Partial Server Outage with one NOAM server intact and both SOAMs failed)

For a partial server outage with an NOAM server intact and available; SOAM servers are recovered using recovery procedures of base hardware and software and then executing a database restore to the active SOAM server using a database backup file obtained from the SOAM servers. All other servers are recovered using recovery procedures of base hardware and software. Database replication from the active NOAM server will recover 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 execute the procedure. The actual procedures' detailed steps are in **Procedure 2**. The major activities are summarized as follows:

Recover Standby NOAM server (*if needed*) by recovering base hardware, software and the database.

- Recover the base hardware.
- Recover the software.

Recover Active SOAM server by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.
- Recover the Database.

Recover any failed **SOAM and MP** servers by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.
- The database has already been restored at the active SOAM server and does not require restoration at the SO and MP servers.

Note: Use the release document matrix from **Section 3.1.1** Release Document Matrixto determine which document is referenced for the applicable DSR release.

S T E	This procedure pe site have failed. T	rforms recovery if at least 1 NOAM server is available but all SOAM servers in a his includes any SOAM server that is in another location.					
– P #	Check off (√) each step number.	each step as it is completed. Boxes have been provided for this purpose under each					
	If this procedure fa	ails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.					
1	WorkaroundsRefer to Appendix G. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.						
2	Gather Required Materials	Gather the documents and required materials listed in Section 3.1 Required Materials					
3	NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:					
		http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>					
		Login as the <i>guiadmin</i> user:					
		ORACLE					
		Oracle System Login					
		Log In Enter your username and password to log in					
		Username: guiadmin					
		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.					

4	Active NOAM:	Navigate to Main Menu -> Status & Manage -> HA
	Set Failed Servers to Standby	 Status & Manage Network Elements Server HA Database KPIs Processes
		Select Edit
		Set the Max Allowed HA Role drop down box to Standby for the failed servers.
		Select Ok
		Ok Cancel
5	RMS NOAM	1. HW vendor to replace the failed equipment
	Failure	2. Execute the "iLO Configuration Procedure" appendix from [3]
		 Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference.
		4. Confirm necessary software images are present on the PMAC.
		 If the failed NOAM is co-hosted with the PMAC on the first rack mount server, execute procedure "Continue TVOE Configuration on First RMS Server" - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.
		 If the failed NOAM is NOT co-hosted with the PMAC on the first rack mount server, execute procedure <i>"Initial Product Manufacture of</i> <i>Application Server"</i> - Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR software installation/configuration guide reference.
		Now execute procedure <i>"Configure TVOE on Additional RMS Servers(s)"</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.

6	HP-Class Blade Failure	If the failed server is an HP C-Class Blade, execute this step; otherwise skip to the next step.
		1. HW vendor to replace the failed equipment
		 Execute procedure "Confirm/Update blade Server BIOS Settings" – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference.
		 Execute procedure "Configure Blade Server iLO Password for Administrator Account" – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference.
		 Perform any needed firmware upgrades – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference.
		 For NOAM/SOAM servers, execute procedure <i>"IPM Servers Using PM&C Application"</i> - Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference.
6	RMS NOAM	1. HW vendor to replace the failed equipment
	Failure	2. Execute the <i>"iLO Configuration Procedure"</i> appendix from [3]
		 Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference.
		4. Confirm necessary software images are present on the PMAC.
		 If the failed NOAM is co-hosted with the PMAC on the first rack mount server, execute procedure "Continue TVOE Configuration on First RMS Server" - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.
		 If the failed NOAM is NOT co-hosted with the PMAC on the first rack mount server, execute procedure <i>"Initial Product Manufacture of</i> <i>Application Server"</i> - Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR software installation/configuration guide reference.
		Now execute procedure <i>"Configure TVOE on Additional RMS Servers(s)"</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.

7	Configure TVOE on Server Blades	For NOAMs on TVOE server Blades and SOAMs, execute procedure "Configure TVOE on Server Blades" - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.
8	Create VMs	For NOAMs, execute procedure <i>"Create NOAM Guest VMs"</i> - Refer to Table 5 for the applicable DSR software installation and configuration reference.
		For SOAMs, execute procedure <i>"Create SOAM Guest VMs"</i> - Refer to Table 5 for the applicable DSR software installation and configuration reference.
9 □	IPM Failed Guest/Servers	IPM the failed guests/servers by executing procedure <i>"IPM Blades and VMs"</i> - Refer to Table 5 for the applicable DSR software installation and configuration reference.
10 □	Install DSR application on Failed Guests/Servers	Install the DSR application on the failed guests/server by executing procedure <i>"Install Application Software on Blades"</i> - Refer to Table 5 for the applicable DSR software installation and configuration reference.
11	Repeat for Remaining Failed Servers	If necessary, repeat steps 1-7 for all remaining failed servers.
12	NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:
		http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>
		Login as the <i>guiadmin</i> 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: ••••••
		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.

Page | 55

13	NOAM VIP GUI: Recover Standby NOAM	Install the second NOAM server by executing procedure "Configure the Second NOAM Server", steps 1, 2, 4-6, and 8 - Refer to Table 5 for the applicable DSR software installation and configuration reference. Note: Execute step 7 if Netbackup is used. If NetBackup is used, execute procedure "Install NetBackup Client" - Refer to Table 5 for the applicable DSR software installation and configuration reference.
	NOAM VIP GUI: Restart DSR application	Navigate to Main Menu->Status & Manage Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered standby NOAM server and click on Restart. Stop Restart Reboot NTP Sync Report
	NOAM VIP GUI: Set HA on Standby NOAM	Navigate to Status & Manage -> HA Status & Manage Network Elements Server Database KPIs Processes Files Click on Edit at the bottom of the screen Select the standby NOAM server, set it to Active Press OK

	NOAM VIP GUI: Stop Replication to the C-Level Servers of this Site.	Inhibit Replication to the working C Level Servers which belong to the same site as of the failed SOAM servers, as the recovery of Active SOAM will cause the database wipeout in the C level servers because of the replication Execute Appendix E . Inhibit A and B Level Replication on C-Level Servers
17	NOAM VIP GUI: Recover Active SOAM Server	 Install the First SOAM server by executing procedure "Configure the SOAM Servers", steps 1-3, 5-8 Refer to Table 5 for the applicable DSR software installation and configuration reference. Note: If you are using Netbackup, also execute step 10.
	NOAM VIP GUI: Restart DSR application	Navigate to Main Menu->Status & Manage Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered Active SOAM server and click on Restart. Stop Restart Reboot NTP Sync Report



		Novigoto to Main Manu - Status & Managa - Eilas
20	NUAN VIF GUI.	Navigale lo main menu->Slalus & manage->rnes
		Select the Active SOAM convert The following coreen will enneer. Click on
		Select the Active SOAM server. The following screen will appear. Click on
	SUAM Database ("ba	Upload as shown below and select the file SO Provisioning and Configuration.
	Database file	file backed up after initial installation and provisioning.
		Delete View Upload Download Pause U 0 used (0%) of 0 available System utilization: 0 (0%) of 0 available.
		Click on Browse and Locate the backup file and click on Open as shown below.
		۵
		File:
		Browse
		Upload
		Cancel
		Choose file ? X
		Look In: PV3 V W V Log
		My Reckup FV3 to:
		Desktop
		My Documents
		My Computer
		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
		My Network File name: Backup FV3.lgz P Open Places D () D ()
		Pries or type: All Fries (*.*)
		Click on the Upload button.
		The file will take a few seconds to upload depending on the size of the backup
		data. The file will be visible on the list of entries after the upload is complete.

21	Recovered SOAM GUI: Login	Establish a GUI session on the recovered SOAM server. Open the web browser and enter a URL of: http:// <recovered_soam_ip_address> Login as the <i>guiadmin</i> user: ORACLE</recovered_soam_ip_address>
		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.

22	Recovered	Click on Main Menu->Status & Manage->Database
	Verify the	Select the Active SOAM server and click on the Compare.
	Archive Contents and	Enable Provisioning Report Inhibit Replication Backup Compare Restore Man Audit Suspend Auto Audit
	Database Compatibility	The following screen is displayed; click the button for 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
		CBackup nopribide02 configuration NETWORK_OAIHP 20100928, 021502 AUTO tar CBackup nopribide02 configuration NETWORK_OAIHP 2010029, 021501 AUTO tar CBackup nopribide02 configuration NETWORK_OAIHP 20101002, 021502 AUTO tar CBackup nopribide02 configuration NETWORK_OAIHP 20101002, 021502 AUTO tar CBackup nopribide02 configuration NETWORK_OAIHP 20101002, 021502 AUTO tar CBackup nopribide02 configuration NETWORK_OAIHP 20101003, 021501 AUTO tar CBackup nopribide02 configuration NETWORK_OAIHP 20101003, 021502 AUTO tar CBackup nopribide02 configuration NETWORK_OAIHP 20101005, 021502 AUTO tar CBackup nopribide02 configuration NETWORK_OAIHP 20101005, 021502 AUTO tar
		Verify that the output window matches the screen below.
		Note: You will get a database mismatch regarding the NodeIDs of the blades. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix H. My Oracle Support (MOS)
		The selected distance does born base(7 or 01/13/2011 at 13.4.07 EDT and contains the following comment:
		Statistica Consultatio The difference are competitive The difference are competitive for Care Consultation
		The node types are compatible. Tomote start of the services before restorem this database. The topology's hot compatible. Contact tradile customer services before restorem this database.
		Discrepancies III Server allow 1111 121 has different (main III) in correct equipy and the selected backup file Prover a file shift 1111 has different when princede to 10070 dB III Server Address (1157) rails different Main (file main III) in correct equipy and the selected backup file Correct and III Correct Address (1157) rails different Main (file main III) in correct equipy and the selected backup file Correct and III Correct Address (1157) rails different Main (file main III) in correct equipy and the selected backup file Correct and III Correct Address (1157) rails different Main (11607) rails (116000) rails (1160000) rails (116000) rails (116000) rails (116000) rails (116000) rails (1160000) rails (1160000) rails (1160000) rails (1160000) rails (1160000) rails (11600000) rails (11600000) rails (11600000) rails (11600000) rails (11600000) rails (116000000) rails (11600000000000000000000000000000000000
		Use Compatibility Use Compatibility The user and submetherization data are compatible. Output
		Provisions/add/ordsputtion Provisions/add/ordsputtion Control AddressExtence Control Control AddressExtence Control Control AddressExtence Control Control AddressExtence Control Control Control AddressExtence Cont
		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 SOAM:
		Topology Compatibility THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.
		Note: We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility.
		If the verification is successful, Click BACK button and continue to next step in this procedure.
Page		E57520-02

23	Recovered SOAM GUI: Restore the	Select the Active SOAM server, and click on Restore as shown below.
	Database	The following screen will be displayed. Select the proper back up provisioning and configuration file.
		Select archive to Restore on server: blade02 Backup.npqr.blade02.Configuration.NETWORK_OAMP.20100928_021502.AUTO.tar Backup.npqr.blade02.Configuration.NETWORK_OAMP.20100929_021501.AUTO.tar Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101002_021502.AUTO.tar Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101002_021502.AUTO.tar Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101002_021502.AUTO.tar Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101002_021502.AUTO.tar Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101002_021502.AUTO.tar Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101002_021502.AUTO.tar Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101005_021501.AUTO.tar Backup.npqr.blade02.Configuration.NETWORK_OAMP.20101005_0
		Click OK Button. The following confirmation screen will be displayed.
		If you get an error that the NodelDs do not match. That is expected. If no other errors beside the NodelDs are displayed, select the Force checkbox as shown above and Click OK to proceed with the DB restore.
		Database Restore Confirm
		Discrepancies: - 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: B1787.161 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.
		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, the user will be logged out of XMI SOAM GUI since the restored Topology is old data.
24	Recovered SOAM GUI:	Wait for 5-10 minutes for the System to stabilize with the new topology:
	Monitor and Confirm database	Monitor the Info tab for " Success ". This will indicate that the backup is complete and the system is stabilized.
	restoral	Note: Do not pay attention to alarms until all the servers in the system are completely restored.
		Note: The Configuration and Maintenance information will be in the same state it was backed up during initial backup.
25	NOAM VIP GUI: Recover Remaining	Install the remaining failed SOAM servers by executing procedure <i>"Configure the SOAM Servers"</i> , steps 1-3, 5-8 Refer to Table 5 for the applicable DSR software installation and configuration reference.
	SUAINI Servers	Note: If you are using Netbackup, also execute step 10.

26	NOAM VIP GUI:	Navigate to Status & Manage -> HA
	Set HA on SOAM Servers	Status & Manage Network Elements Server Database Database KPIs Processes Tasks Files Click on Edit at the bottom of the screen
		For each SOAM server whose Max Allowed HA Role is set to Standby, set it to Active Press OK
27	Recovered Server: Sync NTP	 1) Perform the following to retrieve the remote NTP server: \$ sudo ntpq -np Example output: [admusr@NOAM-2 ~]\$ ntpq -np remote refid st t when poll reach delay offset jitter *10.240.9.186 10.250.33.2 3 u 356 1024 377 1.409 0.113 2.434 2) Stop ntpd service: \$ sudo service ntpd stop 3) Sync the date to the ntp remote server: \$ sudo ntpdate <ntp remote="" server=""></ntp> Note: The remote server below will be that of the one gathered in sub step 1.
		4) Start the ntp service:
		<pre>\$ sudo service ntpd start</pre>

28	NOAM VIP GUI: Restart DSR application	Navigate to Main Menu->Status & Manage->Server, Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered server and click on Restart.
		Stop Restart Reboot NTP Sync Report
29	NOAM VIP GUI: Start Replication on working C- Level Servers	Un-Inhibit (<i>Start</i>) Replication to the working C-Level Servers which belong to the same site as of the failed SOAM servers. Execute Appendix F . Un-Inhibit A and B Level Replication on C-Level Servers If the <i>"Repl Status"</i> is set to "Inhibited", click on the Allow Replication button as shown below using the following order, otherwise if none of the servers are inhibited, skip this step and continue with the next step: Active NOAM Server Standby NOAM Server Active SOAM Server Standby SOAM Server Standby SOAM Server Standby DR NOAM Server MP/IPFE Servers (<i>if applicable</i>) Active DR NOAM Server Standby DR NOAM Server Standby DR NOAM Server MP/IPFE Servers (<i>if MPs are configured as Active/Standby, start with the Active MP, otherwise the order of the MPs does not matter</i>) SBRS (<i>if SBR servers are configured, start with the active SBR, then standby, then spare</i>) Verify that the replication on all the working servers is allowed. This can be done by clicking on each server and checking that the button below shows "Inhibit Replication", and NOT "Allow Replication" Backup. Compare.

20	NOAM VIP GUI:	
	Recover the C- Level Server (DA-MP, SBRs, IPFE, SS7-MP)	Execute procedure <i>"Configure MP Blades Servers"</i> , Steps 1, 5, 6, 7, 8, and 9 Refer to Table 5 for the applicable DSR software installation/configuration guide reference.
		Note: Also execute step 10 and 11 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.
		Note: – DSR 5.0/6.0/7.0 ONLY : If this server is an IPFE server, ensure ipfeNetUpdate.sh from procedure <i>"IP Front End (IPFE) Configuration (Optional)"</i> from [17] has been executed.
		Repeat this step for any remaining failed MP servers.
31	NOAM VIP GUI:	Un-Inhibit (Start) Replication to the ALL C-Level Servers
	Start replication on ALL C-Level Servers	Navigate to Status & Manage -> Database
		🚊 😋 Status & Manage
		🚽 🎆 Network Elements
		Server 🤤
		Processes
		🖬 🧰 Tasks
		🔚 📑 Files
		If the <i>"Repl Status"</i> is set to "Inhibited", click on the Allow Replication button as shown below using the following order:
		Active NOAMP Server
		Standby NOAMP Server
		Active SOAM Server Standby SOAM Server
		Spare SOAM Server (<i>if applicable</i>)
		Active DR NOAM Server
		 Standby DR NOAM Server MP/IPEE Servers (if MPs are configured as Active/Standby start with
		the Active MP, otherwise the order of the MPs does not matter)
		Verify that the replication on all servers is allowed. This can be done by clicking on each server and checking that the button below shows "Inhibit Replication", and NOT "Allow Replication".
		Disable Provisioning Report Allow Replication Backup Compare Restore

32	NOAM VIP GUI: Set HA on all C- Level Servers	Navigate to Status & Manage Status & Manage Network Elements Server Database KPIS Processes Tasks Files
		Click on Edit at the bottom of the screen For each server whose Max Allowed HA Role is set to Standby, set it to Active Press OK
33	Active SOAM: Prepare recovered SOAM for optional feature activation (DSR 5.0/6.0/7.0)	For DSR 5.0/6.0/7.0: If DSR 7.1, skip this step Establish an SSH session to the Active SOAM, login as <i>admusr</i> . Execute the following command: \$ irem DsrApplication where "name in ('RBAR','FABR','PCA','MD-IWF','DM-IWF','CPA','GLA')"
34	Active SOAM: Verify Preparation (DSR 5.0/6.0/7.0)	<pre>For DSR 5.0/6.0/7.0: If DSR 7.1, skip this step Execute the following command to verify preparation of optional feature activation: \$ iqt -z -h -p -fname DsrApplication where "name in ('RBAR', 'FABR', 'PCA', 'MD-IWF', 'DM-IWF', 'CPA', 'GLA')" Note: There should be no output of this command, if there is, verify the correct entry of the command in step 26.</pre>
35	ACTIVE NOAM: Perform key exchange between the active-NOAM and recovered servers.	Establish an SSH session to the Active NOAM, login as admusr . Execute the following command to perform a keyexchange from the active NOAM to each recovered server: \$ keyexchange admusr@<recovered hostname="" server=""></recovered> Note: If an export server is configured, perform this step.

36		Establish an SSH session to the active NOAM, login as <i>admusr.</i>						
	Pofor to soction							
	Features	1.5 Ontional Featuresto activate any features that were previously activated						
	NOAM VIP GUI:	Navigate to Main Menu -> Status & Manage -> Database						
37	Fetch and Store							
	the database	🛓 😋 Status & Manage						
	Report for the	Network Elements						
	Newly Restored	Server						
	Data and Save it							
		🔄 💽 Database						
		- KPIs						
		🔤 🤤 Processes						
		🖬 🧰 Tasks						
		🔤 🖬 Files						
		Select the active NOAM server and click on the Report button at the bottom of						
		the page. The following screen is displayed:						
		Main Menu: Status & Manage -> Database [Report]						
		dsr Database Status Report =						
		Report Generated: Wed Aug 19 16:49:08 2015 EDT From: Network OAM&P on host Oahu-NOAM-2						
		Report Version: 7.1.0.0.0-71.19.0 User: guiadmin						
		General						
		Hostname : Oahu-NOAM-2						
		Database Birthday : 2015-07-07 12:31:27 EDT Appworks Database Version : 6.0						
		Application Database Version :						
		Capacities and Utilization						
		Disk Utilization 3.1%: 281M used of 9.1G total, 8.4G available Memory Utilization 26.9%: 1415M used of 5266M total, 3851M available						
		liarme						
		Naisteraraa in Brograda						
		Backup operation success						
		Replication Audit Status						
		Not found						
		Service Information						
		End of dsr Database Status Report						
		Click on Save and save the report to your local machine.						

38	ACTIVE NOAM: Verify	Login to the Active NOAM via SSH terminal as <i>root(5.0) or admusr(6.0+)</i> user. Execute the following command:							
	Replication	C suda improtate m							
	Servers	Ş SUGO Irepstat -m							
		Output like below shall be generated:							
		Policy 0 ActStb [DbReplication]							
		Oahu-DAMP-1 Active							
		BC From Oahu-SOAM-2 Active 0 0.50 ^0.15%cpu 25B/s A=me							
		CC To Oahu-DAMP-2 Active 0 0.10 0.14%cpu 25B/s A=me							
		Oahu-DAMP-2 Stby							
		BC From Oahu-SOAM-2 Active 0 0.50 ^0.11%cpu 31B/s A=C3642.212							
		CC From Oahu-DAMP-1 Active 0 0.10 ^0.14 1.16%cpu 31B/s A=C3642.212							
		Oahu-IPFE-1 Active							
		BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 24B/s A=C3642.212							
		Oahu-IPFE-2 Active							
		BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 28B/s A=C3642.212							
		Oahu-NOAM-1 Stby							
		AA From Oahu-NOAM-2 Active 0 0.25 ^0.03%cpu 23B/s							
		Oahu-NOAM-2 Active							
		AA To Oahu-NOAM-1 Active 0 0.25 1%R 0.04%cpu 61B/s							
		AB To Oahu-SOAM-2 Active 0 0.50 1%R 0.05%cpu 75B/s							
		Oahu-SOAM-1 Stby							
		BB From Oanu-SOAM-2 Active 0 0.50 ~0.03%cpu 2/B/S							
		AB From Oabu-NOAM-2 Active 0 0.50 ^0.03%cpu 24B/s							
		BB To Ω_{abu} -SOAM-1 Active $0.0.50$ 1%B Ω_{abu} -SOAM-1 32B/s							
		BC To Oahu-IPFE-1 Active 0 0.50 1%R 0.04%cpu 21B/s							
		BC To Oahu-SS7MP-2 Active 0 0.50 1%R 0.04%cpu 21B/s							
		irepstat (40 lines) (h)elp (m)erged							

39	NOAM VIP GUI:	Click on Main Menu->Status and Manager->Database											
_	Verify the												
	Database states	📋 🚍 Status & Manage											
		💽 I	Vetwor	rk Ele	ments								
		1	Server										
		💓 I	HA										
		Database											
			-										
		💓 F	Proces	ses									
		Verify that the	e "OAM	Max	HA Ro	le" is eith	ner "A	ctive"	or "S	tandb	y" foi	[·] NOA	М
		and SOAM ar	nd "App	olicatio	on Max	HA Role	e" for	MPs	is "Ac	tive", a	and th	hat the	•
		status is "Nor	mal" as	show	n belc	W:							
		Network Element	Server		Role	OAM Max	Application Max HA	Status	DB Level	OAM Repl	SIG Repl	Repl	Repl Audit
		NO 10303	102		Network OAM&	P Active	Role	Normal	0	Normal	NotApplica	bl Allowed	AutoinProg
		SO_10303 F	SBR		MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg
		SO_10303	1P2		MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg
		SO_10303 S NO 10303 N	301 101		System OAM Network OAM&	P Standby	005	Normal	0	Normal	NotApplica	bl Allowed bl Allowed	AutoInProg
		SO_10303	PFE		MP	Active	00S	Normal	0	Normal	Normal	Allowed	AutoInProg
		SO_10303 S	802		System OAM	Active	008	Normal	0	Normal	NotApplica	bl Allowed	AutoInProg
		Click on Main	Monu	-> Sta	tue an	d Manac		1					
40	Vorify the HA	CIICK OIT Wall	wenu	->5la	ius an	น เพลเาลยู	Je->11						
	Status	📥 👝 Ota		1-1-2-2	10								
	Status	📄 🚔 Stat	tus & M	lanag	je								
	Status	💼 😑 Stat	tus & M Networ	lanag k Elei	je ments								
	Status	😑 🚖 Stal	tus & M Networ Gerver	lanag k Elei	je ments								
	Status	💼 🥽 Stal	tus & M Networ Server	1anag k Elei	je ments								
	Status	Stal 🚗 🧧	tus & M Networ Server 1A	1ana <u>c</u> k Elei	je ments								
	Status	i - Stal	tus & N Networ Gerver <mark>1A</mark> Databa	1ana <u>o</u> k Elei se	je ments								
	Status	i = - Stat	tus & M Networ Gerver HA Databa (PIs	1anag k Elei se	je ments								
	Status		tus & M Networ Server <mark>1A</mark> Databa (PIs	lana <u>c</u> k Elei se	je ments								
	Status	Stal	tus & M Networ Gerver 1A Databa (PIs Process	lana <u>c</u> k Elei se ses	je ments								
	Status		tus & M Networ Gerver 1A Databa (PIs Process	lana <u>c</u> k Eler se ses	je ments								
	Status	Select the rov	tus & N Networ Gerver A Databa Oataba Process v for all	lanag k Eler ses of the	e serve	ers							
	Status	Select the rov Verify that the	tus & N Networ Gerver 14 Oataba (PIs Process v for all e "HA R	lanag k Eler se ses of the cole" is	e s eithe	ers "Active"	' or "S	Standl	ру".				
	Status	Select the rov Verify that the	tus & M Networ Gerver HA Databa (PIs Process v for all e "HA R	lanag k Eler se ses of the cole" is	e serve s eithe	ers r "Active"	' or "S	Standl	oy".				
	Status	Select the rov Verify that the	tus & N Networ Gerver IA Databa (PIs Process V for all e "HA R	Aanag k Eler se ses of the cole" is	e serve a serve s eithe	ers r "Active" Mate Hostname Life	' or "S	Standl	ру".	Server Ro	le	Active VIPs	
	Status	Select the rov Verify that the	tus & N Networ Gerver IA Databa (PIs Process V for all e "HA R OAMMax Active	Annag k Eler se ses of the cole" is Application Max HA Role	e serve s eithe Adoved HA Active	ers r "Active" Mate Hostname Lits NO1	' Or "S	Stands	ру".	Server Ro Network O	le AJA&P	Active VIPs 10.240.70 13	2
	Status	Select the rov Verify that the	tus & N Networ Gerver 1A Databa (PIs Process v for all e "HA R Active Statuty Active	Annag k Eler se ses of the cole" is Application Max HA Role	e serve s eithe Adtwe Active	ers r "Active" Mate Hostname Lis No1 S02 S01	' Or "S st Networ N0_10 S0_10	Standt rk Element 1303 303	oy".	Server Ro Network O System O/	le AM&P MM	Active VIPs 10.240.70.13 10.240.70.13	2
	Status	Select the rov Verify that the No2 So1 So2 MP1	tus & N Networ Gerver HA Databa (PIs Process V for all e "HA R Adive Standby Active Standby Standby	Application Max HA Cos Cos Cos Cos Cos Cos Cos Cos Cos Cos	e serve s eithe a Max Active Active Active	ers r "Active" Mate Hostname Lis No1 SO2 SO1 MP2	' Or "S st Networ N0_10 S0_10 S0_10 S0_10	Stands rk Element 303 303 303	Dy".	Server Ro Network O System O/ MP	le AM&P M	Active VIPs 10.240.70.13 10.240.70.13	2
	Status	Select the rov Verify that the No2 So1 So2 MP1 MP2 PEE	tus & N Networ Gerver HA Databa (PIs Process V for all Process V for all MMAX Adve Standy Adve Standy Adve	Active Active Active Active Active Active Active Active Active	e serve s eithe Adtve Active Active Active	ers r "Active" Mate Hostname Lit NO1 SO2 SO1 MP2 MP1	' OF "S st Network No_10 SO_10 SO_10 SO_10 SO_10 SO_10	Stands rk Element 303 303 303 303 303	oy".	Server Ro Network O System O/ MP MP	le AM&P M	Active VIPs 10.240.70.13 10.240.70.13	2
	Status	Select the rov Verify that the NO2 SO1 SO2 MP1 MP2 IPFE	tus & N Networ Gerver 1A Databa (PIs Process V for all Process V for all CAM Max Active Standy Active Standy Active	Application Max HA Role OOS OOS Active Active OOS	e serve s eithe Active Active Active Active	ers r "Active" Mate Hostname Lis NO1 SO2 SO1 MP2 MP1	Y Or "S at Networ N0_10 S0_10 S0_10 S0_10 S0_10 S0_10	Stands rk Element 1303 303 303 303 303 303 303	Dy".	Server Ro Network O System O/ MP MP MP	le AJA&P MM	Active VIPs 10.240.70.13 10.240.70.13	2
	Status	Select the rov Verify that the No2 So1 So2 MP1 MP2 IFFE	tus & N Networ Gerver A Oataba (PIs Process V for all OAM Max Active Standby Active Standby Active	Application Max HA Role OOS Active Active OOS	e serve s eithe Adtve Active Active Active Active	ers r "Active" Mate Hostname Lie NO1 SO2 SO1 MP2 MP1	Y OF "S st Network NO_10 SO_10 SO_10 SO_10 SO_10 SO_10	Standl rk Element 1303 303 303 303 303 303 303 303)у".	Server Ro Network O System O/ System O/ MP MP MP	le Alf&P MM MM	Active VIPs 10.240.70.13 10.240.70.13	2





46	SOAM VIP GUI:	Navigate to Main Menu -> Diameter -> Maintenance -> Applications
	Enable Optional Features	Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups DA-MPs Select the optional feature application configured in step 29. Click the Enable button. Disable Pause updates
47	SOAM VIP GUI: Re-enable Transports if Needed (Applicable ONLY for DSR 6.0+)	Navigate to Main Menu->Transport Manager -> Maintenance -> Transport Transport Manager Configuration Maintenance Transport Select each transport and click on the Enable button Enable Disable Block Verify that the Operational Status for each transport is Up.
48	SOAM VIP GUI: Re-enable MAPIWF application if needed (Applicable ONLY for DSR 6.0+)	Navigate to Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users
49	SOAM VIP GUI:	Navigate to Main Menu->SS7/Sigtran->Maintenance->Links
----	--------------------------	--
	Re-enable links	
	II needed (Applicable	
		i → Maintenance
		Local SCCP Users
	0.0+)	
		Remote MTP3 Users
		in the second seco
		Click on Enable button for each link.
		Enable Disable
		Verify that the Operational Status for each link is Up
50	Active NOAM:	If recovering a DSR 5.0/6.0 system and POLICY AND CHARGING DRA
50	Verify Sync Split	application is activated then execute this step.
	Scope Data (If	Notes If recovering a DCD 7.04 eventer DO NOT evenute this step
	CHARGING	Note: If recovering a DSR 7.0+ system, DO NOT execute this step
	DRA is	Login to the Active NOAM VIP via SSH terminal as root(5.0) or admusr(6.0+)
	activated):	user.
	5.0/6.0 Only	
		Execute the following steps:
		Go to Appworks bin directory:
		Course of the Mart O (and the for
		5 Sudo ca /usr/TKLC/appworks/bin/
		Execute the PCRF sync script in "reportonly" mode to check whether PCRF
		data syncing is required or not. This is a read-only mode that does not modify
		the database:
		\$ sudo ./syncPcrikererencesAfterRestore.sn -reportonly
		If the Report Summary shows one or more PCREs "need to be synced" then
		repeat the script execution again but using the "sync" option instead of
		"reportenly" in order to sync the database.
		The "sync" option will modify the database:
		\$ sudo /sunaParfPeferencesAfterPestore sh _suna
		y bud ./ syncronierenceshiterkestore.sh sync
		Re-execute the PCRF sync script in "reportonly" mode to verify all PCRF data is
		in sync. Examine the Report Summary output of the script. Verify the number of
		"PCRF record(s) processed in "total" is equal to the number of "PCRF record(s)
		already in sync":
		\$ sude /sunaPartPoterongesAfterPostero sh _reportering
		y successfully successfully

51	SOAM VIP GUI: Examine All	Navigate to Main Menu->Alarms & Events->View Active
	Alarms	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 Appendix H. My Oracle Support (MOS).
52	NOAM VIP GUI: Examine All	Login to the NOAM VIP if not already logged in.
	Alarms	Navigate to Main Menu->Alarms & Events->View Active
53	Backup and Archive All the Databases from the Recovered System	Execute Appendix A . DSR Database Backup to back up the Configuration databases:

5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact)

For a partial server outage with an SOAM server intact and available; NOAM servers are recovered using recovery procedures of base hardware and software and then executing a database restore to the active NOAM server using a NOAM database backup file obtained from external backup sources such as customer servers or NetBackup. All other servers are recovered using recovery procedures of base hardware and software. Database replication from the active NOAM/active SOAM server will recover 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 execute the procedure. The actual procedures' detailed steps are in **Procedure 3**. The major activities are summarized as follows:

Recover Active NOAM server by recovering base hardware, software and the database.

- Recover the base hardware.
- Recover the software.
- Recover the database

Recover **NOAM servers** by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.

Recover any failed **SOAM and MP servers** by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.
- Database is already intact at one SOAM server and does not require restoration at the other SOAM and MP servers.

S T F	This procedure pe intact. This include	erforms recovery if ALL NOAM servers are failed but 1 or more SOAM servers are es any SOAM server that is in another location (spare SOAM server).
– P #	Check off (√) each step number.	h step as it is completed. Boxes have been provided for this purpose under each
	If this procedure fa	ails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.
1	Workarounds	Refer to Appendix G . Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
2	Gather Required Materials	Gather the documents and required materials listed in Section 3.1 Required Materials
3	RMS NOAM Failure	If the failed server is a rack mount server based NOAM, execute this step; otherwise skip to the next step .
		1. HW vendor to replace the failed equipment
		2. Execute the "iLO Configuration Procedure" appendix from [3]
		 Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference.
		4. Confirm necessary software images are present on the PMAC.
		 If the failed NOAM is co-hosted with the PMAC on the first rack mount server, execute procedure "Continue TVOE Configuration on First RMS Server" - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.
		 If the failed NOAM is NOT co-hosted with the PMAC on the first rack mount server, execute procedure "Configure TVOE on Additional RMS Servers(s)" - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.

4	HP-Class Blade Failure	If the failed server is an HP C-Class Blade, execute this step; otherwise skip to the next step.
		1. HW vendor to replace the failed equipment
		 Execute procedure "Confirm/Update blade Server BIOS Settings" – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference.
		 Execute procedure "Configure Blade Server iLO Password for Administrator Account" – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference.
		 Perform any needed firmware upgrades – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference.
		 For NOAM/SOAM servers, execute procedure <i>"IPM Servers Using PM&C Application"</i> - Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference.
5	Configure TVOE on Server Blades	For NOAMs on TVOE server Blades and SOAMs, execute procedure "Configure TVOE on Server Blades" - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.
6	Create VMs	For NOAMs, execute procedure <i>"Create NOAM Guest VMs"</i> - Refer to Table 5 for the applicable DSR software installation and configuration reference.
		For SOAMs, execute procedure <i>"Create SOAM Guest VMs"</i> - Refer to Table 5 for the applicable DSR software installation and configuration reference.
7	IPM Failed Guest/Servers	IPM the failed guests/servers by executing procedure <i>"IPM Blades and VMs"</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.
8	Install DSR application on Failed	Install the DSR application on the failed guests/server by executing procedure <i>"Install Application Software on Blades"</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.
	Guests/Servers	
9	Repeat for	If necessary, repeat steps 1-7 for all remaining failed servers.
	Remaining Failed Servers	
10	Install	If NetBackup is used execute procedure "Install NetBackup Client (Optional)" -
10	NetBackup	Refer to Table 5 for the applicable DSR software installation/configuration
	Client	guide reference.

11	Obtain Latest Database Backup and	Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources.
	Network Configuration Data.	From required materials list in Section 3.1 Required Materials; use site survey documents and Network Element report (if available), to determine network configuration data.
12	Execute DSR	Verify the networking data for Network Elements
	Installation Procedure for the First NOAM	Note: Use the backup copy of network configuration data and site surveys (Step 2)
		Configure the first NOAM server by executing procedure <i>"Configure the First NOAM NE and Server"</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.
		Configure the NOAM server group by executing procedure <i>"Configure the NOAM Server Group"</i> - Refer to Table 5 for the applicable DSR software installation and configuration reference
13	NOAM GUI: Login	Login to the NOAM GUI as the <i>guiadmin</i> user:
		Oracle System Login
		Log In Enter your username and password to log in
		Username: guiadmin
		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.
		Other names may be trademarks of their respective owners.

14	NOAM GUI:	Browse to Main Menu->Status & Manage->Files
	Upload the Backed up Database File	 Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files
		Select the Active NOAM server. The following screen will appear:
		Cpa1-NO Cpa1-IPFE Cpa1-Sbr1 Cpa1-Mp1 Cpa1-Mp2 Cpa1-Mp3 Cpa1-Sbr2
		Size Size Type Interstating Backup.dsr.Cpa1-N0.Configuration.NETWORK_OAMP.20120321_021501.AUTO.tar 720 KB tar 2012-03-21 06:15:02 UTC
		Click on Upload as shown below and select the file <i>"NO Provisioning and Configuration:"</i> file backed up after initial installation and provisioning.
		Click on Browse and locate the backup file and click on Open as shown below.
		File: Define: Define: Cancel
		Choose file ? X Look in: P V3 Wig Backup EAGLEVpeCOMProvidg: ? X Wig Backup FV3.ge: P V3_NetHawk.bt Desktop Iv My Documents: Iv My Documents: Iv My Documents: Iv My Documents: Iv My Recert Backup PV3.tgz File name: Backup PV3.tgz Files of type: All Files (*.*)
		Click on the Upload button.
		The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.

	NOAM GUI:	Click on Main Menu->Status & Manage->Database
15	Disable	
	Provisioning	 Status & Manage Network Elements Server Replication Collection HA Database KPIs Processes
		Files Disable Provisioning by clicking on Disable Provisioning button at the bottom of the screen as shown below. Disable Provisioning Report Inhibit/Allow Backup Compare Restore A confirmation window will appear, press OK to disable Provisioning. Message from webpage Inhibit/Allow OK Cancel The message "Warning Code 002" will appear.

16 NOAM GUI:	Click on Main Menu->Status & Manage->Database
	Select the Active NOAM server and click on the Compare.
Contents and	Enable Provisioning Report Inhibit Replication Backup Compare Restore Man Audit Suspend Auto Audit
Compatibility	The following screen is displayed; click the button for 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 DEachup papt blade02 Configuration NETWORK, OAMP 20100928, 021503 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 20100920, 021501 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 20100920, 021501 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010092, 021501 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup papt blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup patter blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup patter blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup patter blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup patter blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup patter blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup patter blade02 Configuration NETWORK, OAMP 2010002, 021502 AUTO far OBachup patter blade02 Configuration NETWORK, OAMP 2010002, 02
	Creactup rupt modeoz. Comparator He HYOR Cover zu to too zuz for An Total -
	Verify that the output window matches the screen below.
	Note: You will get a database mismatch regarding the NodelDs of the blades. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix H. My Oracle Support (MOS)
	The selected database came from biose07 on 01/192011 at 13.43.47 EDT and contains the following comment:
	Archiel Contents Providence According and Configuration data
	Unital A contraction To disclose an encounter the disclose and encounter the disclose and encounter the disclose and encounter To encounter To encounter
	Transformer Contractifies The COPPLETED ATTRACT CONTACT TEXELEC CUSTOMER SERVICES BEFORE RESTORING THES DATABASE.
	Discreptione — His Server as 2110-123 has different scale TB is current topology and the selected backup file. — His Server Address Cl197.24 has different (select backup file and the selected backup file. — DH Server Address Cl197.24 has different (select backup file and topology and the selected backup file. — Current hod DD (157.24. Selected backup file and ED 1827) CU — HI Server Address B177.14 has different (select backup file and topology and the selected backup file. — Current hod DD (177.14. Selected backup file and ED 1827) CU — HI Server Address B177.14 has different (select Backup file backup file. — Current hod DD (177.14. Selected backup file backup file backup file.
	- Lase: Connactability - The user and authentication data are compatible. - The user and authentication data are compatible.
	Controls Productions/secOnfliquention Table Instruct Control Table Structure Control Control AddicentEfformers Control Solicited 0 Control AddicentEfformers Control Solicited 1 Control AddicentEfformers Control Solicited 1 Control AddicentEfformers Control Solicited 1
	Constant Automatic contracts and Database Compatibilities must be the following:
	Archive Contents: Configuration data
	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 NOAM:
	Topology Compatibility THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.
	Note: We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility.
	If the verification is successful, Click BACK button and continue to next step in this procedure.
Page 81	E57520-02

	ACTIVE NOAM	
17	Restore the	Select the Active NOAM server, and click on Restore as shown below
	Database	Select the Active NOAM server, and click on Restore as shown below.
		The following screen will be displayed. Select the proper back up provisioning
		and configuration file.
		Database Restore
		Select archive to Restore on server: blade02
		Archive Backup.npgr.biade02.Configuration.NETWORK_OAMP.20100929_021501.AUT0.tar Backup.npgr.biade02.Configuration.NETWORK_OAMP.20100930_021501.AUT0.tar OBackup.npgr.biade02.Configuration.NETWORK_OAMP.20101002_021502.AUT0.tar Backup.npgr.biade02.Configuration.NETWORK_OAMP.20101003_021502.AUT0.tar OBackup.npgr.biade02.Configuration.NETWORK_OAMP.20101003_021502.AUT0.tar OBackup.npgr.biade02.Configuration.NETWORK_OAMP.20101003_021502.AUT0.tar OBackup.npgr.biade02.Configuration.NETWORK_OAMP.20101003_021502.AUT0.tar OBackup.npgr.biade02.Configuration.NETWORK_OAMP.20101005_021501.AUT0.tar
		Ok) Cancel
		Click OK Button. The following confirmation screen will be displayed.
		If you get an error that the NodelDs do not match. That is expected. If no other errors beside the NodelDs are displayed, select the Force checkbox as shown above and Click OK to proceed with the DB restore.
		Database Restore Confirm
		Incompatible database selected
		Discrepancies: - 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: B1787.161 Selected backup file node ID: B2073.087 - Current node ID: B1787.161 Selected backup file node ID: B2073.087 - Current node ID: B1787.161 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.
		Ok Cancel
		Note: After the restore has started, the user will be logged out of XMI NO GUI since the restored Topology is old data.

18	NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: <pre>http://<primary_noam_vip_ip_address></primary_noam_vip_ip_address></pre> Login as the guiadmin user:
		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.
19	NOAM VIP GUI: Monitor and Confirm database restoral	 Wait for 5-10 minutes for the System to stabilize with the new topology: Monitor the Info tab for "Success". This will indicate that the backup is complete and the system is stabilized. Following alarms must be ignored for NOAM and MP Servers until all the Servers are configured: Alarms with Type Column as "REPL", "COLL", "HA" (with mate NOAM), "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 will be in the same state
		it was backed up during initial backup.
20	Login	admusr(6.0+) user.

21	ACTIVE NOAM:	IF DSR 7.1, SKIP THIS STEP
	Restore /etc/hosts/ File of the Active	Execute the following command:
	NOAM (DSR	<pre>\$ sudo AppWorks AppWorks_AppWorks updateServerAliases</pre>
	5.0/6.0/7.0 ONLY)	<noam host="" name=""></noam>
22	NOAM VIP GUI:	Navigate to Main Menu->Status & Manage->Database
	Re-enable	
	Provisioning	(Enable Provisioning) Report Inhibit/Allow Replication Backup Com
		Click on the Enable Provisioning . A pop-up window will appear to confirm as shown below, press OK .
		Message from webpage Image: Constraint of the second s
23	NOAM VIP GUI: Recover Standby NOAM	Install the second NOAM server by executing procedure <i>"Configure the Second NOAM Server"</i> , steps 1-3, and 5-8 - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.
		Note: Execute step 7 if Netbackup is used.
		If NetBackup is used, execute procedure <i>"Install NetBackup Client"</i> - Refer to Table 5 for the applicable DSR software installation and configuration reference.
		Note: If Topology or nodeld alarms are persistent after the database restore, refer to Appendix G . Workarounds for Issues not fixed in this Release
24	NOAM VIP GUI: Recover the	Recover the remaining SOAM servers (standby, spare) by repeating the following steps for each SOAM server:
	Failed SOAM Servers	 Install the remaining SOAM servers by executing reference Procedure "Configure the SOAM Servers", steps 1-3, and 5-8 Refer to Table 5 for the applicable DSR software installation/configuration guide reference.
		Note: Execute step 10 as well if Netbackup is used.
		 If you are using Netbackup, execute procedure "Install Netbackup Client" - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.

25	NOAM VIP GUI: Set HA on all C- Level Servers	Navigate to Status & Manage -> HA
		 KPIs Processes Tasks Files
		For each conver whose Max Allowed HA Pole is set to Standby, set it to Active
26	Recovered Server: Login	Establish an SSH to the recovered server's XMI address:
27	Recovered Server: Sync	1) Perform the following to retrieve the remote NTP server:
	NTP	\$ sudo ntpq -np
		Example output:
		<pre>[admusr@NOAM-2 ~]\$ ntpq -np remote refid st t when poll reach delay offset jitter ===================================</pre>
		======================================
		2) Stop ntpd service:
		<pre>\$ sudo service ntpd stop</pre>
		3) Sync the date to the ntp remote server:
		<pre>\$ sudo ntpdate <ntp remote="" server=""></ntp></pre>
		Note: The remote server below will be that of the one gathered in sub step 1.
		4) Start the ntp service:
		<pre>\$ sudo service ntpd start</pre>

28	NOAM VIP GUI:	Navigate to Main Menu->Status & Manage->Server,
	Restart DSR application	Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select each recovered server and click on Restart. Stop Restart Reboot NTP Sync Report
29	Active SOAM:	For DSR 5.0/6.0/7.0: If DSR 7.1, skip this step.
	Prepare recovered	Establish an SSH session to the Active SOAM, login as admusr.
	SOAM for optional feature	Execute the following command:
	activation (DSR 5.0/6.0/7.0)	<pre>\$ irem DsrApplication where "name in ('RBAR','FABR','PCA','MD-IWF','DM-IWF','CPA','GLA')"</pre>
30	Active SOAM:	For DSR 5.0/6.0/7.0: If DSR 7.1, skip this step
	Preparation (DSR	Execute the following command to verify preparation of optional feature activation:
	5.0/6.0/7.0)	<pre>\$ iqt -z -h -p -fname DsrApplication where "name in ('RBAR','FABR','PCA','MD-IWF','DM-IWF','CPA','GLA')"</pre>
		Note: There should be no output of this command, if there is, verify the correct entry of the command in step 24 .
31	ACTIVE NOAM:	Establish an SSH session to the Active NOAM, login as <i>admusr.</i>
	exchange between the	Execute the following command to perform a keyexchange from the active NOAM to each recovered server:
	and recovered	<pre>\$ keyexchange admusr@<recovered hostname="" server=""></recovered></pre>
	5017015.	Note: If an export server is configured, perform this step.
32	ACTIVE NOAM: Activate	Establish an SSH session to the active NOAM, login as admusr.
	Optional Features	Refer to section 1.5 Optional Featuresto activate any features that were previously activated.



34	ACTIVE NOAM:	Login to the	e Active NOA	M via SSH	termi	nal as	root	(5.0) d	or adn	nusr(l	6.0+)	user.
5.	Verify	Execute the	e following co	mmand:								
	Replication											
	Between Servers.	Ş sudo	irepstat -	m								
		Output lik	e below shall	be genera	ted:							
		Policy	0 ActStb [D	bReplicati	on] -							
		PDII06_MP1										
		BC From	PDII06-SO1 A	ctive	0	0 50 /	0 179		28/0	∆ −nor		
		CC From	PDII06-MP2 A	ctive	0	0.30	0.17	0 888	20/3	2B/c	7-noi	20
		BDU06-MP2	Active	CLIVE	0	0.10	0.1/	0.00%	icpu J.	20/3	A-1101	ile
		PC From	PDU06-901 A	ativo	0	0 50 /	0 109		30/0	∆-nor		
		CC TO	PDU06-MD1 A	ativo	0	0.30	0.10%	cpu 3		A=nor	1e	
		CC TO	RDUU6-MPI A	clive	0	0.10	0.083	scpu z	UB/S	A=nor	ie	
		RD006-NOI	ACLIVE		0	0 50 1	0 0	0.2.0	01 D	1-		
		AB TO	RDUU6-SUI A	ctive	0	0.50 1	18R U.	03%CD	ou ZIB	/ S		
		RDU06-SOI	Active		<u>,</u>							
		AB From	RDU06-NOI A	ctive	0	0.50 /	`0.04 ⁸	cpu 2	4B/s			
1		BC To	RDU06-MP1 A	ctive	0	0.50 1	1%R 0.	04%cp	ou 21B.	/s		
		BC To	RDU06-MP2 A	ctive	0	0.50 1	1%R 0.	07%cp	ou 21B	/s		
35	NOAM VIP GUI:	Click on Ma	ain Menu->S	tatus and	Mana	ger->l	Datab	ase				
55	Verify the											
	Database states	📄 🚍 S	tatus & Man	age								
		🧃	🕯 Network E	lements								
			Server									
			Derver									
		🌆) HA									
			⁹ Database									
			KP15									
		🚺	Processes									
		Verify that	the "OAM Ma	x HA Role'	' is eit	her "A	ctive"	or "S	tandb	v" for	NOA	М
		and SOAM	and "Applica	tion Max H	IA Rol	e" for	MPs i	s "Ac	tive", a	and th	at the	;
		status is "N	lormal" as she	own below:								
		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
		NO_10303	N02	Network OAM&P	Active	005	Normal	0	Normal	NotApplicab	I Allowed	AutoInProg
		SO_10303	PSBR MP2	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg
		SO_10303	S01	System OAM	Standby	OOS	Normal	0	Normal	NotApplicab	Allowed	AutoInProg
		NO_10303	N01	Network OAM&P	Standby	008	Normal	0	Normal	NotApplicab	I Allowed	AutoInProg
		SO_10303	IPFE S02	MP System OAM	Active	008	Normal	0	Normal	Normal	Allowed	AutoInProg
			002	ojotom Onin	P NOR Y C	000			Honnal	. too oppredu		Automit rog

36	NOAM VIP GUI: Verify the HA	Click on Main I	Menu	->Stat	us an	d Manage	e->HA		
	Status 🖕 📩 Status & Manage								
		💓 Ne	💿 🗄 🔤 💽 Network Elements						
			Conver						
			erver						
		🕼 HA	Δ						
		🚽 🔤 💽 Da	ataba	se					
		💓 KF	'IS						
		Dr	orace	00					
			ocess	000					
		Select the row	for all	of the	serve	ers			
		Verify that the '	'HA R	ole" is	eithe	r "Active" c	or "Standby".		
		,					1		
							-		
			0.000	Application	Max		-		
		Hostname	OAM Max HA Role	Application Max HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role	Active VIPs
		Hostname NO2	OAM Max HA Role Active	Application Max HA Role	Max Allowed HA Role Active	Mate Hostname List	Network Element	Server Role Network OAM&P	Active VIPs 10.240.70.132
		Hostname NO2 SO1	OAM Max HA Role Active Standby	Application Max HA Role 00S 00S	Max Allowed HA Role Active Active	Mate Hostname List NO1 SO2	Network Element NO_10303 S0_10303	Server Role Network OAM&P System OAM	Active VIPs 10.240.70.132
		Hostname NO2 SO1 SO2	OAM Max HA Role Active Standby Active	Application Max HA Role 00S 00S 00S	Max Allowed HA Role Active Active Active	Mate Hostname List NO1 SO2 SO1	Network Element NO_10303 SO_10303 SO_10303	Server Role Network OAM&P System OAM System OAM	Active VIPs 10.240.70.132 10.240.70.133
		Hostname NO2 SO1 SO2 MP1	OAM Max HA Role Active Standby Active Standby	Application Max HA Role OOS OOS OOS Active	Max Allowed HA Role Active Active Active Active	Mate Hostname List NO1 SO2 SO1 MP2	Network Element NO_10303 SO_10303 SO_10303 SO_10303	Server Role Network OAM&P System OAM System OAM MP	Active VIPs 10.240.70.132 10.240.70.133
		Hostname NO2 SO1 SO2 MP1 MP2	OAM Max HA Role Active Standby Active Standby Active	Application Max HA Role OOS OOS OOS Active Active	Max Allowed HA Role Active Active Active Active Active	Mate Hostname List NO1 SO2 SO1 MP2 MP1	Network Element No_10303 S0_10303 S0_10303 S0_10303 S0_10303 S0_10303	Server Role Network OAM&P System OAM MP MP	Active VIPs 10.240.70.132 10.240.70.133
		Hostname NO2 SO1 SO2 MP1 MP2 IPFE	Active Standby Active Standby Standby Active Active	Application Max HA Role OOS OOS OOS Active Active OOS	Max Allowed HA Role Active Active Active Active Active Active	Mate Hostname List NO1 SO2 SO1 MP2 MP1	Network Element NO_10303 SO_10303 SO_10303 SO_10303 SO_10303 SO_10303 SO_10303	Server Role Network OAM&P System OAM System OAM MP MP	Active VIPs 10.240 70.132 10.240 70.133
		Hostname NO2 SO1 SO2 MP1 MP2 IPFE	OAM Max HA Role Active Standby Active Standby Active Active	Application Max HA Role OOS OOS OOS Active Active OOS	Max Allowed HA Role Active Active Active Active Active Active	Mate Hostname List NO1 SO2 SO1 MP2 MP1	Network Element NO_10303 SO_10303 SO_10303 SO_10303 SO_10303 SO_10303	Server Role Network OAM&P System OAM System OAM MP MP MP	Active VIPs 10.240.70.132 10.240.70.133
		Hostname NO2 SO1 SO2 MP1 MP2 IPFE	OAM Max HA Role Active Standby Active Standby Active Active	Application Max HA Role OOS OOS OOS Active Active OOS	Max Allowed HA Role Active Active Active Active Active Active	Mate Hostname List NO1 SO2 SO1 MP2 MP1	Network Element NO_10303 S0_10303 S0_10303 S0_10303 S0_10303 S0_10303 S0_10303	Server Role Network OAM&P System OAM System OAM MP MP	Active VIPs 10.240.70.132 10.240.70.133
		Hostname NO2 SO1 SO2 MP1 MP2 IPFE	OAM Max HA Role Active Standby Active Standby Active Active	Application Max HA Role OOS OOS Active Active OOS	Max Allowed HA Role Active Active Active Active Active Active	Mate Hostname List NO1 SO2 SO1 MP2 MP1	Network Element NO_10303 SO_10303 SO_10303 SO_10303 SO_10303 SO_10303 SO_10303	Server Role Network OAM&P System OAM System OAM MP MP MP	Active VIPs 10.240.70.132 10.240.70.133

37	Active NOAM:	If recovering a DSR 5.0/6.0 system and POLICY AND CHARGING DRA
	Scope Data (If	application is activated then execute this step.
	POLICY AND CHARGING	Note: If recovering a DSR 7.0+ system, DO NOT execute this step
	DRA is activated): 5 0/6 0 Only	Login to the Active NOAM VIP via SSH terminal as <i>root(5.0) or admusr(6.0+)</i> user.
		Execute the following steps:
		Go to Appworks bin directory:
		<pre>\$ sudo cd /usr/TKLC/appworks/bin/</pre>
		Execute the PCRF sync script in "reportonly" mode to check whether PCRF data syncing is required or not. This is a read-only mode that does not modify the database:
		<pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -reportonly</pre>
		If the Report Summary shows one or more PCRFs "need to be synced", then repeat the script execution again but using the "sync" option instead of "reportonly" in order to sync the database.
		The "sync" option will modify the database:
		<pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -sync</pre>
		Re-execute the PCRF sync script in "reportonly" mode to verify all PCRF data is in sync. Examine the Report Summary output of the script. Verify the number of "PCRF record(s) processed in "total" is equal to the number of "PCRF record(s) already in sync":
		<pre>\$ sudo./syncPcrfReferencesAfterRestore.sh -reportonly</pre>





42	SOAM VIP GUI:	Navigate to Main Menu -> Diameter -> Maintenance -> Applications
	Enable Optional Features	Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups Applications DA-MPs Select the optional feature application configured in step 31. Click the Enable button. Enable Disable Pause updates
43	SOAM VIP GUI: Re-enable Transports if Needed (Applicable ONLY for DSR 6.0+)	Navigate to Main Menu->Transport Manager -> Maintenance -> Transport Transport Manager Configuration Maintenance Transport Select each transport and click on the Enable button Enable Disable Block Verify that the Operational Status for each transport is Up.
44	SOAM VIP GUI: Re-enable MAPIWF application if needed (Applicable ONLY for DSR 6.0+)	Navigate to Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users SS7/Sigtran Configuration Maintenance Cocal SCCP Users Remote Signaling Points Remote MTP3 Users Linksets Links Click on the Enable button corresponding to MAPIWF Application Name. Enable Disable Verify that the SSN Status is Enabled.

45	SOAM VIP GUI: Re-enable links if needed (Applicable ONLY for DSR 6.0+)	Navigate to Main Menu->SS7/Sigtran->Maintenance->Links
46	SOAM VIP GUI: Examine All Alarms	Navigate to Main Menu->Alarms & Events->View Active
47	NOAM VIP GUI: Examine All Alarms	Login to the NOAM VIP if not already logged in. Navigate to Main Menu->Alarms & Events->View Active
48	Restore GUI Usernames and Passwords	If applicable, Execute steps in Section 6.0 to recover the user and group information restored.
49 □	Backup and Archive All the Databases from the Recovered System	Execute Appendix A . DSR Database Backup to back up the Configuration databases:

5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)

For a partial outage with an NOAM server and an SOAM server intact and available, only base recovery of hardware and software is needed. The intact NO and SOAM servers are capable of restoring the database via replication to all 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 execute the procedure. The actual procedures' detailed steps are in Procedure 4. The major activities are summarized as follows:

Recover Standby NOAM server by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.

The database is intact at the active NOAM server and does not require restoration at the standby NOAM server.

- Recover any failed SO and MP servers by recovering base hardware and software.
- Recover the base hardware.
- Recover the software.

The database in intact at the active NOAM server and does not require restoration at the SO and MP servers.

• Re-apply signaling networks configuration if the failed blade is an MP.

S T F	This procedure pe server is intact and	rforms recovery if at least 1 NOAM server is intact and available and 1 SOAM d available.
– P #	Check off (√) each step number.	n step as it is completed. Boxes have been provided for this purpose under each
	If this procedure fa	ails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.
1	Workarounds	Refer to Appendix G . Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
2	Gather Required Materials	Gather the documents and required materials listed in Section 3.1 Required Materials
3	NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:
		http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>
		Login as the <i>guiadmin</i> user:
		ORACLE
		Oracle System Login Fri Mar 20 12:29:52 2015 EDT
		Enter your username and password to log in
		Username: guiadmin Password: ••••••
		Change password
		Log in
		Welcome to the Oracle System Login.
		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.

		No. Sector to Mala Manage Officer O. Manager J. J.A.
4		Navigate to main menu -> Status & manage -> HA
	Set Falled	
	Standby	📋 🤤 Status & Manage
	Clandby	🔤 🔤 Network Elements
		Server
		🔤 💽 Database
		- Martin KPIs
		- Martin - M
		Select Edit
		Set the Max Allowed HA Role drop down box to Standby for the failed servers.
		Select Ok
		Ok Cancel
_	RMS NOAM	1. HW vendor to replace the failed equipment
4		
5	Failure	
5	Failure	2. Execute the <i>"iLO Configuration Procedure"</i> appendix from [3]
5	Failure	2. Execute the <i>"iLO Configuration Procedure"</i> appendix from [3]
5	Failure	 Execute the <i>"iLO Configuration Procedure"</i> appendix from [3] Recover the PMAC and any associated hardware, OAs, and switches
5	Failure	 Execute the <i>"iLO Configuration Procedure"</i> appendix from [3] Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for
5	Failure	 Execute the <i>"iLO Configuration Procedure"</i> appendix from [3] Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference.
5	Failure	 Execute the "<i>iLO Configuration Procedure</i>" appendix from [3] Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference. Confirm necessary software images are present on the PMAC.
5	Failure	 Execute the <i>"iLO Configuration Procedure"</i> appendix from [3] Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference. Confirm necessary software images are present on the PMAC.
5	Failure	 Execute the <i>"iLO Configuration Procedure"</i> appendix from [3] Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference. Confirm necessary software images are present on the PMAC. If the failed NOAM is co-hosted with the PMAC on the first rack mount
5	Failure	 Execute the <i>"iLO Configuration Procedure"</i> appendix from [3] Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference. Confirm necessary software images are present on the PMAC. If the failed NOAM is co-hosted with the PMAC on the first rack mount server, execute procedure <i>"Continue TVOE Configuration on First RMS</i>
5	Failure	 Execute the "iLO Configuration Procedure" appendix from [3] Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference. Confirm necessary software images are present on the PMAC. If the failed NOAM is co-hosted with the PMAC on the first rack mount server, execute procedure "Continue TVOE Configuration on First RMS Server" - Refer to Table 5 for the applicable DSR software
5	Failure	 Execute the "iLO Configuration Procedure" appendix from [3] Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference. Confirm necessary software images are present on the PMAC. If the failed NOAM is co-hosted with the PMAC on the first rack mount server, execute procedure "Continue TVOE Configuration on First RMS Server" - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.
5	Failure	 Execute the <i>"iLO Configuration Procedure"</i> appendix from [3] Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference. Confirm necessary software images are present on the PMAC. If the failed NOAM is co-hosted with the PMAC on the first rack mount server, execute <i>procedure "Continue TVOE Configuration on First RMS Server"</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference. If the failed NOAM is NOT co-hosted with the PMAC on the first rack
5	Failure	 Execute the "iLO Configuration Procedure" appendix from [3] Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference. Confirm necessary software images are present on the PMAC. If the failed NOAM is co-hosted with the PMAC on the first rack mount server, execute procedure "Continue TVOE Configuration on First RMS Server" - Refer to Table 5 for the applicable DSR software installation/configuration guide reference. If the failed NOAM is NOT co-hosted with the PMAC on the first rack mount server, execute procedure "Configure TVOE on Additional RMS
5	Failure	 Execute the <i>"iLO Configuration Procedure"</i> appendix from [3] Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference. Confirm necessary software images are present on the PMAC. If the failed NOAM is co-hosted with the PMAC on the first rack mount server, execute <i>procedure "Continue TVOE Configuration on First RMS Server"</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference. If the failed NOAM is NOT co-hosted with the PMAC on the first rack mount server, execute procedure <i>"Configure TVOE on Additional RMS Servers(s)"</i> - Refer to Table 5 for the applicable DSR software
5	Failure	 Execute the <i>"iLO Configuration Procedure"</i> appendix from [3] Recover the PMAC and any associated hardware, OAs, and switches Refer to Table 6: DSR PMAC Disaster Recovery Reference Table for the applicable PMAC disaster recovery reference. Confirm necessary software images are present on the PMAC. If the failed NOAM is co-hosted with the PMAC on the first rack mount server, execute <i>procedure "Continue TVOE Configuration on First RMS</i> <i>Server"</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference. If the failed NOAM is NOT co-hosted with the PMAC on the first rack mount server, execute procedure <i>"Configure TVOE on Additional RMS</i> <i>Servers</i>(s)" - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.

6	HP-Class Blade	If the failed server is an HP C-Class Blade, execute this step; otherwise skip to
	Failure	the next step.
		1. HW vendor to replace the failed equipment
		 Execute procedure "Confirm/Update blade Server BIOS Settings" – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference.
		 Execute procedure "Configure Blade Server iLO Password for Administrator Account" – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference.
		 Perform any needed firmware upgrades – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference
		 For NOAM/SOAM TVOE Host servers, execute procedure "IPM Servers Using PM&C Application" - Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference.
7	Configure TVOE on Server Blades	For NOAMs on TVOE server Blades and SOAMs, execute procedure "Configure TVOE on Server Blades" - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.
8	Create VMs	For NOAMs, execute procedure <i>"Create NOAM Guest VMs"</i> - Refer to Table 5 : DSR Software Installation/Configuration Reference Table for the applicable DSR software installation/configuration guide reference.
		For SOAMs, execute procedure <i>"Create SOAM Guest VMs"</i> - Refer to Table 5: DSR Software Installation/Configuration Reference Table for the applicable DSR software installation/configuration guide reference.
9	IPM Failed Guest/Servers	IPM the failed guests/servers by executing procedure <i>"IPM Blades and VMs"</i> - Refer to Table 5: DSR Software Installation/Configuration Reference Table for the applicable DSR software installation/configuration guide reference.
10	Install DSR	Install the DSR application on the failed guests/server by executing procedure
	application on Failed	<i>Install Application Software on Blades"</i> - Refer to Table 5: DSR Software Installation/Configuration Reference Tablefor the applicable DSR software
	Guests/Servers	installation/configuration guide reference.
11	Repeat for	If necessary, repeat steps 1-7 for all remaining failed servers.
	Remaining Failed Servers	

	NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: http:// <primary_noam_vip_ip_address> Login as the <i>guiadmin</i> user: ORACLE Oracle System Login</primary_noam_vip_ip_address>
		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 Velcome 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.
13	NOAM VIP GUI: Recover Standby NOAM if needed	If the failed server is a NOAM, install the second NOAM server by executing procedure <i>"Configure the Second NOAM Server"</i> , steps 1, 4, 5, 6 - Refer to Table 5: DSR Software Installation/Configuration Reference Table for the applicable DSR software installation/configuration guide reference. Note: Execute step 7 if Netbackup is used. If NetBackup is used, execute procedure <i>"Install NetBackup Client"</i> - Refer to Table 5: DSR Software Installation/Configuration Reference Table for the applicable DSR software installation/Configuration Reference Table for the applicable DSR software Installation/Configuration Reference Table for the applicable DSR software installation/Configuration Reference Table for the applicable DSR software installation/Configuration guide reference.
14	NOAM VIP GUI: Recover the Failed SOAM Servers if needed	 If the failed server is an SOAM, recover the remaining SOAM servers (standby, spare) by repeating the following steps for each SOAM server: 1. Install the remaining SOAM servers by executing reference Procedure <i>"Configure the SOAM Servers"</i>, steps 1, 5, 6, 7, and 8 Refer to Table 5: DSR Software Installation/Configuration Reference Table for the applicable DSR software installation/configuration guide reference. Note: Execute step 10 as well if Netbackup is used. 2. If you are using Netbackup, execute procedure <i>"Install Netbackup Client"</i> - Refer to Table 5: DSR Software Installation/Configuration Reference Table for the applicable for the applicable 5: not set to the text of text of text of the text of the text of text of text of text of text of text of the text of t

15	NOAM VIP GUI: Set HA on Recovered Servers	Navigate to Status & Manage -> HA
		 Catabase KPIs Processes Tasks Files
		Click on Edit at the bottom of the screen
		For each server whose Max Allowed HA Role is set to Standby, set it to Active
		Press OK
16	Recovered Server: Login	Establish an SSH to the recovered server's XMI address:
17	Recovered Server: Sync NTP	 Perform the following to retrieve the remote NTP server: \$ sudo ntpq -np
		Example output:
		<pre>[admusr@NOAM-2 ~]\$ ntpq -np remote refid st t when poll reach delay offset jitter ===================================</pre>
		======================================
		2) Stop ntpd service:
		\$ sudo service ntpd stop
		3) Sync the date to the ntp remote server:
		<pre>\$ sudo ntpdate <ntp remote="" server=""></ntp></pre>
		Note: The remote server below will be that of the one gathered in sub step 1.
		4) Start the ntp service:
		<pre>\$ sudo service ntpd start</pre>

18	NOAM VIP GUI:	Navigate to Main Menu->Status & Manage->Server,
	Restart DSR application	Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered server and click on Restart .
19	NOAM VIP GUI: Recover the C- Level Server (DA-MP, SBRs, IPFE, SS7-MP)	 Execute procedure "Configure MP Blades Servers", Steps 1-2, and 6-9 Refer to Table 5: DSR Software Installation/Configuration Reference Table for the applicable DSR software installation/configuration guide reference. Note: Also execute step 10-12 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. Note: -DSR 5.0/6.0/7.0 ONLY: If this server is an IPFE server, ensure ipfeNetUpdate.sh from procedure "IP Front End (IPFE) Configuration (Optional)" from [17] has been executed. Repeat this step for any remaining failed MP servers.
20	NOAM VIP GUI: Restart DSR Application on recovered C- Level Servers.	Navigate to Main Menu->Status & Manage Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered servers and click on Restart. Stop Restart Reboot NTP Sync Report

21	NOAM VIP GUI: Set HA on all C- Level Servers	Navigate to Status & Manage Status & Manage Network Elements Server Database MPIS Processes Files
		Click on Edit at the bottom of the screen
		For each server whose Max Allowed HA Role is set to Standby, set it to Active
		Press OK
22	ACTIVE NOAM: Login	Login to the recovered Active NOAM via SSH terminal as root (5.0) or admusr(6.0+) user.
23	Active SOAM:	For DSR 5.0/6.0/7.0: If DSR 7.1, skip this step
	recovered SOAM for	Establish an SSH session to the Active SOAM, login as admusr.
	optional feature activation (DSR	Execute the following command:
	5.0/6.0/7.0)	<pre>\$ irem DsrApplication where "name in ('RBAR','FABR','PCA','MD-IWF','DM-IWF','CPA','GLA')"</pre>
24	Active SOAM:	For DSR 5.0/6.0/7.0: If DSR 7.1, skip this step.
	Preparation (DSR 5.0/6.0/7.0)	Execute the following command to verify preparation of optional feature activation:
		<pre>\$ iqt -z -h -p -fname DsrApplication where "name in ('RBAR','FABR','PCA','MD-IWF','DM-IWF','CPA','GLA')"</pre>
		Note: There should be no output of this command, if there is, verify the correct entry of the command in step 22 .
25	ACTIVE NOAM: Perform key	Establish an SSH session to the Active NOAM, login as <i>admusr.</i>
	exchange between the active-NOAM	Execute the following command to perform a keyexchange from the active NOAM to each recovered server:
	and recovered servers.	S keyexchange admusr@ <recovered hostname="" server=""></recovered>

26	ACTIVE NOAM:	Establish an SSH session to the active NOAM, login as admusr.								
	Optional	Refer to section								
	Features	1.5 Optional Featuresto activate any features that were previously activated.								
27	NOAM VIP GUI:	Navigate to Configuration-> Server -> Database								
27	Fetch and Store									
27	NOAM VIP GUI: Fetch and Store the database Report for the Newly Restored Data and Save it	Navigate to Configuration-> Server -> Database								
		Click on Save and save the report to your local machine								

28	ACTIVE NOAM:	Login to the	e Active NOAN	/l via SSH	termi	nal as	root(′5.0) o	or adn	nusr(6	6.0+)	user.
20	Verify	Execute the following command:										
	Replication	A such increases a										
	Servers.	\$ sudo :	irepstat -r	n								
		Output like	e below shall l	be genera	ted:							
	Doliou O NotCth (DeDorlisstics)											
		RDU06-MP1	Stby									
		BC From	RDU06-SO1 Ac	tive	0	0.50 ^	0.17%	cpu 4	2B/s	A=non	le	
		CC From	RDU06-MP2 Ac	tive	0	0.10 ^	0.17	0.88%	cpu 3	2B/s	A=noi	ne
		RDU06-MP2	Active									
		BC From	RDU06-SO1 Ac	tive	0	0.50 ^	0.10%	cpu 3	3B/s	A=non	le	
		CC To	RDU06-MP1 Ac	tive	0	0.10	0.08%	cpu 2	0B/s	A=non	le	
		RDU06-NO1	Active									
		AB To	RDU06-SO1 Ac	tive	0	0.50 1	.%R 0.	03%cp	ou 21B	/s		
		RDU06-SO1	Active									
		AB From	RDU06-NO1 Ac	tive	0	0.50 ^	0.04%	cpu 2	4B/s			
		BC To	RDU06-MP1 Ac	tive	0	0.50 1	.%R 0.	04%cp	ou 21B	/s		
		BC To	RDU06-MP2 Ac	tive	0	0.50 1	.%R 0.	07%cp	ou 21B	/s		
29	NOAM VIP GUI:	Click on Ma	ain Menu->St	atus and	Mana	ger->I	Datab	ase				
_	Verify the	÷ • •										
	Database states		tatus & Mana 	ige								
		🚺	Network Ele	ements								
		🧃	Server									
			нΔ									
			Database									
		🦉	KPIs									
		🜆										
			a									
		Verify that t			' ic oit	hor "Δ	ctivo"	or "S	tandh	v" for		N/
		and SOAM	and "Applicat	ion Max H		e" for	MPs i	s "Act	tive" a	and the	at the	1VI
		status is "N	ormal" as sho	wn below:		0 101		0 / 10				
		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
		NO_10303	N02	Network OAM&P	Active	008	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg
		SO_10303 SO_10303	PSBR MP2	MP	Active Active	Active Active	Normal Normal	0	Normal Normal	Normal Normal	Allowed	AutoInProg AutoInProg
		SO_10303	S01	System OAM	Standby	008	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg
		NO_10303	NO1	Network OAM&P	Standby	008	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg
		SO_10303	S02	System OAM	Active	005	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg

	Click on Main I	Menu	->Stat	us an	d Manage	e->HA			
Status	🚔 🚔 Status & Manage								
Clarad	📮 🦕 Status & Manage								
	🔤 💽 Network Elements								
	Conver								
	Server 🔤 Server								
		•							
	💽 Da	ataba	se						
	💓 KI	21S							
	Dr	ocaee	00						
		oceaa	000						
	Select the row	Select the row for all of the servers							
	Verify that the "HA Role" is either "Active" or "Standby".								
			ole" is	eithe	r "Active" o	or "Standby".			
			Ole" is	eithe ^{Max}	r "Active" o	or "Standby".			
	Hostname	OAM Max HA Role	Ole" is Application Max HA Role	eithe Max Allowed HA Role	r "Active" o	Dr "Standby".	Server Role	Active VIPs	
	Hostname NO2	OAM Max HA Role Active	Ole" is Application Max HA Role	eithe Max Allowed HA Role Active	r "Active" (Mate Hostname List NO1	Dr "Standby". Network Element N0_10303	Server Role Network OAM&P	Active VIPs 10.240.70.132	
	Hostname NO2 SO1	OAM Max HA Role Active Standby	Application Max HA Role	eithe Max Allowed HA Role Active Active	r "Active" c Mate Hostname List NO1 SO2	Network Element N0_10303 80_10303	Server Role Network OAM&P System OAM	Active VIPs 10.240.70.132	
	Hostname NO2 SO1 SO2	OAM Max HA Role Active Standby Active	Ole" is Application Max HA Role 00S 00S 00S	Max Allowed HA Role Active Active Active	r "Active" c Mate Hostname List NO1 SO2 SO1	Network Element N0_10303 S0_10303 S0_10303	Server Role Network OAM&P System OAM System OAM	Active VIPs 10.240.70.132 10.240.70.133	
	Hostname NO2 SO1 SO2 MP1	OAM Max HA Role Active Standby Active Standby	Ole" is Application Max HA Role OOS OOS OOS Active	Active Active Active Active	r "Active" c Mate Hostname List NO1 SO2 SO1 MP2	Network Element N0_10303 S0_10303 S0_10303 S0_10303	Server Role Network OAM&P System OAM System OAM	Active VIPs 10.240.70.132 10.240.70.133	
	Hostname NO2 SO1 SO2 MP1 MP2	OAM Max HA Role Active Standby Active Standby Active	Ole" is Application Max HA Role OOS OOS OOS Active Active	eithe	r "Active" c Mate Hostname List NO1 SO2 SO1 MP2 MP1	Network Element N0_10303 S0_10303 S0_10303 S0_10303 S0_10303 S0_10303	Server Role Network OAM&P System OAM System OAM MP MP	Active VIPs 10.240.70.132 10.240.70.133	
	Hostname NO2 SO1 SO2 MP1 MP2 IPFE	OAM Max HA Role Active Standby Active Standby Active Active	Ole" is Application Max HA Role OOS OOS OOS Active Active OOS	Active Active Active Active Active Active Active Active Active Active	Mate Hostname List NO1 SO2 SO1 MP2 MP1	Network Element N0_10303 S0_10303 S0_10303 S0_10303 S0_10303 S0_10303 S0_10303 S0_10303	Server Role Network OAM&P System OAM System OAM MP MP MP	Active VIPs 10.240.70.132 10.240.70.133	
	Hostname NO2 SO1 SO2 MP1 IPFE	OAM Max HA Role Active Standby Active Standby Active Active	Ole" is Application Max HA Role OOS OOS OOS Active Active OOS	eithe Allowed HA Role Active Active Active Active Active Active Active	n "Active" (Mate Hostname List NO1 SO2 SO1 MP2 MP1	Network Element N0_10303 S0_10303 S0_10303 S0_10303 S0_10303 S0_10303 S0_10303 S0_10303 S0_10303	Server Role Network OAM&P System OAM System OAM MP MP MP	Active VIPs 10.240.70.132 10.240.70.133	
	Hostname NO2 SO1 SO2 MP1 MP2 IPFE	OAM Max HA Role Active Standby Active Standby Active Active	Ole" is Application Max HA Role OOS OOS OOS Active Active OOS	eithe Max Allowed HA Role Active Active Active Active Active Active	Mate Hostname List NO1 SO2 SO1 MP2 MP1	Network Element NO_10303 SO_10303 SO_10303 SO_10303 SO_10303 SO_10303 SO_10303 SO_10303 SO_10303	Server Role Network OAM&P System OAM System OAM MP MP MP MP	Active VIPs 10.240.70.132 10.240.70.133	
	Hostname NO2 SO1 SO2 MP1	OAM Max HA Role Active Standby Active Standby	Ole" is Application Max HA Role OOS OOS OOS Active	Active Active Active Active	r "Active" c Mate Hostname List NO1 SO2 SO1 MP2	Network Element N0_10303 S0_10303 S0_10303 S0_10303	Server Networ System System MP	Role k OAM&P i OAM i OAM	

31	Active NOAM:	If recovering a DSR 5.0/6.0 system and POLICY AND CHARGING DRA
	Scope Data (If	application is activated then execute this step.
	POLICY AND CHARGING	Note: If recovering a DSR 7.0+ system, DO NOT execute this step
	DRA is activated): 5.0/6.0 Only	Login to the Active NOAM VIP via SSH terminal as <i>root(5.0) or admusr(6.0+)</i> user.
		Execute the following steps:
		Go to Appworks bin directory:
		<pre>\$ sudo cd /usr/TKLC/appworks/bin/</pre>
		Execute the PCRF sync script in "reportonly" mode to check whether PCRF data syncing is required or not. This is a read-only mode that does not modify the database:
		<pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -reportonly</pre>
		If the Report Summary shows one or more PCRFs "need to be synced", then repeat the script execution again but using the "sync" option instead of "reportonly" in order to sync the database.
		The "sync" option will modify the database:
		<pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -sync</pre>
		Re-execute the PCRF sync script in "reportonly" mode to verify all PCRF data is in sync. Examine the Report Summary output of the script. Verify the number of "PCRF record(s) processed in "total" is equal to the number of "PCRF record(s) already in sync":
		<pre>\$ sudo./syncPcrfReferencesAfterRestore.sh -reportonly</pre>




37	SOAM VIP GUI:	Navigate to Main Menu -> Diameter -> Maintenance -> Applications
	Features	Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups Applications DA-MPs Select the optional feature application configured in step 22. Click the Enable button. Enable Disable Pause updates
38	SOAM VIP GUI: Re-enable Transports if Needed (Applicable ONLY for DSR 6.0+)	Navigate to Main Menu->Transport Manager -> Maintenance -> Transport Transport Manager Configuration Maintenance Maintenance Transport Select each transport and click on the Enable button Enable Disable Block Verify that the Operational Status for each transport is Up.
39	SOAM VIP GUI: Re-enable MAPIWF application if needed (Applicable ONLY for DSR 6.0+)	Navigate to Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users



44	Backup and Archive All the Databases from the Recovered System	Execute Appendix A . DSR Database Backup to back up the Configuration databases:
	System	

5.1.5 Recovery Scenario 5 (Both NOAM servers failed with DR-NOAM available)

For a partial outage with both NOAM servers failed but a DR NOAM available, the DR NOAM is switched from secondary to primary then recovers the failed NOAM 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 execute the procedure. The actual procedures' detailed steps are in Procedure 5. The major activities are summarized as follows:

Switch DR NOAM from secondary to primary

Recover the failed NOAM servers by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.
- The database is intact at the newly active NOAM server and does not require restoration.

If applicable, recover any failed SOAM and MP servers by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.
- The database in intact at the active NOAM server and does not require restoration at the SOAM and MP servers.

S	This procedure pe	rforms recovery if both NOAM servers have failed but a DR NOAM is available	
E P #	Check off ($\sqrt{2}$) each step as it is completed. Boxes have been provided for this purpose under each step number.		
	If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.		
1	Workarounds	Refer to Appendix G . Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.	
2	Gather Required Materials	Gather the documents and required materials listed in Section 3.1 Required Materials	
3	Switch DR NOAM to Primary	Execute Appendix C . Switching DR NOAM Site to Primary to have the DR NOAM become active.	

4	Recover System	If ALL	SOAM servers have failed, execute Procedure 2
	oystem	If ALL	NOAM servers have failed, execute the following steps:
		1)	Procedure 4: Steps 3-7, 8-10
		2)	Perform a keyexchange between the newly active NOAM and the recovered NOAM PMAC:
			From a terminal window connection on the active NOAM as the <i>admusr</i> user, exchange SSH keys for <i>admusr</i> between the active NOAM and the recovered NOAM's PMAC server using the keyexchange utility, using the management IP address for the PMAC server.
			When prompted for the password, enter the password for the <i>admusr</i> user of the PMAC server.
			<pre>\$ keyexchange admusr@<recovered_pmac_ip address=""></recovered_pmac_ip></pre>
			Note: if keyexchange fails, edit /home/admusr/.ssh/known_hosts and remove blank lines, and retry the keyexchange commands.
		3)	Use the PMAC GUI to determine the control network IP address of the recovered VMs. From the PMAC GUI, navigate to Main Menu -> Software -> Software Inventroy
			Perform a keyexchange between the recovered PMAC and the recovered guests:
			From a terminal window connection on the recovered PMAC as the <i>admusr</i> user, exchange SSH keys for <i>admusr</i> between the PMAC and the recovered VM guests using the keyexchange utility, using the control network IP addresses for the VM guests
			When prompted for the password, enter the password for the <i>admusr</i> user of the VM guest.
			<pre>\$ keyexchange admusr@<recovered_vm_control_ip address=""></recovered_vm_control_ip></pre>
			Note: if keyexchange fails, edit /home/admusr/.ssh/known_hosts and remove blank lines, and retry the keyexchange commands.
		4)	Procedure 4: 12-13(For each NOAM))

5	Perform Key exchange between Active NOAM and Recovered NOAMs	Perform a keyexchange between the newly active NOAM and the recovered NOAM servers: From a terminal window connection on the active NOAM as the admusr user, exchange SSH keys for admusr between the active NOAM and the recovered NOAM servers using the keyexchange utility, using the host names of the recovered NOAMs. When prompted for the password, enter the password for the admusr user of the recovered NOAM servers. \$ keyexchange admusr@<recovered_noam hostname=""></recovered_noam>
6	NOAM VIP GUI: Restart DSR application	Navigate to Main Menu->Status & Manage Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select each recovered NOAM server and click on Restart. Stop Restart Reboot NTP Sync Report

7	NOAM VIP GUI: Set HA on Recovered NOAMs	Navigate to Status & Manage Status & Manage Network Elements Server Database KPIs Processes Files Click on Edit at the bottom of the screen For each NOAM server whose Max Allowed HA Role is set to Standby, set it to Active Press OK
8	Recovered Active NOAM: Prepare	For DSR 5.0/6.0/7.0: If DSR 7.1, skip this step. Establish an SSH session to the Active SOAM, login as <i>admusr.</i>
	NOAM for optional feature	Execute the following command:
	activation (DSR 5.0/6.0/7.0)	<pre>\$ irem DsrApplication where "name in ('PCA','MD- IWF','DM-IWF')"</pre>
9	Recovered Active NOAM:	For DSR 5.0/6.0/7.0: If DSR 7.1, skip this step
	Verify Preparation (DSR	Execute the following command to verify preparation of optional feature activation:
	5.0/6.0/7.0)	<pre>\$ iqt -z -h -p -fname DsrApplication where "name in ('PCA','MD-IWF','DM-IWF')"</pre>
		Note: There should be no output of this command, if there is, verify the correct entry of the command in step 5 .

10	Recovered Active NOAM: Activate Optional Features	Establish an SSH session to the Active NOAM, login as admusr . If PCA was previously activated, execute the following commands: \$ cd /usr/TKLC/dsr/prod/maint/loaders/activate \$./load.pcaActivateStandByAscoped If MAP-Diameter IWF was previously activated, execute the following
		<pre>commands: \$ cd /usr/TKLC/dsr/prod/maint/loaders/activate \$./load.mapinterworkingActivateAsourced</pre>
11	Recovered Standby NOAM: Prepare and Activate Recovered Standby NOAM for Optional Feature Activation.	Repeat Steps 5-7 for the preparing and activating previously activated features on the recovered Standby NOAM.
12	Switch DR NOAM Back to Secondary	Once the system have been recovered: Execute Appendix D . Returning a Recovered Site to Primary to have the recovered NOAM become primary again.
13	Recovered Servers: Verify Alarms	Navigate to Main Menu -> Alarms & Events -> View Active

5.1.6 Recovery Scenario 6 (Database Recovery)

5.1.6.1 Recovery Scenario 6: 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.DSR.HPC02-NO2.FullDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2
 - o Backup.DSR.HPC02-NO2.FullRunEnv.NETWORK_OAMP.20140524_223507.UPG.tar.bz2

Note: During recovery, the corrupted Database will get replaced by the sever Runtime backup. Any configuration done after taking the backup will not be visible post recovery.

Procedure 6: Recovery Scenario 6 (Case 1)

S	This procedure pe	This procedure performs recovery if database is corrupted in the system		
T E P #	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.			
		, , , , , , , , , , , , , , , , , , ,		
1	Workarounds	Refer to Appendix G . Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.		
2	NOAM VIP GUI: Set Failed Servers to Standby	Navigate to Main Menu -> Status & Manage -> HA		

Procedure 6: Recovery Scenario 6 (Case 1)

3	Server in Question: Login	Establish an SSH session to the server in question. Login as <i>root(5.0)</i> or <i>admusr(6.0+)</i> user.
	6	
4	Server in Question:	Execute the following command to bring the system to runlevel 3.
	Change runlevel to 3	\$ sudo init 3
5	Server in Question: Recover System	Execute the following command and follow the instructions appearing the console prompt
		<pre>\$ sudo /usr/TKLC/appworks/sbin/backout_restore</pre>
6	Server in Question:	Execute the following command to bring the system back to runlevel 4.
	Change runlevel to 4	<pre>\$ sudo init 6</pre>
7	Server in Question:	Execute the following command to verify if the processes are up and running
	Verify the server	<pre>\$ sudo pm.getprocs</pre>
8	NOAM VIP GUI: Set Failed	Navigate to Status & Manage -> HA
	Servers to Active	Status & Manage Network Elements Server
		💽 Database 🛅 KPIs
		Processes
		🖬 🛅 Tasks
		Click on 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

Procedure 6: Recovery Scenario 6 (Case 1)

9	Active NOAM: Verify Sync Split	If recovering a DSR 5.0/6.0 system and POLICY AND CHARGING DRA application is activated then execute this step.
	Scope Data (If POLICY AND	Note: If recovering a DSR 7.0+ system, DO NOT execute this step
	DRA is activated): 5.0/6.0.001v	Login to the Active NOAM VIP via SSH terminal as <i>root(5.0) or admusr(6.0+)</i> user.
		Execute the following steps:
		Go to Appworks bin directory:
		<pre>\$ sudo cd /usr/TKLC/appworks/bin/</pre>
		Execute the PCRF sync script in "reportonly" mode to check whether PCRF data syncing is required or not. This is a read-only mode that does not modify the database:
		<pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -reportonly</pre>
		If the Report Summary shows one or more PCRFs "need to be synced", then repeat the script execution again but using the "sync" option instead of "reportonly" in order to sync the database.
		The "sync" option will modify the database:
		<pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -sync</pre>
		Re-execute the PCRF sync script in "reportonly" mode to verify all PCRF data is in sync. Examine the Report Summary output of the script. Verify the number of "PCRF record(s) processed in "total" is equal to the number of "PCRF record(s) already in sync":
		<pre>\$ sudo./syncPcrfReferencesAfterRestore.sh -reportonly</pre>
10	Backup and Archive All the Databases from the	Execute Appendix A . DSR Database Backup to back up the Configuration databases:
	Recovered System	

5.1.6.2 Recovery Scenario 6: Case 2

For a partial outage with

- Server having a corrupted database
- Replication channel is not inhibited or
- Server has the same release as that of its Active parent

Procedure 7: Recovery Scenario 6 (Case 2)

S T E	This procedure performs recovery if database got corrupted in the system and system is in the state to get replicated			
С Р #	Check off (√) each step number.	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.		
	If this procedure fa	ails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.		
1	Workarounds	Refer to Appendix G . Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.		
2	NOAM VIP GUI: Set Failed Servers to Standby	Navigate to Main Menu -> Status & Manage -> HA Status & Manage Network Elements Server Database KPIs Processes Select Edit Set the Max Allowed HA Role drop down box to Standby for the failed servers. Select Ok Ok Cancel		
3	Server in Question: Login	Establish an SSH session to the server in question. Login as <i>root(5.0)</i> or <i>admusr(6.0+)</i> user.		
4	Server in Question: Take Server out of Service	Execute the following command to take the server out of service. \$ sudo bash -1 \$ sudo prod.clobber		

Procedure 7: Recovery Scenario 6 (Case 2)

5	Server in Question: Take Server to DbUp State and Start the Application	Execute the following commands to take the server to Dbup and start the DSR application: \$ sudo bash -1 \$ sudo prod.start	
6	Server in Question: Verify the Server State	Execute the following commands to verify the processes are up and running: \$ sudo pm.getprocs Execute the following command to verify if replication channels are up and running: \$ sudo irepstat Execute the following command to verify if merging channels are up and running:	
7	NOAM VIP GUI: Restart DSR application	Navigate to Main Menu->Status & Manage Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select each recovered server and click on Restart. Stop Restart Reboot NTP Sync Report	

Procedure 7: Recovery Scenario 6 (Case 2)

8	NOAM VIP GUI:	Navigate to Status & Manage -> HA
	Set Failed Servers to Active	Status & Manage Network Elements Server Database KPIs Processes Files Click on 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
9	Backup and Archive All the Databases from the Recovered System	Execute Appendix A . DSR Database Backup to back up the Configuration databases:

6.0 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 will not impact security or accessibility.

6.1 Restoring a Deleted User

- User 'testuser' exists in the selected backup file but not in the current database.

These users were removed prior to creation of the backup and archive file. They will be reintroduced by system restoration of that file.

6.2 Keeping a Restored user

Procedure 8: Keep Restored User

S T	Perform this proce	edure to keep users that will be restored by system restoration.
- E P #	Check off (√) eacl step number.	n step as it is completed. Boxes have been provided for this purpose under each
	If this procedure f	ails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.
1	Before Restoration: Notify Affected Users Before Restoration	Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.
2	After Restoration:	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:
	NOAM VIP	http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>
		Login as the <i>guiadmin</i> user: CRACLE® Oracle System Login Fri Mar 20 12:29:52 2015 EDT
		Log In Enter your username and password to log in Username: guiadmin Password: Other password Change password Change password Log In Device 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.

Procedure 8: Keep Restored User

2	After	Navigate to Administration -> Access Control -> Users
3	Restoration:	
	Reset User Passwords	 Main Menu Administration General Options Access Control Cessions Sessions Certificate Management Authorized IPs SFTP Users
		Select the user
		Click the Change Password button
		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 the Continue button

6.3 Removing a Restored User

Procedure 9: Remove the Restored User

S T	Perform this proce	edure to remove users that will be restored by system restoration
E P #	Check off (√) each step number.	step as it is completed. Boxes have been provided for this purpose under each
п	If this procedure fa	ails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.
1	After Restoration: Login to the NOAM VIP	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: <pre>http://<primary_noam_vip_ip_address></primary_noam_vip_ip_address></pre>
		<text><image/><section-header><section-header><section-header><form></form></section-header></section-header></section-header></text>

Procedure 9: Remove the Restored User

2	After Restoration:	Navigate to Administration -> Access Control -> Users
	Reset User Passwords	Main Menu General Options General Options Access Control General General Certificate Management Authorized IPs SFTP Users Select the user
		Click the Delete button
		Insert Edit Delete Report Change Password
		Delete selected users?
		OK Cancel
		Click the OK button to confirm.

6.4 Restoring a Modified User

These users have had a password change prior to creation of the backup and archive file. The will be reverted by system restoration of that file.

- The password for user 'testuser' 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 will reset their password during this maintenance operation.

After Restoration:

Log in and reset the passwords for all users in this category. See the steps in **Procedure 8** for resetting passwords for a user.

6.5 Restoring an Archive that does not contain a Current User

These users have been created after the creation of the backup and archive file. The will be deleted by system restoration of that file.

- User 'testuser' exists in current database but not in the selected backup file.

If the user is no longer desired, do not perform any additional steps. The user is permanently removed.

Procedure 10: Restoring an Archive that does not Contain a Current User

S T	Perform this proce	edure to remove users that will be restored by system restoration
E P #	Check off (√) each step number.	n step as it is completed. Boxes have been provided for this purpose under each
	If this procedure fa	ails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.
1	Before Restoration: Notify Affected Users Before Restoration	Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.
2	Before Restoration:	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:
	NOAM VIP	http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>
		Login as the <i>guiadmin</i> 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.
		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.

Procedure 10: Restoring an Archive that does not Contain a Current User

	Before	Navigate to Administration -> Access Control -> Users
3	Restoration:	
	Record user	🖻 🚊 Main Menu
	settings	📋 🚔 Administration
		General Options
		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	Establish a GUI session on the NOAM server by using the VIP IP address of the
4	Restoration:	NOAM server. Open the web browser and enter a URL of:
	Login	http:///Doing.wo.NO.W. UTD. TD. http://www.
		http://tpimary_NOAM_VIP_IP_Address/
		Login as the quiadmin user:
		ORACLE
		Oracle System Login
		Log In
		Dessword:
		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.

Procedure 10: Restoring an Archive that does not Contain a Current User



7.0 IDIH Disaster Recovery

The fdconfig xml file you use for disaster recovery is different from the one used for fresh installation. The one for disaster recovery has hostname-**upgrade_**xx-xx-xx.xml file format. It took out the oracle server installation part since for disaster recovery it is not needed.

Note: the fdconfig xml file for disaster recovery is exactly the same as the one for upgrade and this file should have been created during the latest upgrade or fresh installation. In case the file is not found, please refer to fresh installation section to re-create it.

S	This procedure pe	erforms disaster recovery preparation steps for the IDIH.
і Е #	Check off (√) each step number. If this procedure fa	n step as it is completed. Boxes have been provided for this purpose under each ails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.
1	PMAC GUI:	Open web browser and enter:
	Login	http:// <pmac_mgmt_network_ip></pmac_mgmt_network_ip>
		<section-header></section-header>

Procedure 11: IDIH Disaster Recovery Preparation

Procedure 11: IDIH Disaster Recovery Preparation

2	PMAC GUI:	Navigate to Main Menu -> Software -> Manage Software Images
	Verify necessary	
	IDIH images are	Software
	available	Software Inventory
		Manage Software Images
		Verify the current IDIH TVOE , TPD , Oracle , Application and Mediation images are listed.
		Note: If the necessary software images are not available please follow the instructions from the applicable IDIH release installation and configuration guides – Referenced in Table 9 IDIH Installation Reference Table
3	Oracle Guest: Login	Establish an SSH session to the Oracle guest, login as <i>admusr</i> .
	Oracle Guest:	Execute the following command to perform a database health check:
4	Perform	Execute the following command to perform a database health check.
	Database Health	<pre>\$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i</pre>
	check	
		Output:
		admusr@thunderbolt-ora-
		[admusr@thunderbolt-ora ~]\$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i
		10:10:52: STARTING HEALTHCHECK PROCEDURE 10:10:52: date: 05-12-15, hostname: thunderbolt-ora
		10:10:52: TFD VERSION: 7.0.1.0.0-86.20.0 10:10:52:
		10:10:52: Checking disk free space
		10:10:52: No disk space issues found 10:10:52: Checking syscheck - this can take a while
		10:10:58: No errors in syscheck modules 10:10:58: Checking Alarm Manager alarmStatus
		10:11:00: No alarms found
		10:11:00: Checking Statefiles 10:11:00: Statefiles do not exist
		10:11:00: Checking runlevel 10:11:00: Runlevel is OK (N 4)
		10:11:00: Checking upgrade log
		10:11:00: Analyzing date
		10:11:00: NTP deamon is running 10:11:00: Server is synchronized with ntp server
		10:11:00: Checking NTP status
		10:11:00: Ntp settings is OK
		10:11:00: Checking server entries in host file. 10:11:00: oracle is present in /etc/hosts
		10:11:00: mediation is present in /etc/hosts 10:11:00: appserver is present in /etc/hosts
		10:11:00: Ping server entries in host file.
		10:11:00: Ping server oracle 10:11:00: Ping server mediation
		10:11:00: Ping server appserver 10:11:00: Check gracie Server
		10:11:01: Oracle server and resources online
		10:11:01: AII tests passed: 10:11:01: ENDING HEALTHCHECK PROCEDURE WITH CODE 0 [admusr@thunderbolt-ora ~]\$

S T	This procedure pe application servers	rforms disaster recovery for the IDIH by re-installing the mediation and s.
Р #	Check off (√) each step number.	n step as it is completed. Boxes have been provided for this purpose under each
	If this procedure fa	ails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.
1	PMAC GUI:	Open web browser and enter:
	Login	http:// <pmac_mgmt_network_ip></pmac_mgmt_network_ip>
		Login as <i>pmacadmin</i> user:
		ORACLE
		Oracle System Login
		Log In Enter your username and password to log in
		Username: pmadadmin Password: Channe assword
		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. Copyright © 2010. Oracle and/or its affiliates. All rights reserved.
2	Remove existing	Navigate to Main Menu -> VM Management
	Application Server	💼 😋 Software
	Server	Software Inventory
		📑 VM Management
		Select the application guest,
		Click on the Delete button.
		Edit Delete Clone Guest Regenerate Device Mapping ISO
		Install OS Upgrade Accept Upgrade Reject Upgrade

Procedure 12: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

Procedure 12: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

3	Remove existing Mediation Server	Navigate to Main Menu -> VM Management Software Software Manage Software Images Manage Software Images Management Select the Mediation guest, Click on the Delete button. Edit Delete Clone Guest Regenerate Device Mapping ISO Install OS Upgrade
4	PMAC: Establish SSH session and Login	Establish an SSH session to the PMAC, login as <i>admusr</i> .
5	PMAC: Re- install the Mediation and Application Servers	Execute the following command (Enter your upgrade file) : \$ cd /var/TKLC/smac/guest-dropin \$ sudo fdconfig config -file= <hostname-upgrade_xx-xx- xx>.xml Warning: If you run the fdconfig without "upgrade" in the XML filename, the database will be destroyed and you will lose all of the existing data.</hostname-upgrade_xx-xx-

PMAC GUI: If not already done so, establish a GUI session on the PMAC server. 6 Monitor the Configuration Navigate to Main Menu -> Task Monitoring 🛓 🚞 Status and Manage 📑 Task Monitoring 🤣 Help 🔁 Logout Monitor the IDIH configuration to completion. Alternatively, you can monitor the fdconfig status through the command line after executing the fdconfig command: Example: - 0 × Admusr@bertie:/var/TKLC/smac/guest-dropin admusr@bertie guest-dropin]\$ sudo fdconfig config --file=d-ray_04-21-15.xml Request to start a new configuration Running d-ray 04-21-15.xml configuration Configuration file processing complete Created a deployment database file: deploy_d-ray_20150511T093944_630c.fdcdb Preparing to run the configuration steps PM&C has no in progress tasks RMS is already provisioned, skipping: 1 RMS is already provisioned, skipping: 10.250.36.27 Server discovery complete: [RMS ip: 10.250.36.27] Hostname for [RMS ip: 10.250.36.27] already set to d-ray skipping

Procedure 12: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

Appendix A. DSR Database Backup

Proce	ocedure 13: Restoring an Archive that does not Contain a Current User			
S T F	The intent of this p NOAM or SOAM s	procedure is to back up the provision and configuration information from an server after the disaster recovery is complete		
– P #	Check off (√) each step number.	n step as it is completed. Boxes have been provided for this purpose under each		
	If this procedure f	fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.		
1	NOAM/SOAM VIP: Login	Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server.		
		Open the web browser and enter a URL of:		
		http:// <primary_noam soam_vip_ip_address=""></primary_noam>		
		Login as the guiadmin user:		
		ORACLE		
		Oracle System Login Fri Mar 20 12:29:52 2015 EDT		
1				
		Log In		
		Enter your username and password to log in		
		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 sava are registered trademarks of Oracle Corporation and/or its anniates. Other names may be trademarks of their respective owners.		

Procedure 13: Restoring an Archive that does not Contain a Current User

2	NOAM/SOAM	Navigate to Ma	in Menu -> Status & Manage -> Database
2	VIP: Backup		
	Configuration	🚔 🖴 Status	& Manage
	Data for the		a Hanage
		- 🔊 Netv	vork Elements
	System		
		🚽 🔤 💓 Serv	er
		📄 🔤 💽 Data	base
		🚽 🔤 🌇 Proc	esses
		Select the Activ	e NOAM Server and Click on Backup button
		Disable Provisioning	Report Inhibit Replication Backup Compare Restore Man Audit Suspend Auto Audit
		Make sure that	the checkboxes next to "Configuration" is checked.
			5
		Database Backu	n
		Field	Valua
		Server: Jetta-NO-1	value
		Coloct data far bookun	Provisioning
		Select data for backup	Configuration
			Oqzip
		Compression	© bzip2
			Onone *
		Archive Name	Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150428_09311 *
		_	
		Comment	
			Ok Cancel
		Enter a filenam	e for the backup and press OK
			· ·
1		1	

Procedure 13: Restoring an Archive that does not Contain a Current User



Procedure 13: Restoring an Archive that does not Contain a Current User

4	NOAM/SOAM	From the previous step, choose the backup file.	
	VIP: Download the file to a local machine.	Select the Download button	
		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.	
		Select OK to confirm the download.	
		You have chosen to onen:	
		II1.Configuration.NETWORK_OAMP.20150418_021510.AUTO.tar	
		which is: tar Archive (13.5 MB)	
		What should Firefox do with this file?	
		Open with 7-Zip File Manager (default) Save File Do this <u>a</u> utomatically for files like this from now on.	
		OK Cancel	
5	Upload the	Transfer the backed up image saved in the previous step to a secure location	
	to Secure	where the Server backup lies are retched in case of system disaster recovery.	
	Location		
6	Backup Active	Repeat Steps 2 through 5 to back up the Active SOAM	

Appendix B. Recovering/Replacing Failed 3rd Party Components (Switches, OAs)

The following procedures provide steps to recover 3rd party devices (switches, OAs). Follow the appropriate procedure as needed for your disaster recovery.

Procedure 14: Recovering a Failed Aggregation Switch (Cisco 4948E/4948E-F)

S T	The intent of this procedure is to recover a failed Aggregation (4948E / 4948E-F) Switch.					
E P #	Prerequisites for t	this procedure are: of the networking xml configuration files of HP Misc Firmware DVD or ISO ess and hostname of the failed switch pount position of the failed switch				
	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.					
	If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.					
1	Recover failed Aggregation	Login to the PMAC via SSH as <i>root(5.0)</i> or <i>admusr(6.0+)</i>				
	Switches: Cisco 4948E/4948E-F	Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell:				
		<pre>sudo ssh-keygen -R <4948_switch_ip></pre>				
		Refer to procedure <i>"Replace a failed 4948/4948E/4948E-F switch (c-Class system)</i> (netConfig)" to replace a failed Aggregation switch Refer to Table 7 : Platform Configuration Reference Table for the applicable platform configuration reference.				
		Note: You will need a copy of the HP Misc Firmware DVD or ISO (or firmware file obtained from the appropriate hardware vendor) and of the original networking xml files custom for this installation. These will either be stored on the PMAC in a designation location, or can be obtained from the NAPD.				

Procedure 15: Recovering a Failed Enclosure Switch (Cisco 3020)

S T E P #	 The intent of this procedure is to recover a failed Enclosure (3020) Switch. Prerequisites for this procedure are: A copy of the networking xml configuration files A copy of HP Misc Firmware DVD or ISO IP address and hostname of the failed switch Interconnect Bay position of the enclosure switch Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance. 		
1	Recover failed Enclosure Switch: Cisco 3020	Login to the PMAC via SSH as <i>root(5.0)</i> or <i>admusr(6.0+)</i> Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell: <u>sudo ssh-keygen -R <enclosure_switch_ip></enclosure_switch_ip></u> Refer to procedure <i>"Reconfigure a failed 3020 switch (netConfig)"</i> to replace the failed enclosure switch Refer to Table 7 : Platform Configuration Reference Table for the applicable platform configuration reference. Note: You will need a copy of the HP Misc Firmware DVD or ISO and of the original networking xml files custom for this installation. These will either be stored on the PMAC in a designation location, or can be obtained from the NAPD.	

Procedure 16: Recovering a Failed Enclosure Switch (HP 6120XG)				
S T E P #	 The intent of this procedure is to recover a failed Enclosure (6120XG) Switch. Prerequisites for this procedure are: A copy of the networking xml configuration files IP address and hostname of the failed switch Interconnect Bay position of the enclosure switch Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance. 			
1	Recover failed Enclosure Switch: HP 6120XG	Login to the PMAC via SSH as <i>root(5.0)</i> or <i>admusr(6.0+)</i> Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell: <u>sudo ssh-keygen -R <enclosure_switch_ip></enclosure_switch_ip></u> Refer to procedure " <i>Reconfigure a failed HP 6120XG switch (netConfig)</i> " to replace the failed enclosure switch Refer to Table 7 : Platform Configuration Reference Table for the applicable platform configuration reference. Note: You will need a copy of the HP Misc Firmware DVD or ISO and of the original networking xml files custom for this installation. These will either be stored on the PMAC in a designation location, or can be obtained from the NAPD.		
S T E P #	 The intent of this procedure is to recover a failed Enclosure (6125XLG/6125G) Switch. Prerequisites for this procedure are: A copy of the networking xml configuration files Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance. 			
-----------------------	--	--		
	Recover failed Enclosure Switch: HP 6125XLG/6125 G	Login to the PMAC via SSH as <i>root(5.0)</i> or <i>admusr(6.0+)</i> Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell: <u>sudo ssh-keygen -R <enclosure_switch_ip></enclosure_switch_ip></u> Refer to procedure <i>"Reconfigure a failed HP 6125XG, 6125XLG switch (netConfig)"</i> to replace the failed enclosure switch Refer to Table 7: Platform Configuration Reference Table for the applicable platform configuration reference. Note: You will need a copy of the HP Misc Firmware DVD or ISO and of the original networking xml files custom for this installation. These will either be stored on the PMAC in a designation location, or can be obtained from the NAPD.		

Procedure 17: Recovering a Failed Enclosure Switch (HP 6125XLG, HP 6125G)

Procedure 18: Recovering a Failed Enclosure OA

S T P #	The intent of this p Check off ($$) each step number. If this procedure fa	procedure is to recover a failed Enclosure Onboard Administrator. In step as it is completed. Boxes have been provided for this purpose under each ails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.
1	Recover Failed Enclosure OA	Refer to procedure <i>"Replacing Onboard Administrator in a system with redundant OA"</i> to replace a failed Enclosure OA Refer to Table 7 : Platform Configuration Reference Table for the applicable platform configuration reference.

Appendix C. Switching DR NOAM Site to Primary

Upon the loss of a Primary DSR NOAM Site, the DR NOAM Site should become primary. The following steps are used to enable such switchover.

Preconditions:

- User cannot access the primary DSR
- User still can access the DR DSR
- Provisioning clients are disconnected from the primary DSR
- Provisioning has stopped

	•	•	
S T	The intent of this procedure is to switch a DR site to Primary.		
E P #	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.		
π	If this procedure fa	ails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.	
1	DR-NOAM VIP: Login	Establish a GUI session on the DR-NOAM server by using the VIP IP address of the DR-NOAM.	
		Open the web browser and enter a URL of:	
		http:// <primary_dr_noam_vip_ip_address></primary_dr_noam_vip_ip_address>	
		Login as the <i>guiadmin</i> user:	
		CRACEC	
		Oracle System Login Fri Mar 20 12:29:52 2015 EDT	
		Log In Enter your username and password to log in	
		Username: guiadmin	
		Password: ••••••	
		Log In	
		Welcome to the Oracle System Login.	
		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.	
		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.	

2	DR-NOAM VIP:	Navigate to Main Menu -> Status & Manage -> Server
	Disable DSR Application on DR-NOAM Servers	 Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files
		Select the row that has the Active DR-NOAM server.
		Select the Stop button.
		Stop Restart Reboot NTP Sync Report
		Note: At this time, HA switch over causes an automatic logout.
3	DR-NOAM VIP:	Establish a GUI session on the DR-NOAM server by using the VIP IP address
	Login	
		Open the web browser and enter a URL of:
		http:// <primary_dr_noam_vip_ip_address></primary_dr_noam_vip_ip_address>
		Login as the <i>guiadmin</i> 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
		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.

4	DR-NOAM VIP:	Repeat step 2 to disable the DSR application on the now active DR NOAM.		
	Repeat	Note: The DSR application should now be stopped on all DR-NOAMs.		
5	DR-NOAM VIP: Verify DSR application is stopped	Verify that " PROC " column on both DR DSR servers show " Man " indicating that application is manually stopped		
6	Primary DR- NOAM: Establish an SSH session	Login via SSH to the physical IP of the chosen primary DR-NOAM server as root(5.0) or admusr(6.0+) user.		
7	Primary DR- NOAM: Change Role to Primary	Execute the command <pre>\$ sudo top.setPrimary</pre>		
		Note: This step makes the DR DSR take over as the Primary. Execute the following command to verify the role was changed to primary: \$ sudo top.myrole		
		System generates several replication and collection alarms as replication/collection links to/from former Primary NOAM servers becomes inactive.		
8	Primary DR- NOAM: Verify Replication	Inactive. Navigate to Main Menu -> Status & Manage Status & Manage Network Elements Server HA Database KPIs Processes It may take several minutes for replication; afterward the "DB" and "Reporting Status" columns should show "Normal". DB Reporting Status Norm Norm Norm Norm Norm Norm		

9 □	9 New Primary NOAM: Re- enable the Navigate to Main Menu -> Status & Manage -> Server □ Image Image	
	application.	 Network Elements Server HA Database KPIs Processes
		Select the row that has the active New-Primary NOAM server.
		Click the Restart button and then click the OK button.
		Stop Restart Reboot NTP Sync Report
		Verify that " PROC " column now shows "Norm".
		Proc
		Norm
		Norm
		Provisioning can now resume to the VIP of the new-Primary DSR
10	New Primary NOAM:	Lower the durability admin status to (NOAM pair) to exclude former-Primary NOAM servers from the provisioning database durability.
	Decrease the Durability Admin	A value greater than 2 must be adjusted downward.
	Status	Navigate to Main Menu -> Administration -> General Options
		🗉 🚊 Main Menu
		 Administration General Options Access Control
		Set "cm.idb.durableAdminState" to 2 (NOAM pair)
		cm.idb.durableAdminState 2 *
		Click the OK button

11	New Primary	Repeat steps 8-9 for standby of the new-Primary NOAM server.
11	NOAM: Repeat	
	for standby of	
	new-primary	
	NOAM Server	

Appendix D. Returning a Recovered Site to Primary

S T	The intent of this	The intent of this procedure is to return a recovered site to primary.		
- E P #	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.			
	If this procedure f	ails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.		
1	Primary NOAM VIP: Login	Establish a GUI session on the primary NOAM server by using the VIP IP address of the primary NOAM.		
		Open the web browser and enter a URL of:		
		http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>		
		Login as the <i>guiadmin</i> user:		
		ORACLE		
		Oracle System Login		
		Fn Mar 20 12:29:52 2015 ED1		
		Log In		
		Enter your username and password to log in		
		Username: quiadmin		
		Username: guiadmin Password: ••••••		
		Username: guiadmin Password: •••••• Change password		
		Username: guiadmin Password: •••••• Change password Log In		
		Username: guiadmin Password: •••••• Change password Log In Welcome to the Oracle System Login.		
		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.		

2	Primary NOAM	Navigate to Main Menu -> Status & Manage -> Server
	Disable DSR Application on DR-NOAM Servers	Status & Manage Network Elements Server HA Database KPIs Processes Files Select the row that has the Active DR-NOAM server. Select the Stop button.
		Stop Restart Reboot NTP Sync Report Note: At this time, HA switch over causes an automatic logout.
3	Primary NOAM VIP: Login	Establish a GUI session on the primary NOAM server by using the VIP IP address of the NOAM. Open the web browser and enter a URL of:
		http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>
		Login as the <i>guiadmin</i> user: CRACLE® Oracle System Login Fri Mar 20 12:29:52 2015 EDT
		Log In Enter your username and password to log in
		Username: guiadmin
		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.

4	Primary NOAM VIP: Repeat	Repeat step 2 to d	disable the DSR application on the now active $\overline{\text{DR}}$ NOAM.	
	•	Note: The DSR ap	plication should now be stopped on all DR-NOAMs.	
5	Primary NOAM VIP: Verify DSR application is stopped.	Verify that " PROC " column on both DR DSR servers show " Man " indicating that application is manually stopped		
6	Primary NOAM VIP: Establish an SSH session	Login via SSH to the physical IP of the chosen primary DR-NOAM server as <i>root(5.0)</i> or <i>admusr(6.0+)</i> user.		
7	Primary NOAM VIP: Change Role to Secondary	Execute the command <pre>\$ sudo top.setSecondary</pre>		
		Note: This step makes the primary NOAM to revert to DR-NOAM		
		Execute the following command to verify the role was changed to secondary:		
		\$ sudo top.my	yrole	
0	New DR-NOAM	Navigate to Main Menu -> Status & Manage -> Server		
0	VIP: Verify			
	Replication	🖻 📥 Status & I	Manage	
		Network Elements		
		Server		
		📑 HA		
		- 🔄 Database		
		💽 KPIs 💽 Processes		
		It may take several	minutes for replication: afterward the "DB" and "Poporting	
		Status" columns s	should show "Normal".	
		DB	Reporting Status	
		Norm	Norm	
		Norm	Norm	
		Norm	Norm	

9	New DR-NOAM	Navigate to Main Menu -> Status & Manage -> Server
	the application.	 Status & Manage Network Elements Server HA Database KPIs Processes
		Select the row that has the formerly Primary NOAM server.
		Click the Restart button and then click the OK button.
		Stop Restart Reboot NTP Sync Report
		Verify that "PROC" column now shows "Norm".
		Proc
		Norm
		Norm
	To Po Primory	Login via SSH to the physical ID of the chosen primery DD NOAM converses
10	NOAM VIP: Establish an SSH session	root(5.0) or admusr(6.0+) user.
11	To-Be-Primary	Execute the following command:
	VIP: Set To-be- Primary DSR NOAM to Primary	<pre>\$ sudo top.setPrimary</pre>
		Note: This step makes the DSR take over as the Primary.
		Execute the command to verify the server role was changed to Primary:
		\$ sudo top.myrole
		System generates several replication and collection alarms as replication/collection links to/from former Primary NOAM servers becomes inactive.

12	New Primary	Navigate to Main Menu -> Status & Manage -> Server		
	enable the	📋 🚔 Status & Manage		
	application.	🔤 💽 Network Elements		
		s 🚽 💓 Server		
		HA IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		
		Database		
		Select the row that has the active New-Primary NOAM server.		
		Click the Restart button and then click the OK button.		
		Stop Restart Reboot NTP Sync Report		
		Verify that " PROC " column now shows "Norm".		
		Proc		
		Norm		
		Norm		
		Norm		
13	New Primary	Repeat Step 12 on the second recovered NOAM.		
	Repeat on	Provisioning can now resume to the VIP of the new-Primary DSR.		
	Second Recovered			
	NOAM	Monitor Main Menu -> Status & Manage -> Server screen at new-Primary		
14	DSR NOAM	DSR.		
	VIP: Verify Replication	It may take several minutes for replication; afterward the "DB" and "Reporting		
		Status" columns should show "Normal"		
		Note: the inetmerge process might have to be restarted if replication is taking		
		excessive time. To restart it, ssh to the active site NOAM and run the following command to restart the replication process:		
		For DSR 5.0:		
		<pre>\$ pm.kill inetmerge</pre>		
		For DSR 6.0/7.0/7.1:		
		<pre>\$ sudo pm.kill inetmerge</pre>		

16	New Primary NOAM VIP: Set	If you reduced the durability status in procedure 19, raise durability admin status to its former value (NOAM + DRNOAM)						
	status to include DR-NOAM	Navigate to Main Menu -> Administration -> General Options						
	(Optional)	🖃 🚊 Main Menu						
		🛓 🔄 Administration						
		General Options						
		🚊 🧰 Access Control						
		Set "durableAdminState" to 3(NO DRNOAM)						
		cm.idb.durableAdminState 3 *						
		Click the OK button						
		Now new DRNOAM DSR servers are part of provisioning database durability.						

Appendix E. Inhibit A and B Level Replication on C-Level Servers

Procedure 21: Inhibit A and B Level Replication on C-Level Servers

S T E	The intent of this procedure is to inhibit A and B level replication on all C Level servers of this site Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each										
– P #	step number.	ber.									
	If this procedure fa	cedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.									
1	Active NOAM: Login	Login to the Active NOAM server via SSH as <i>root(5.0) or admusr(6.0+)</i> user.									
2	Active NOAM: Inhibit	Execute the following command:									
	replication on all C level Servers	<pre>\$ for i in \$(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<soam name="" of="" site_ne="" the<br="">site>'"); do iset -finhibitRepPlans='A B' NodeInfo where "nodeName='\$i'"; done Note: SOAM Site_NE name of the site can be found out by logging into the Active NOAM GUI and going to Configuration->Server Groups screen. Please see the snapshot below for more details. E.g. if ServerSO1 belong to the site which is being recovered then siteId will be SO_HPC03.</soam></pre>									
		Filter +									
			Server Group Name	Level	Parent	Function	Servers				
			NPSC	C	9096	DSR (multi- active cluster)	NE SO_HPC03 SO_HPC03	Server ServerNP1 ServerNP2	HA Role Pref	VPs	
			NCSG		NOVE	OSR (active(standb pair)	NO_HPC03 NO_HPC03	Server ServerNO1 ServerNO2	HA Role Pref	VIPs 10.240.10.166 10.240.10.166	
			505G	B	NOSG	DSR (achielstand) pari)	NE SOUTIERS SOUTIERS	ServerS01 ServerS02	HA Role Pref	VIPs 10.240.10,186 10.240.10,186	

Procedure 21: Inhibit A and B Level Replication on C-Level Servers

3	Active NOAM: Verify Replication has been Inhibited.	After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled. Verification of replication inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site e.g. Site SO_HPC03 shall be set as 'A B': Perform the following command:						
		Expected ou nodeld excludeTables A1386.099 B1754.109 C2254.131 C2254.233	utput: nodeName NO1 SO1 MP2 MP1	hostNam NO1 SO1 MP2 MP1	ne nodeCapability Active Active Active Active Active	inhibitRepPlans A B A B	siteId NO_HPC03 SO_HPC03 SO_HPC03 SO_HPC03	

Appendix F. Un-Inhibit A and B Level Replication on C-Level Servers

11000										
S T	The intent of this p site	procedure is to	Un-ir	nhibit	A and B	level r	eplicatio	on on al	II C Level se	rvers of this
Р #	Check off (√) each step number.	step as it is completed. Boxes have been provided for this purpose under each								
	If this procedure fa	If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.								
1	Active NOAM: Login to the Active NOAM server via SSH as root(5.0) or admusr(6.0+) user. Login Login									
2	Active NOAM:	Execute the f	follow	ing co	ommand					
	Un-Inhibit replication on all C level Servers	<pre>\$ for i i "nodeId I iset -fir done Note: SOAN Active NOAN Please see th site which is</pre>	.n \$.ike .hibi 1 GUI ne sn being	(iqt 'C*' itRep NE n and (apshc recov	-p -z and s >Plans=	-h -: iiteIo -'' No he site Config for mo en site	fhostN d=' <so odeInf can be guration re detai Id will b</so 	ame No AM_Sit o when found o n->Serv ls. E.g. e SO_H	odeInfo wh te_NE_name re "nodeNa out by loggin /er Groups s if ServerSO ⁷ IPC03.	nere e>>'"); do ame='\$i'"; ig into the screen. 1 belong to the
		Main Menu: Configu	ration -:	> Server	Groups					6
		Fiter •							Non Aug 25	.02:26:27 291
		Server Group N	amé Level	Parent	Function	Servers				
		MPSG	С	909G	DSR (multi- active cluster)	NE SOJHPOI3 SOJHPOI3	Server ServerNP1 ServerNP2	HA Role Pref	VPs	
		NOSG	٨	NONE	OSR (active(standb pair)	NO_HPC03 NO_HPC03	ServerN01 ServerN02	HA Role Pref	VIPs 10.240 10.166 10.240 10.166	
		SOSG	В	NOSG	DSR (achielstandb pair)	NE SOUTIESS SOJHPOD	Server ServerS01 SenerS02	HA Role Pref	VIPs 10.240 10.105 10.240 10.185	
	1	1								

Procedure 22: Un-Inhibit A and B Level Replication on C-Level Servers

Procedure 22: Un-Inhibit A and B Level Replication on C-Level Servers

3	Active NOAM: Verify Replication has	After executing above steps to un-inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.							
	been Inhibited.	Verification of replication un-inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site e.g. Site SO_HPC03 shall be set as 'A B': Perform the following command:							
		\$ sudo iqt NodeInfo Expected output: nodeld nodeName A1386.099 NO1 NO1 Active S01 SO1 ACtive SO_HPC03 C2254.131 MP2 MP1 Active SO_HPC03 C2254.233 MP1							

Appendix G. Workarounds for Issues not fixed in this Release

Issue	Associated PR	Workaround
Inetmerge alarm after force restore Incorrect NodeID	222826	Correct the RecognizedAuthority table on the restored NOAM after the disaster recovery. Update the clustered field of the recognizedAuthority table to have the clustered shown by top.myrole command: \$ top.myrole myNodeId=A3603.215 myMasterCapable=true Then update the clusterId field in RecognizedAuthority table to have the same clustered from the above command: \$ ivi RecognizedAuthority e.g. iload -ha -xU -frecNum -fclusterId -ftimestamp RecognizedAuthority \ <<'!!!!
Inetsync alarms after performing disaster recovery	222828	Restart the Inetsync service on all affected servers using the following commands: \$ pm.set off inetsync \$ pm.set on inetsync
Active NO /etc/hosts file does not contain server aliases after force restore done. Note: This is no longer needed in DSR 7.1 Active NO cannot communicate with other Servers	222829,234357	Release 5.0: From the recovered NOAM server command line, execute: \$ AppWorks AppWorks_AppWorks updateServerAliases <no host<br="">Name></no>

SOAM VIP reports no servers at the Status	Bug 20045979	Perform the following command to see
& Manage Server screen.		the 'db' directory permission:
		\$ ls -ltr
		drwx523 root root 20480 Nov 11 22:44 db < Not Correct
		Perform the following command to change the directory permissions:
		\$ sudo chmod 777 db
		Verify the directory permissions are correct:
		\$ ls -ltr drwxrwxrwx 523 root root 20480 Nov 11 22:44 db < Correct

Appendix H. My Oracle Support (MOS)

MOS (<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 MOS 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, there are multiple layers of menus selections. Make the selections in the sequence shown below on the Support telephone menu:

1. For the first set of menu options, select 2, "New Service Request". You will hear another set of menu options.

2. In this set of menu options, select 3, "Hardware, Networking and Solaris Operating System Support". A third set of menu options begins.

3. In the third set of options, select 2, "Non-technical issue". Then you will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.