

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®

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.



CAUTION:

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

Table of Contents	3
List of Procedures	4
List of Tables	5
List of Figures	5
1.0 Introduction	5
1.1 Purpose and Scope	5
1.2 References	6
1.3 Acronyms	7
1.4 Terminology	8
1.5 Optional Features	9
2.0 General Description	10
2.1 Complete Server Outage (All Servers)	11
2.2 Partial server outage with one NOAM server intact and both SOAMs failed	11
2.3 Partial server outage with both NOAM servers failed and one SOAM server intact	11
2.4 Partial server outage with NOAM and one SOAM server intact	11
2.5 Partial Service outage with corrupt database	11
3.0 Procedure Overview	12
3.1 Required Materials	12
3.1.1 Release Document Matrix	13
3.2 Disaster Recovery Strategy	14
4.0 Procedure Preparation	16
5.0 Disaster Recovery Procedure	17
5.1 Recovering and Restoring System Configuration	19
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)	51
5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact)	75
5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)	95
5.1.5 Recovery Scenario 5 (Both NOAM servers failed with DR-NOAM available)	112
5.1.6 Recovery Scenario 6 (Database Recovery)	118
6.0 Resolving User Credential Issues after Database Restore	124
6.1 Restoring a Deleted User	124
6.2 Keeping a Restored user	125

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	113
Procedure 6: Recovery Scenario 6 (Case 1)	118
Procedure 7: Recovery Scenario 6 (Case 2)	121
Procedure 8: Keep Restored User	125
Procedure 9: Remove the Restored User	127
Procedure 10: Restoring an Archive that does not Contain a Current User	130
Procedure 11: IDIH Disaster Recovery Preparation	133
Procedure 12: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)	135
Procedure 13: Restoring an Archive that does not Contain a Current User	138
Procedure 14: Recovering a Failed Aggregation Switch (Cisco 4948E/4948E-F)	142
Procedure 15: Recovering a Failed Enclosure Switch (Cisco 3020)	143
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.....	151

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

Figure 1. Determining Recovery Scenario	15
---	----

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	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 (RBAR)	DSR RBAR Feature Activation Procedure, E58665
Map-Diameter Interworking (MAP-IWF) – DSR 6.0+	DSR MAP-Diameter IWF Feature Activation Procedure, E58666
Policy and Charging Application (PCA)	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • All NOAM servers failed • All SOAM servers failed
Recovery of one or more servers with at least one NOAM server intact	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • All NOAM servers failed • 1 or more SOAM servers intact
Recovery of one or more server with at least one NOAM and one SOAM server intact.	<ul style="list-style-type: none"> • 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
2. 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.

SUDO

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

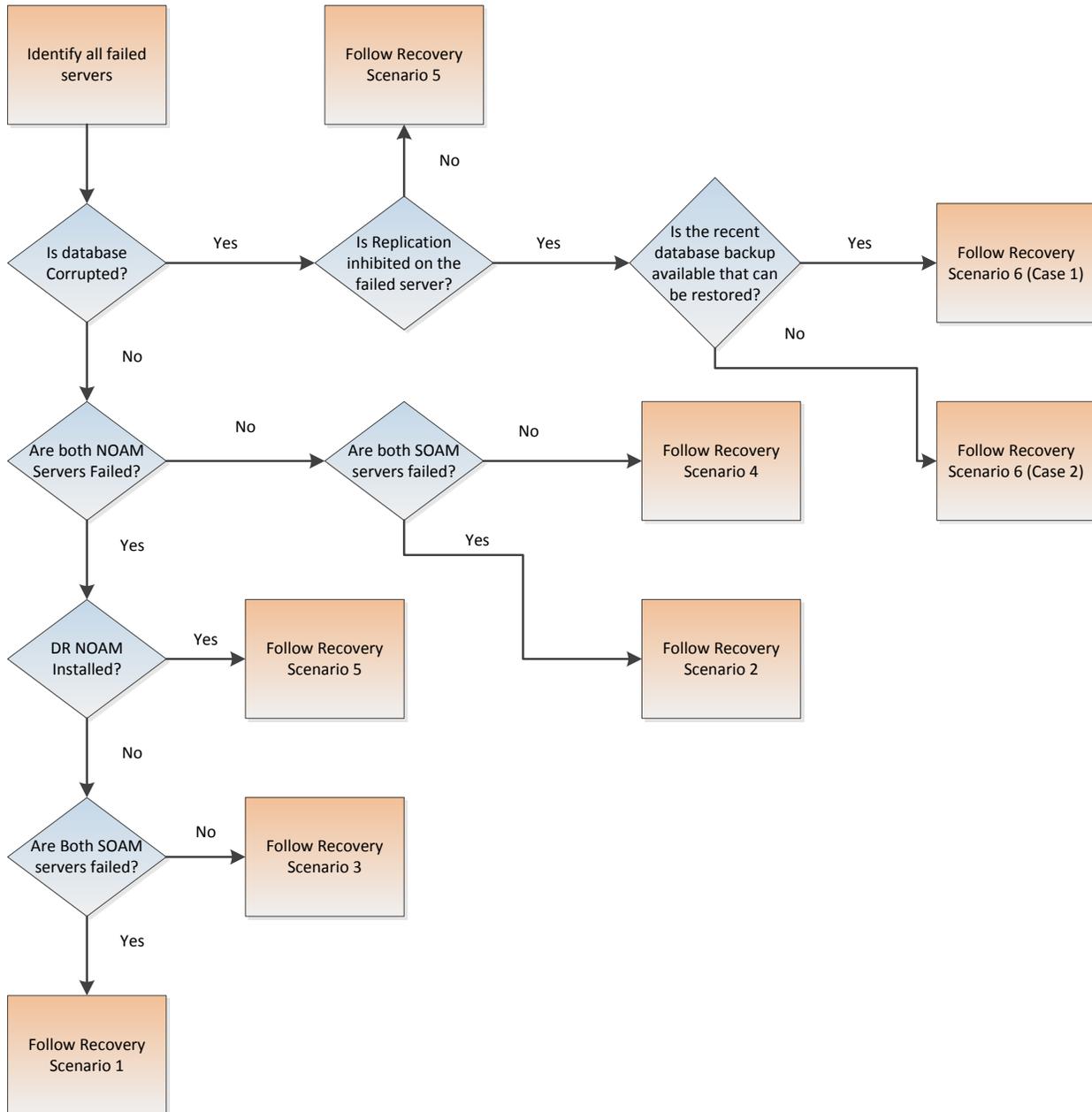
IDIH Release	Reference
IDIH 6.0	[8]
IDIH 7.0	[8]
IDIH 7.1	[17]

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).

Figure 1. Determining Recovery Scenario



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.

Table 10. Recovery Scenarios

Recovery Scenario	Failure Condition	Section
1	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> At least 1 NOAM server is intact and available. All SOAM servers failed. MP servers may or may not be failed. 	Section 0
3	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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)

5	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 Matrix to 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

Procedure 1: Recovery Scenario 1

S T E P #	<p>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</p> <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Workarounds	Refer to Appendix G . Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
2 <input type="checkbox"/>	Gather Required Materials	Gather the documents and required materials listed in Section 3.1 Required Materials
3 <input type="checkbox"/>	RMS NOAM Failure	<p>If the failed server is a rack mount server based NOAM, execute this step; otherwise skip to the next step.</p> <ol style="list-style-type: none"> 1. HW vendor to replace the failed equipment 2. Execute the <i>"iLO Configuration Procedure"</i> 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. 5. 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. 6. If the failed NOAM is NOT co-hosted with the PMAC on the first rack mount server, execute <i>procedure "Configure TVOE on Additional RMS Servers(s)"</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.

Procedure 1: Recovery Scenario 1

<p>4 <input type="checkbox"/></p>	<p>HP-Class Blade Failure</p>	<p>If the failed server is an HP C-Class Blade, execute this step; otherwise skip to the next step.</p> <ol style="list-style-type: none"> 1. HW vendor to replace the failed equipment 2. Execute procedure “<i>Confirm/Update blade Server BIOS Settings</i>” – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 3. Execute procedure “<i>Configure Blade Server iLO Password for Administrator Account</i>” – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 4. Perform any needed firmware upgrades – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 5. 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.
<p>5 <input type="checkbox"/></p>	<p>Configure TVOE on Server Blades</p>	<p>For NOAMs on TVOE server Blades and SOAMs, execute procedure “<i>Configure TVOE on Server Blades</i>” - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.</p>
<p>6 <input type="checkbox"/></p>	<p>Create VMs</p>	<p>For NOAMs, execute procedure “<i>Create NOAM Guest VMs</i>” - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.</p> <p>For SOAMs, execute procedure “<i>Create SOAM Guest VMs</i>” - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.</p>
<p>7 <input type="checkbox"/></p>	<p>IPM Failed Guest/Servers</p>	<p>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.</p>
<p>8 <input type="checkbox"/></p>	<p>Install DSR application on Failed Guests/Servers</p>	<p>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.</p>
<p>9 <input type="checkbox"/></p>	<p>Repeat for Remaining Failed Servers</p>	<p>If necessary, repeat steps 1-7 for all remaining failed servers.</p>
<p>10 <input type="checkbox"/></p>	<p>Install NetBackup Client (Optional)</p>	<p>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.</p>

Procedure 1: Recovery Scenario 1

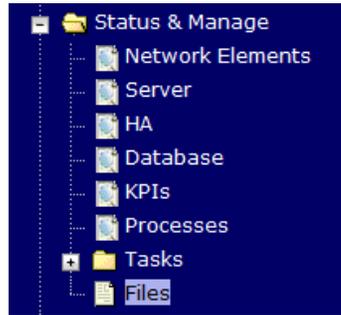
<p>11 <input type="checkbox"/></p>	<p>Obtain Latest Database Backup and Network Configuration Data.</p>	<p>Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources.</p> <p>From required materials list in Section 3.1 Required Materials; use site survey documents and Network Element report (if available), to determine network configuration data.</p>
<p>12 <input type="checkbox"/></p>	<p>Execute DSR Installation Procedure for the First NOAM</p>	<p>Verify the networking data for Network Elements</p> <p>Note: Use the backup copy of network configuration data and site surveys (Step 2)</p> <p>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 and configuration reference.</p> <p>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</p>
<p>13 <input type="checkbox"/></p>	<p>NOAM GUI: Login</p>	<p>Login to the NOAM GUI as the <i>guiadmin</i> user:</p> 

Procedure 1: Recovery Scenario 1

14
□

NOAM GUI:
Upload the
Backed up
Database File

Browse to **Main Menu->Status & Manage->Files**



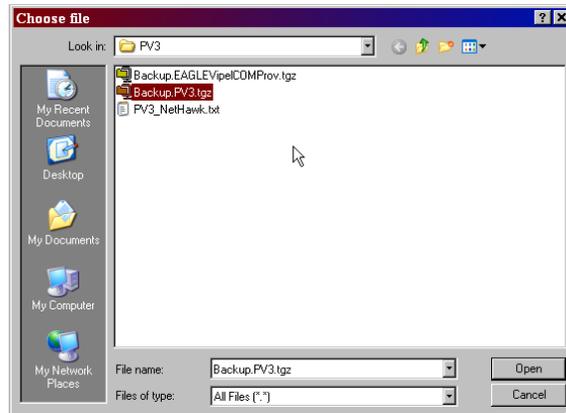
Select the Active NOAM server. The following screen will appear:

File Name	Size	Type	Timestamp
Backup.dsr.Cpa1-NO.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 *“NO Provisioning and Configuration:”* file backed up after initial installation and provisioning.

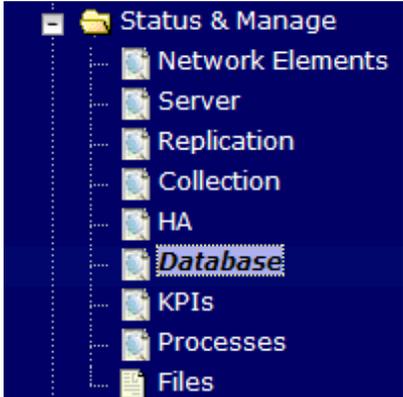


Click on **Browse** and locate the backup file and click on Open as shown below.



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.

Procedure 1: Recovery Scenario 1

15 <input type="checkbox"/>	NOAM GUI: Disable Provisioning	<p>Click on Main Menu->Status & Manage->Database</p>  <p>Disable Provisioning by clicking on Disable Provisioning button at the bottom of the screen as shown below.</p>  <p>A confirmation window will appear, press OK to disable Provisioning.</p>  <p>The message <i>"Warning Code 002"</i> will appear.</p>
--------------------------------	---	--

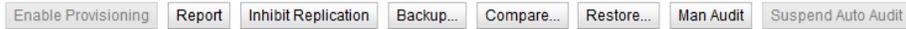
Procedure 1: Recovery Scenario 1

16

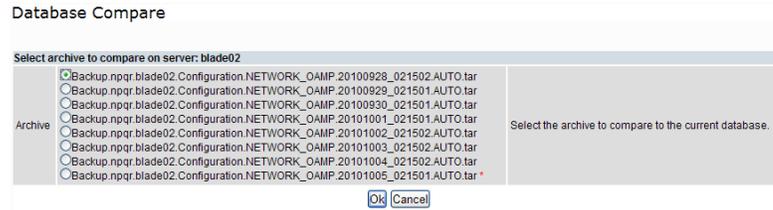


NOAM GUI:
Verify the Archive Contents and Database Compatibility

Select the **Active NOAM** server and click on the **Compare**.

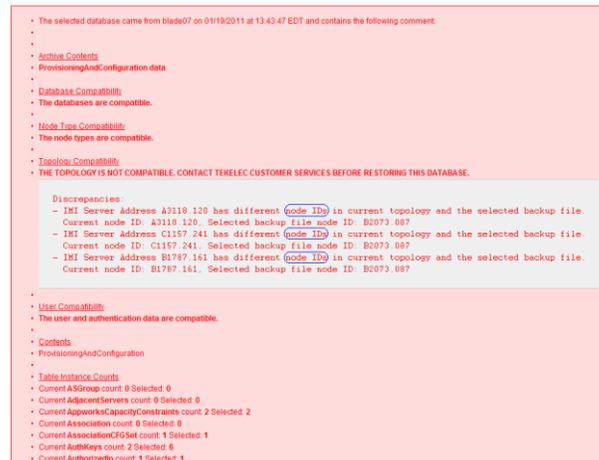


The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 13** of this procedure.



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.



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.

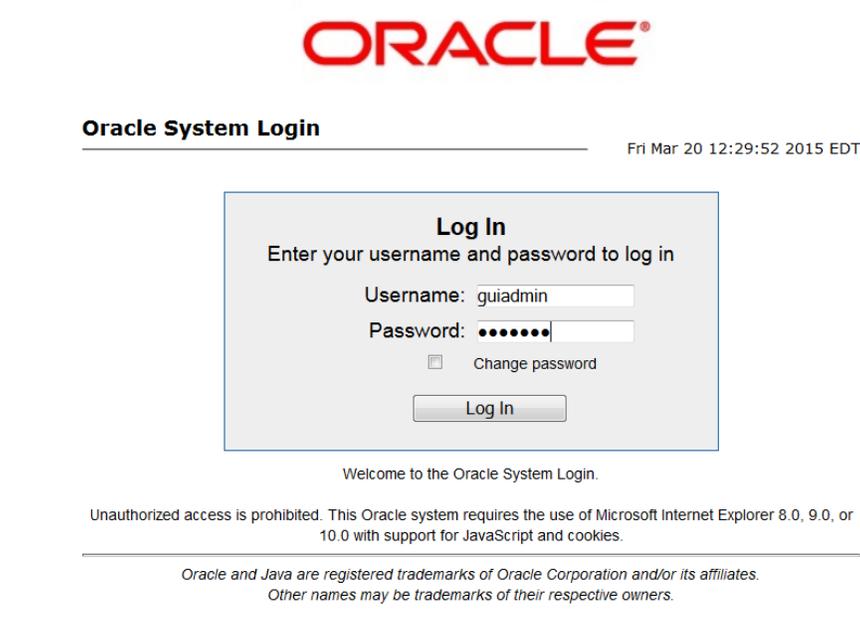
Note: We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility.

If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.

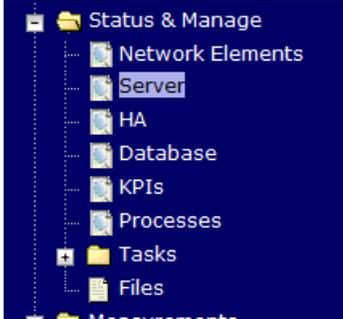
Procedure 1: Recovery Scenario 1

<p>17</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Click on Main Menu->Status & Manage->Database</p> <p>Restore the Database</p> <p>Select the Active NOAM server, and click on Restore as shown below.</p> <p>The following screen will be displayed. Select the proper back up provisioning and configuration file.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>Database Restore</p> <p>Select archive to Restore on server: blade02</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; padding: 2px;">Archive</td> <td style="padding: 2px;"> <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20100928_021502.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20100929_021501.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20100930_021501.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101001_021501.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101002_021502.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101003_021502.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101004_021502.AUTO.tar <input checked="" type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101005_021501.AUTO.tar * </td> <td style="width: 70%; padding: 2px; vertical-align: top;">Select the archive to restore on blade02.</td> </tr> </table> <p style="text-align: right;"><input type="button" value="Ok"/> <input type="button" value="Cancel"/></p> </div> <p>Click OK Button. The following confirmation screen will be displayed.</p> <p>If you get an error that the NodeIDs do not match. That is expected. If no other errors beside the NodeIDs are displayed, select the Force checkbox as shown above and Click OK to proceed with the DB restore.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>Database Restore Confirm</p> <p>Incompatible database selected</p> <div style="background-color: #ffe0e0; padding: 5px; border: 1px solid #ccc;"> <p>Discrepancies:</p> <ul style="list-style-type: none"> - IMI Server Address A3118.120 has different node IDs in current topology and the selected backup 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 backup 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 backup file. Current node ID: B1787.161, Selected backup file node ID: B2073.087 </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>Confirm archive "3bladeHPQR.blade07.Configuration.NETWORK_OAMP.20110119_184253.MAN.tar" to Restore on server: blade07</p> <p>Force Restore? <input checked="" type="checkbox"/> Force <input type="checkbox"/> Force restore on blade07, despite compare errors.</p> <p style="text-align: right;"><input type="button" value="Ok"/> <input type="button" value="Cancel"/></p> </div> </div> <p>Note: After the restore has started, the user will be logged out of XMI NO GUI since the restored Topology is old data.</p>	Archive	<input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20100928_021502.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20100929_021501.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20100930_021501.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101001_021501.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101002_021502.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101003_021502.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101004_021502.AUTO.tar <input checked="" type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101005_021501.AUTO.tar *	Select the archive to restore on blade02.
Archive	<input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20100928_021502.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20100929_021501.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20100930_021501.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101001_021501.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101002_021502.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101003_021502.AUTO.tar <input type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101004_021502.AUTO.tar <input checked="" type="radio"/> Backup.npr:blade02.Configuration.NETWORK_OAMP.20101005_021501.AUTO.tar *	Select the archive to restore on blade02.		

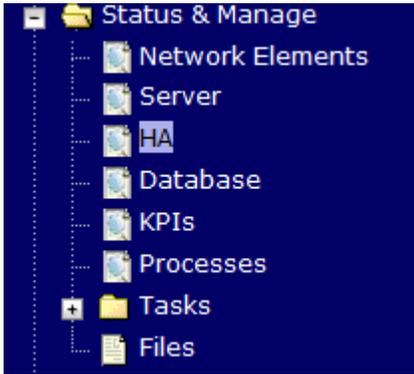
Procedure 1: Recovery Scenario 1

<p>18</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 10px auto;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the <i>guiadmin</i> user:</p> 
<p>19</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Monitor and Confirm database restoral</p>	<p>Wait for 5-10 minutes for the System to stabilize with the new topology:</p> <p>Monitor the Info tab for “Success”. This will indicate that the backup is complete and the system is stabilized.</p> <p>Following alarms must be ignored for NOAM and MP Servers until all the Servers are configured:</p> <p>Alarms with Type Column as “REPL”, “COLL”, “HA” (with mate NOAM), “DB” (about Provisioning Manually Disabled)</p> <p>Note: Do not pay attention to alarms until all the servers in the system are completely restored.</p> <p>Note: The Configuration and Maintenance information will be in the same state it was backed up during initial backup.</p>
<p>20</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Login</p>	<p>Login to the recovered Active NOAM via SSH terminal as root (5.0) or admusr(6.0+) user.</p>

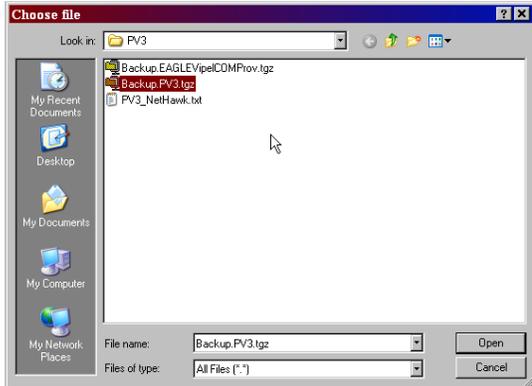
Procedure 1: Recovery Scenario 1

<p>21 <input type="checkbox"/></p>	<p>ACTIVE NOAM: Restore /etc/hosts/ File of the Active NOAM (DSR 5.0/6.0/7.0 ONLY)</p>	<p>IF DSR 7.1, SKIP THIS STEP</p> <p>Execute the following command:</p> <pre style="background-color: #f0f0f0; padding: 5px;">\$ sudo AppWorks AppWorks_AppWorks updateServerAliases <NOAM Host Name></pre>
<p>22 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover Standby NOAM</p>	<p>Install the second NOAM server by executing procedure “<i>Configure the Second NOAM Server</i>”, steps 1, 4, 5, 6 - Refer to Table 5 for the applicable DSR software installation and configuration reference.</p> <p>Note: Execute step 7 if Netbackup is used.</p> <p>If NetBackup is used, execute procedure “<i>Install NetBackup Client</i>” - Refer to Table 5 for the applicable DSR software installation and configuration reference.</p> <p>Note: If Topology or nodeld alarms are persistent after the database restore, refer to Appendix G. Workarounds for Issues not fixed in this Release</p>
<p>23 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Restart DSR application</p>	<p>Navigate to Main Menu->Status & Manage->Server,</p>  <p>Select the recovered standby NOAM server and click on Restart.</p> <div style="display: flex; justify-content: center; gap: 10px;"> Stop Restart Reboot NTP Sync Report </div>

Procedure 1: Recovery Scenario 1

<p>24</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Set HA on Standby NOAM</p>	<p>Navigate to Status & Manage -> HA</p>  <p>Click on Edit at the bottom of the screen</p> <p>Select the standby NOAM server, set it to Active</p> <p>Press OK</p>
<p>25</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Stop Replication to the C-Level Servers of this Site.</p>	<p>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</p>  <p>Execute Appendix E. Inhibit A and B Level</p>  <p>Replication on C-Level Servers</p>
<p>26</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover Active SOAM Server</p>	<p>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.</p> <p>Note: If you are using Netbackup, also execute step 11.</p>

Procedure 1: Recovery Scenario 1

<p>27</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Upload the backed up SOAM Database file</p>	<p>Navigate to Main Menu->Status & Manage->Files</p> <p>Select the Active SOAM server. The following screen will appear. Click on Upload as shown below and select the file “SO Provisioning and Configuration:” file backed up after initial installation and provisioning.</p>  <p>Click on Browse and Locate the backup file and click on Open as shown below.</p>   <p>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.</p>
---	---	--

Procedure 1: Recovery Scenario 1

28 <input type="checkbox"/>	Recovered SOAM GUI: Login	<p>Establish a GUI session on the recovered SOAM server. Open the web browser and enter a URL of:</p> <div data-bbox="492 365 1346 407" style="border: 1px solid black; padding: 2px;"><code>http://<Recovered_SOAM_IP_Address></code></div> <p>Login as the <i>guiadmin</i> user:</p> <div data-bbox="565 499 1349 1087" style="text-align: center;"></div>
--------------------------------	----------------------------------	---

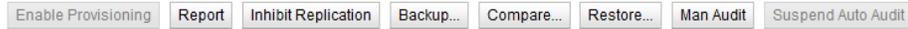
Procedure 1: Recovery Scenario 1

29

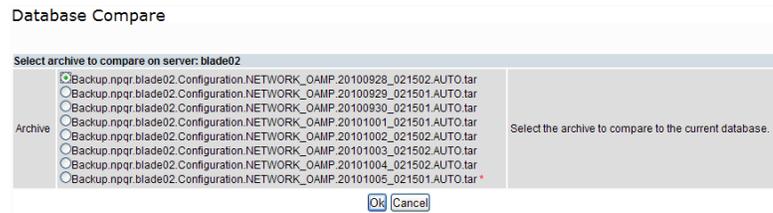
Recovered SOAM GUI:
Verify the Archive Contents and Database Compatibility

Click on **Main Menu->Status & Manage->Database**

Select the **Active SOAM** server and click on the **Compare**.

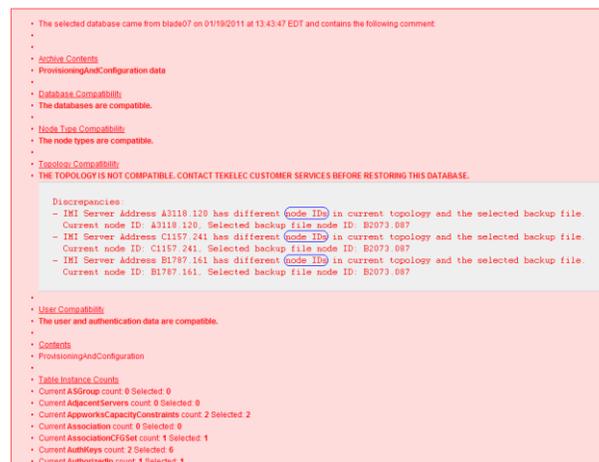


The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 13** of this procedure.



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)**



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:

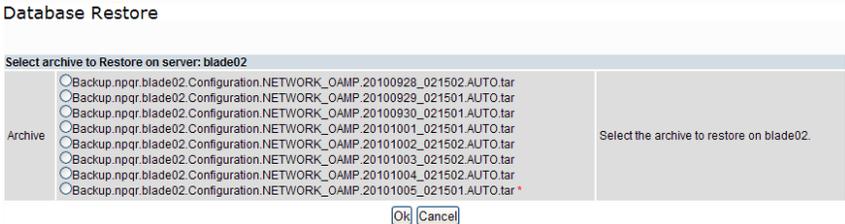
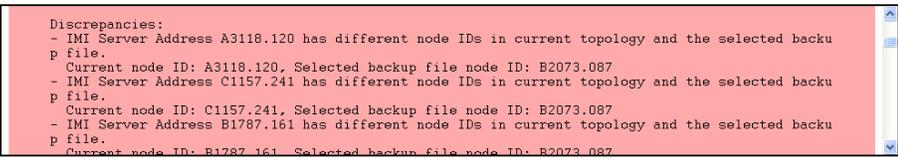
Topology Compatibility

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.

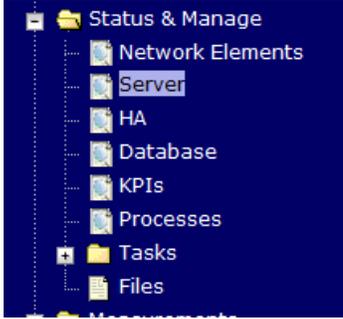
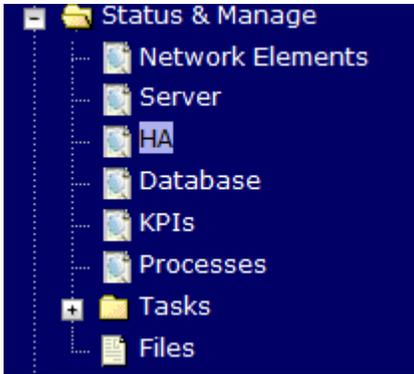
Procedure 1: Recovery Scenario 1

<p>30</p> <p><input type="checkbox"/></p>	<p>Recovered SOAM GUI: Restore the Database</p>	<p>Select the Active SOAM server, and click on Restore as shown below.</p> <p>The following screen will be displayed. Select the proper back up provisioning and configuration file.</p>  <p>Database Restore</p> <p>Select archive to Restore on server: blade02</p> <p>Archive</p> <ul style="list-style-type: none"> <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20100928_021502.AUTO.tar <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20100929_021501.AUTO.tar <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20100930_021501.AUTO.tar <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20101001_021501.AUTO.tar <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20101002_021502.AUTO.tar <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20101003_021502.AUTO.tar <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20101004_021502.AUTO.tar <input checked="" type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20101005_021501.AUTO.tar * <p>Select the archive to restore on blade02.</p> <p><input type="button" value="Ok"/> <input type="button" value="Cancel"/></p> <p>Click OK Button. The following confirmation screen will be displayed.</p> <p>If you get an error that the NodeIDs do not match. That is expected. If no other errors beside the NodeIDs are displayed, select the Force checkbox as shown above and Click OK to proceed with the DB restore.</p> <p>Database Restore Confirm</p> <p>Incompatible database selected</p>  <p>Discrepancies:</p> <ul style="list-style-type: none"> - IMI Server Address A3118.120 has different node IDs in current topology and the selected backup 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 backup 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 backup file. - Current node ID: B1787.161, Selected backup file node ID: B2073.087 <p>Confirm archive "3bladeNPQR.blade07.Configuration.NETWORK_OAMP.20110119_184253.MAN.tar" to Restore on server: blade07</p> <p>Force Restore? <input checked="" type="checkbox"/> Force <input type="checkbox"/> Force restore on blade07, despite compare errors.</p> <p><input type="button" value="Ok"/> <input type="button" value="Cancel"/></p> <p>Note: After the restore has started, the user will be logged out of XMI SOAM GUI since the restored Topology is old data.</p>
<p>31</p> <p><input type="checkbox"/></p>	<p>Recovered SOAM GUI: Monitor and Confirm database restoral</p>	<p>Wait for 5-10 minutes for the System to stabilize with the new topology:</p> <p>Monitor the Info tab for "Success". This will indicate that the backup is complete and the system is stabilized.</p> <p>Note: Do not pay attention to alarms until all the servers in the system are completely restored.</p> <p>Note: The Configuration and Maintenance information will be in the same state it was backed up during initial backup.</p>

Procedure 1: Recovery Scenario 1

<p>32 □</p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 10px auto;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the <i>guiadmin</i> user:</p> <div style="text-align: center; margin: 20px 0;">  </div> <div style="text-align: center;"> <p>Oracle System Login Fri Mar 20 12:29:52 2015 EDT</p> <hr style="width: 50%; margin: 0 auto;"/> <div style="border: 1px solid gray; padding: 10px; width: 80%; margin: 10px auto;"> <p style="text-align: center;">Log In</p> <p style="text-align: center;">Enter your username and password to log in</p> <p>Username: <input type="text" value="guiadmin"/></p> <p>Password: <input type="password" value="••••••"/></p> <p style="text-align: center;"><input type="checkbox"/> Change password</p> <p style="text-align: center;"><input type="button" value="Log In"/></p> </div> <p style="text-align: center; margin-top: 10px;">Welcome to the Oracle System Login.</p> <p style="text-align: center; font-size: small;">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.</p> <hr style="width: 50%; margin: 0 auto;"/> <p style="text-align: center; font-size: x-small;">Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</p> </div>
<p>33 □</p>	<p>NOAM VIP GUI: Recover the Remaining SOAM Servers</p>	<p>Recover the remaining SOAM servers (standby, spare) by repeating the following steps for each SOAM server:</p> <ol style="list-style-type: none"> 1. Install the remaining SOAM servers by executing reference 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. <p>Note: Execute step 11 as well if Netbackup is used.</p> <ol style="list-style-type: none"> 2. If you are using Netbackup, execute procedure “<i>Install Netbackup Client</i>” - Refer to Table 5 for the applicable DSR software installation and configuration reference.

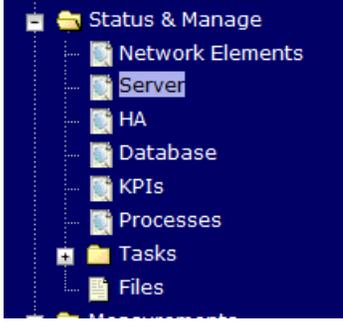
Procedure 1: Recovery Scenario 1

34 <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application	Navigate to Main Menu->Status & Manage->Server ,  Select the recovered standby SOAM server and click on Restart . 
35 <input type="checkbox"/>	NOAM VIP GUI: Set HA on Standby SOAM	Navigate to Status & Manage -> HA  Click on Edit at the bottom of the screen Select the standby SOAM server, set it to Active Press OK

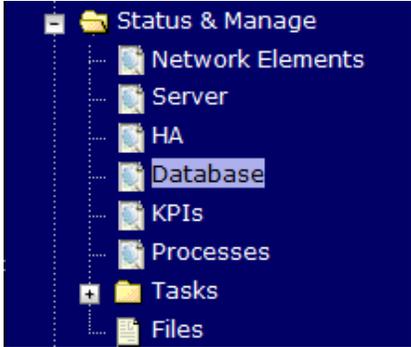
Procedure 1: Recovery Scenario 1

<p>36</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Start Replication on Working C-Level Servers</p>	<p>Un-Inhibit (<i>Start</i>) Replication to the working C-Level Servers which belong to the same site as of the failed SOAM servers.</p> <p>Execute Appendix F. Un-Inhibit A and B Level Replication on C-Level Servers</p> <p>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:</p> <ul style="list-style-type: none"> • 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 (<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>) <p>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”.</p>  <p>The screenshot shows a horizontal row of buttons: 'Disable Provisioning', 'Report...', 'Allow Replication', 'Backup...', 'Compare...', and 'Restore...'. The 'Allow Replication' button is highlighted with a red oval.</p>
<p>37</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover the C-Level Server (DA-MP, SBRs, IPFE, SS7-MP)</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>Repeat this step for any remaining failed MP servers.</p>

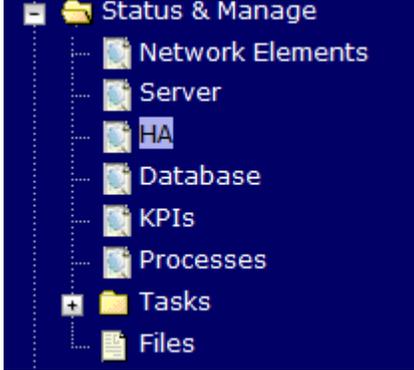
Procedure 1: Recovery Scenario 1

38 <input type="checkbox"/>	NOAM VIP GUI: Restart DSR Application on recovered C-Level Servers.	<p>Navigate to Main Menu->Status & Manage->Server</p>  <p>Select the recovered C-Level servers and click on Restart.</p> <p><input type="button" value="Stop"/> <input type="button" value="Restart"/> <input type="button" value="Reboot"/> <input type="button" value="NTP Sync"/> <input type="button" value="Report"/></p>
--------------------------------	---	---

Procedure 1: Recovery Scenario 1

39 <input type="checkbox"/>	NOAM VIP GUI: Start replication on all C-Level Servers	<p>Un-Inhibit (<i>Start</i>) Replication to the ALL C-Level Servers</p> <p>Navigate to Status & Manage -> Database</p>  <p>If the "<i>Repl Status</i>" is set to "Inhibited", click on the Allow Replication button as shown below using the following order:</p> <ul style="list-style-type: none">• 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 (<i>if MPs are configured as Active/Standby, start with the Active MP, otherwise the order of the MPs does not matter</i>) <p>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".</p> 
--------------------------------	--	---

Procedure 1: Recovery Scenario 1

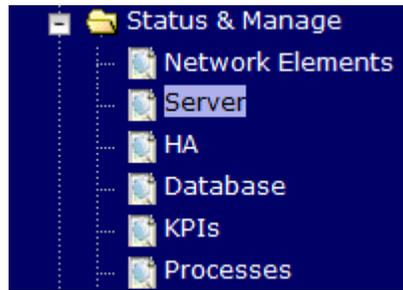
<p>40</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Set HA on all C-Level Servers</p>	<p>Navigate to Status & Manage -> HA</p>  <p>Click on Edit at the bottom of the screen</p> <p>For each server whose Max Allowed HA Role is set to Standby, set it to Active</p> <p>Press OK</p>
<p>41</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Perform key exchange between the active-NOAM and recovered servers.</p>	<p>Establish an SSH session to the Active NOAM, login as admusr.</p> <p>Execute the following command to perform a keyexchange from the active NOAM to each recovered server:</p> <pre>\$ keyexchange admusr@<Recovered Server Hostname></pre> <p>Note: If an export server is configured, perform this step.</p>
<p>42</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Activate Optional Features</p>	<p>Establish an SSH session to the active NOAM, login as admusr.</p> <p>Refer to section 1.5 Optional Features to activate any features that were previously activated.</p>

Procedure 1: Recovery Scenario 1

43

NOAM VIP GUI:
Fetch and Store
the database
Report for the
Newly Restored
Data and Save it

Navigate to **Configuration-> Server**



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]

Tue Oct 05 15:13:38 2010 UTC

```

=====
N P Q R Database Status Report
=====
Report Generated: Tue Oct 05 15:13:38 2010 UTC
From: Active Network OAM&P on host blade07
Report Version: 3.0.13-3.0.0_10.13.0
User: guadmin
=====

General
-----
Hostname           : blade07
Appworks Database Version : 3.0
Application Database Version :
-----

Capacities and Utilization
-----
Disk Utilization   0.6%: 249M used of 40G total, 38G available
Memory Utilization 0.6%: 136M used of 23975M total, 23839M available
-----

Alarms
-----
None
-----

Maintenance in Progress
-----
Restore operation success
-----

Service Information
-----
Part: A_NpqrProvPart
-----

Table Name          Row Size  Num  Memory  Disk
Schema  Avg  Max  Rows  Used / Alloc  Used / Alloc
-----
CgPa              44          1  44 B   44 B   44 B
CgPaGta           52          0    0 B    0 B    0 B
CgPaInfo          64          1  64 B   64 B   64 B
CgPaOpc           36          0    0 B    0 B    0 B
CountryCode       24          306 7344 B 7344 B 7344 B
GTConfig          52          2  104 B  104 B  104 B
MccMnc            40          0    0 B    0 B    0 B
Msisdn            52          0    0 B    0 B    0 B
Msrn              68          0    0 B    0 B    0 B
NpqrNeOptions     276         0    0 B    0 B    0 B
=====

```

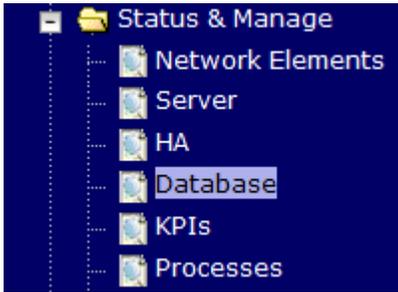
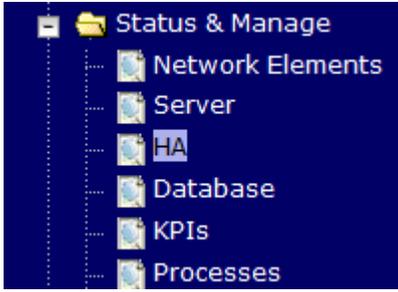
Print Save

Click on **Save** and save the report to your local machine.

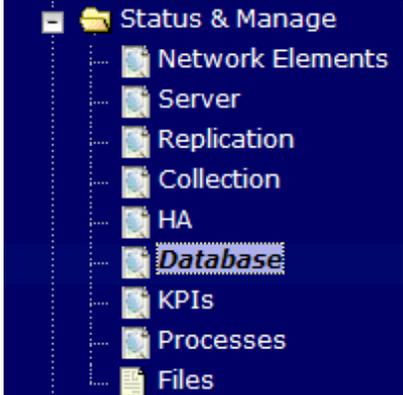
Procedure 1: Recovery Scenario 1

<p>44</p> <p>□</p>	<p>ACTIVE NOAM: Verify Replication Between Servers.</p>	<p>Login to the Active NOAM via SSH terminal as root(5.0) or admusr(6.0+) user. Execute the following command:</p> <pre>\$ sudo irepstat -m</pre> <p>Output like below shall be generated:</p> <pre>-- 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 Oahu-SOAM-2 -- Active AB From Oahu-NOAM-2 Active 0 0.50 ^0.03%cpu 24B/s BB To Oahu-SOAM-1 Active 0 0.50 1%R 0.04%cpu 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</pre>
--------------------	--	--

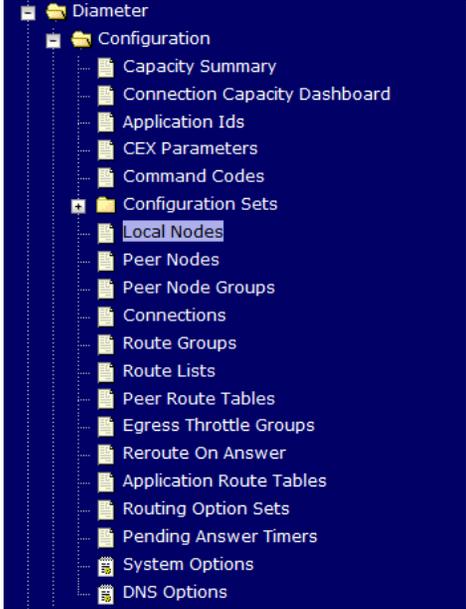
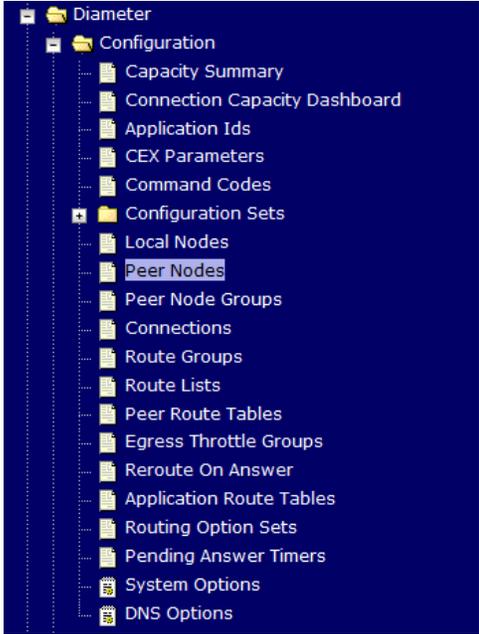
Procedure 1: Recovery Scenario 1

<p>45</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Verify the Database states</p>	<p>Click on Main Menu->Status and Manager->Database</p>  <p>Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below:</p> <table border="1" data-bbox="488 751 1438 955"> <thead> <tr> <th>Network Element</th> <th>Server</th> <th>Role</th> <th>OAM Max HA Role</th> <th>Application Max HA Role</th> <th>Status</th> <th>DB Level</th> <th>OAM Repl Status</th> <th>SIG Repl Status</th> <th>Repl Status</th> <th>Repl Audit Status</th> </tr> </thead> <tbody> <tr> <td>NO_10303</td> <td>NO2</td> <td>Network OAM&P</td> <td>Active</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutolnProg</td> </tr> <tr> <td>SO_10303</td> <td>PSBR</td> <td>MP</td> <td>Active</td> <td>Active</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>Normal</td> <td>Allowed</td> <td>AutolnProg</td> </tr> <tr> <td>SO_10303</td> <td>MP2</td> <td>MP</td> <td>Active</td> <td>Active</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>Normal</td> <td>Allowed</td> <td>AutolnProg</td> </tr> <tr> <td>SO_10303</td> <td>SO1</td> <td>System OAM</td> <td>Standby</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutolnProg</td> </tr> <tr> <td>NO_10303</td> <td>NO1</td> <td>Network OAM&P</td> <td>Standby</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutolnProg</td> </tr> <tr> <td>SO_10303</td> <td>IPFE</td> <td>MP</td> <td>Active</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>Normal</td> <td>Allowed</td> <td>AutolnProg</td> </tr> <tr> <td>SO_10303</td> <td>SO2</td> <td>System OAM</td> <td>Active</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutolnProg</td> </tr> </tbody> </table>	Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status	NO_10303	NO2	Network OAM&P	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg	SO_10303	PSBR	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutolnProg	SO_10303	MP2	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutolnProg	SO_10303	SO1	System OAM	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg	NO_10303	NO1	Network OAM&P	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg	SO_10303	IPFE	MP	Active	OOS	Normal	0	Normal	Normal	Allowed	AutolnProg	SO_10303	SO2	System OAM	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg
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	NO2	Network OAM&P	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg																																																																																
SO_10303	PSBR	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutolnProg																																																																																
SO_10303	MP2	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutolnProg																																																																																
SO_10303	SO1	System OAM	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg																																																																																
NO_10303	NO1	Network OAM&P	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg																																																																																
SO_10303	IPFE	MP	Active	OOS	Normal	0	Normal	Normal	Allowed	AutolnProg																																																																																
SO_10303	SO2	System OAM	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg																																																																																
<p>46</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Verify the HA Status</p>	<p>Click on Main Menu->Status and Manager->HA</p>  <p>Select the row for all of the servers Verify that the “HA Role” is either “Active” or “Standby”.</p> <table border="1" data-bbox="488 1482 1438 1656"> <thead> <tr> <th>Hostname</th> <th>OAM Max HA Role</th> <th>Application Max HA Role</th> <th>Max Allowed HA Role</th> <th>Mate Hostname List</th> <th>Network Element</th> <th>Server Role</th> <th>Active VIPs</th> </tr> </thead> <tbody> <tr> <td>NO2</td> <td>Active</td> <td>OOS</td> <td>Active</td> <td>NO1</td> <td>NO_10303</td> <td>Network OAM&P</td> <td>10.240.70.132</td> </tr> <tr> <td>SO1</td> <td>Standby</td> <td>OOS</td> <td>Active</td> <td>SO2</td> <td>SO_10303</td> <td>System OAM</td> <td></td> </tr> <tr> <td>SO2</td> <td>Active</td> <td>OOS</td> <td>Active</td> <td>SO1</td> <td>SO_10303</td> <td>System OAM</td> <td>10.240.70.133</td> </tr> <tr> <td>MP1</td> <td>Standby</td> <td>Active</td> <td>Active</td> <td>MP2</td> <td>SO_10303</td> <td>MP</td> <td></td> </tr> <tr> <td>MP2</td> <td>Active</td> <td>Active</td> <td>Active</td> <td>MP1</td> <td>SO_10303</td> <td>MP</td> <td></td> </tr> <tr> <td>IPFE</td> <td>Active</td> <td>OOS</td> <td>Active</td> <td></td> <td>SO_10303</td> <td>MP</td> <td></td> </tr> </tbody> </table>	Hostname	OAM Max HA Role	Application Max HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role	Active VIPs	NO2	Active	OOS	Active	NO1	NO_10303	Network OAM&P	10.240.70.132	SO1	Standby	OOS	Active	SO2	SO_10303	System OAM		SO2	Active	OOS	Active	SO1	SO_10303	System OAM	10.240.70.133	MP1	Standby	Active	Active	MP2	SO_10303	MP		MP2	Active	Active	Active	MP1	SO_10303	MP		IPFE	Active	OOS	Active		SO_10303	MP																																	
Hostname	OAM Max HA Role	Application Max HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role	Active VIPs																																																																																			
NO2	Active	OOS	Active	NO1	NO_10303	Network OAM&P	10.240.70.132																																																																																			
SO1	Standby	OOS	Active	SO2	SO_10303	System OAM																																																																																				
SO2	Active	OOS	Active	SO1	SO_10303	System OAM	10.240.70.133																																																																																			
MP1	Standby	Active	Active	MP2	SO_10303	MP																																																																																				
MP2	Active	Active	Active	MP1	SO_10303	MP																																																																																				
IPFE	Active	OOS	Active		SO_10303	MP																																																																																				

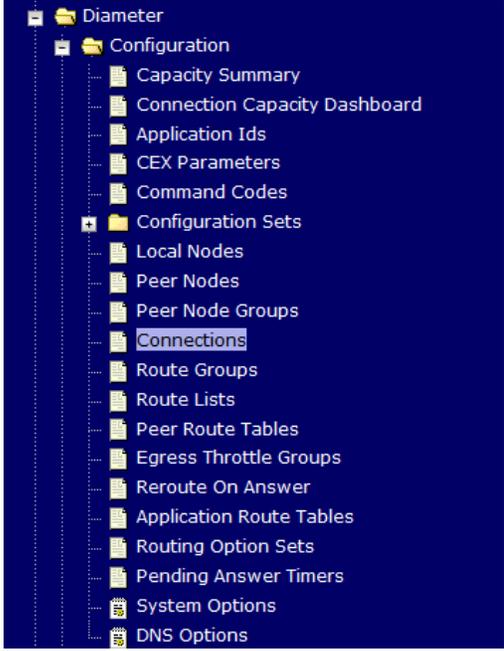
Procedure 1: Recovery Scenario 1

47 <input type="checkbox"/>	NOAM GUI: Enable Provisioning	<p>Click on Main Menu->Status & Manage->Database</p>  <p>Enable Provisioning by clicking on Enable Provisioning button at the bottom of the screen as shown below.</p>  <p>A confirmation window will appear, press OK to enable Provisioning.</p> 
--------------------------------	--	--

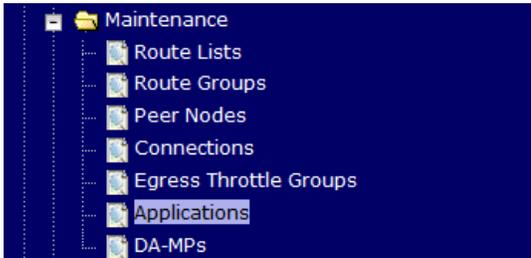
Procedure 1: Recovery Scenario 1

<p>48</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Verify the Local Node Info</p>	<p>Navigate to Main Menu->Diameter->Configuration->Local Node</p>  <p>Verify that all the local nodes are shown.</p>
<p>49</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Verify the Peer Node Info</p>	<p>Navigate to Main Menu->Diameter->Configuration->Peer Node</p>  <p>Verify that all the peer nodes are shown.</p>

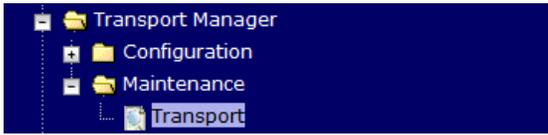
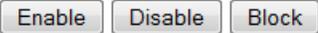
Procedure 1: Recovery Scenario 1

<p>50</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Verify the Connections Info</p>	<p>Navigate to Main Menu->Diameter->Configuration->Connections</p>  <p>Verify that all the connections are shown.</p>
<p>51</p> <p><input type="checkbox"/></p>	<p>MP Servers: Disable SCTP Auth Flag- DSR 7.1 Only</p>	<p>For DSR 7.1 Only: For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix in [17].</p> <p>Execute this procedure on all Failed MP Servers.</p>

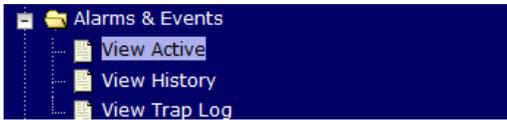
Procedure 1: Recovery Scenario 1

<p>52</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Enable Connections if needed</p>	<p>Navigate to Main Menu->Diameter->Maintenance->Connections</p>  <p>Select each connection and click on the Enable button. Alternatively you can enable all the connections by selecting the EnableAll button.</p> <p><input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="EnableAll"/> <input type="button" value="DisableAll"/> <input type="button" value="Diagnose Start"/> <input type="button" value="Diagnose End"/> <input type="button" value="SCTP STATISTICS"/> <input type="checkbox"/> Pause updates</p> <p>Verify that the Operational State is Available.</p> <p>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</p>
<p>53</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Enable Optional Features</p>	<p>Navigate to Main Menu -> Diameter -> Maintenance -> Applications</p>  <p>Select the optional feature application configured in step 42.</p> <p>Click the Enable button.</p> <p><input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="checkbox"/> Pause updates</p>

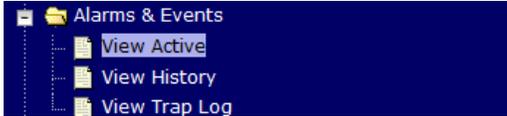
Procedure 1: Recovery Scenario 1

<p>54</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable Transports if Needed (Applicable ONLY for DSR 6.0+)</p>	<p>Navigate to Main Menu->Transport Manager -> Maintenance -> Transport</p>  <p>Select each transport and click on the Enable button</p>  <p>Verify that the Operational Status for each transport is Up.</p>
<p>55</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable MAPIWF application if needed (Applicable ONLY for DSR 6.0+)</p>	<p>Navigate to Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users</p>  <p>Click on the Enable button corresponding to MAPIWF Application Name.</p>  <p>Verify that the SSN Status is Enabled.</p>
<p>56</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable links if needed (Applicable ONLY for DSR 6.0+)</p>	<p>Navigate to Main Menu->SS7/Sigtran->Maintenance->Links</p>  <p>Click on Enable button for each link.</p>  <p>Verify that the Operational Status for each link is Up.</p>

Procedure 1: Recovery Scenario 1

<p>57</p> <p><input type="checkbox"/></p>	<p>Active NOAM: Verify Sync Split Scope Data (If POLICY AND CHARGING DRA is activated): 5.0/6.0 Only</p>	<p>If recovering a DSR 5.0/6.0 system and POLICY AND CHARGING DRA application is activated then execute this step.</p> <p>Note: If recovering a DSR 7.0+ system, DO NOT execute this step</p> <p>Login to the Active NOAM VIP via SSH terminal as root(5.0) or admusr(6.0+) user.</p> <p>Execute the following steps:</p> <p>Go to Appworks bin directory:</p> <pre>\$ sudo cd /usr/TKLC/appworks/bin/</pre> <p>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:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -reportonly</pre> <p>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.</p> <p>The “sync” option will modify the database:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -sync</pre> <p>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”:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -reportonly</pre>
<p>58</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Examine All Alarms</p>	<p>Navigate to Main Menu->Alarms & Events->View Active</p>  <p>Examine all active alarms and refer to the on-line help on how to address them.</p> <p>If needed contact Appendix H. My Oracle Support (MOS).</p>

Procedure 1: Recovery Scenario 1

<p>59 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Examine All Alarms</p>	<p>Login to the NOAM VIP if not already logged in.</p> <p>Navigate to Main Menu->Alarms & Events->View Active</p>  <p>Examine all active alarms and refer to the on-line help on how to address them.</p> <p>If needed contact Appendix H. My Oracle Support (MOS).</p>
<p>60 <input type="checkbox"/></p>	<p>Restore GUI Username and Passwords</p>	<p>If applicable, Execute steps in Section 6.0 to recover the user and group information restored.</p>
<p>61 <input type="checkbox"/></p>	<p>Backup and Archive All the Databases from the Recovered System</p>	<p>Execute Appendix A. DSR Database Backup to back up the Configuration databases:</p>

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.

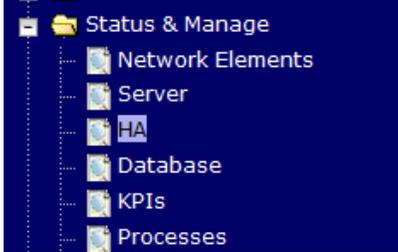
- Recover the base hardware.
- Recover the software.
- The database has already been restored at the active SOAM server and does not require restoration at the SO and MP servers.

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

Procedure 2: Recovery Scenario 2

<p>S T E P #</p>	<p>This procedure performs recovery if at least 1 NOAM server is available but all SOAM servers in a site have failed. This includes any SOAM server that is in another location.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>Workarounds</p>	<p>Refer to Appendix G. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.</p>
<p>2 <input type="checkbox"/></p>	<p>Gather Required Materials</p>	<p>Gather the documents and required materials listed in Section 3.1 Required Materials</p>
<p>3 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>http://<Primary_NOAM_VIP_IP_Address></p> </div> <p>Login as the <i>guiadmin</i> user:</p> <div style="text-align: center; margin: 20px 0;">  </div> <div style="text-align: center; margin: 10px 0;"> <p>Oracle System Login Fri Mar 20 12:29:52 2015 EDT</p> <hr style="width: 50%; margin: 0 auto;"/> </div> <div style="text-align: center; margin: 20px 0;"> <div style="border: 1px solid gray; padding: 10px; width: fit-content; margin: 0 auto;"> <p>Log In Enter your username and password to log in</p> <p>Username: <input type="text" value="guiadmin"/></p> <p>Password: <input type="password" value="••••••"/></p> <p><input type="checkbox"/> Change password</p> <p><input type="button" value="Log In"/></p> </div> </div> <p style="text-align: center; margin: 10px 0;">Welcome to the Oracle System Login.</p> <p style="text-align: center; margin: 10px 0;">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.</p> <hr style="width: 50%; margin: 0 auto;"/> <p style="text-align: center; margin: 10px 0;"><small>Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</small></p>

Procedure 2: Recovery Scenario 2

<p>4</p> <p><input type="checkbox"/></p>	<p>Active NOAM: Set Failed Servers to Standby</p>	<p>Navigate to Main Menu -> Status & Manage -> HA</p>  <p>Select Edit</p> <p>Set the Max Allowed HA Role drop down box to Standby for the failed servers.</p> <p>Select Ok</p> 
<p>5</p> <p><input type="checkbox"/></p>	<p>RMS NOAM Failure</p>	<ol style="list-style-type: none"> 1. HW vendor to replace the failed equipment 2. Execute the <i>“iLO Configuration Procedure”</i> 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. 5. 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. 6. If the failed NOAM is NOT co-hosted with the PMAC on the first rack mount server, execute <i>procedure “Initial Product Manufacture of Application Server”</i> - Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR software installation/configuration guide reference. <p>Now execute <i>procedure “Configure TVOE on Additional RMS Servers(s)”</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.</p>

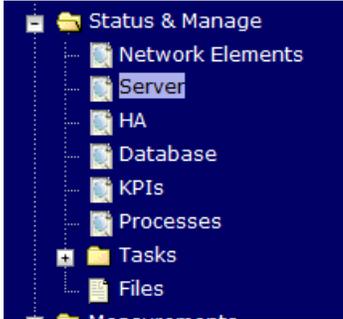
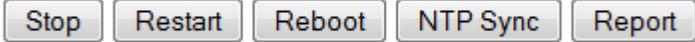
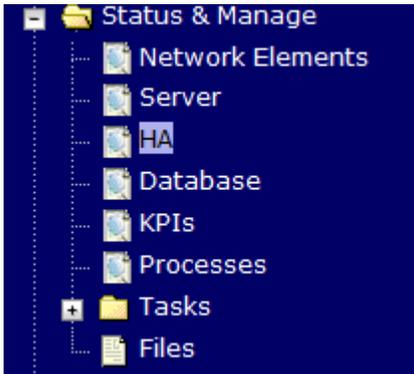
Procedure 2: Recovery Scenario 2

<p>6 □</p>	<p>HP-Class Blade Failure</p>	<p>If the failed server is an HP C-Class Blade, execute this step; otherwise skip to the next step.</p> <ol style="list-style-type: none"> 1. HW vendor to replace the failed equipment 2. Execute procedure “<i>Confirm/Update blade Server BIOS Settings</i>” – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 3. Execute procedure “<i>Configure Blade Server iLO Password for Administrator Account</i>” – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 4. Perform any needed firmware upgrades – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 5. 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.
<p>6 □</p>	<p>RMS NOAM Failure</p>	<ol style="list-style-type: none"> 1. HW vendor to replace the failed equipment 2. Execute the “<i>iLO Configuration Procedure</i>” 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. 5. 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 Server</i>” - Refer to Table 5 for the applicable DSR software installation/configuration guide reference. 6. If the failed NOAM is NOT co-hosted with the PMAC on the first rack mount server, execute procedure “<i>Initial Product Manufacture of Application Server</i>” - Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR software installation/configuration guide reference. <p>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.</p>

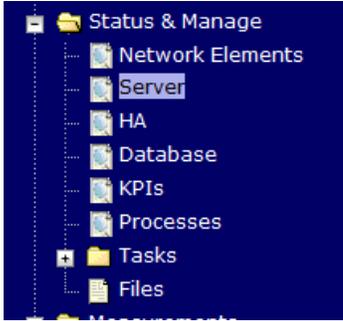
Procedure 2: Recovery Scenario 2

7 <input type="checkbox"/>	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 <input type="checkbox"/>	Create VMs	For NOAMs, execute procedure "Create NOAM Guest VMs" - Refer to Table 5 for the applicable DSR software installation and configuration reference. For SOAMs, execute procedure "Create SOAM Guest VMs" - Refer to Table 5 for the applicable DSR software installation and configuration reference.
9 <input type="checkbox"/>	IPM Failed Guest/Servers	IPM the failed guests/servers by executing procedure "IPM Blades and VMs" - Refer to Table 5 for the applicable DSR software installation and configuration reference.
10 <input type="checkbox"/>	Install DSR application on Failed Guests/Servers	Install the DSR application on the failed guests/server by executing procedure "Install Application Software on Blades" - Refer to Table 5 for the applicable DSR software installation and configuration reference.
11 <input type="checkbox"/>	Repeat for Remaining Failed Servers	If necessary, repeat steps 1-7 for all remaining failed servers.
12 <input type="checkbox"/>	NOAM VIP GUI: Login	<p>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:</p> <div data-bbox="492 930 1344 972" style="border: 1px solid black; padding: 2px;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the <i>guiadmin</i> user:</p> <div data-bbox="492 1060 1344 1648" style="text-align: center;">  </div>

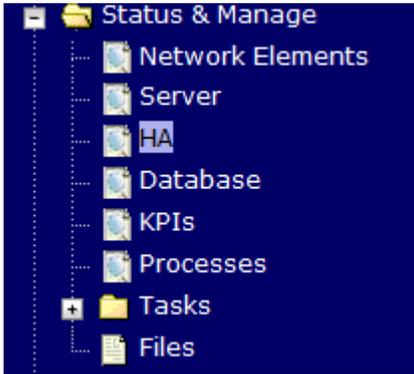
Procedure 2: Recovery Scenario 2

<p>13 □</p>	<p>NOAM VIP GUI: Recover Standby NOAM</p>	<p>Install the second NOAM server by executing procedure “<i>Configure the Second NOAM Server</i>”, steps 1, 2, 4-6, and 8 - Refer to Table 5 for the applicable DSR software installation and configuration reference.</p> <p>Note: Execute step 7 if Netbackup is used.</p> <p>If NetBackup is used, execute procedure “<i>Install NetBackup Client</i>” - Refer to Table 5 for the applicable DSR software installation and configuration reference.</p>
<p>14 □</p>	<p>NOAM VIP GUI: Restart DSR application</p>	<p>Navigate to Main Menu->Status & Manage->Server,</p>  <p>Select the recovered standby NOAM server and click on Restart.</p> 
<p>15 □</p>	<p>NOAM VIP GUI: Set HA on Standby NOAM</p>	<p>Navigate to Status & Manage -> HA</p>  <p>Click on Edit at the bottom of the screen</p> <p>Select the standby NOAM server, set it to Active</p> <p>Press OK</p>

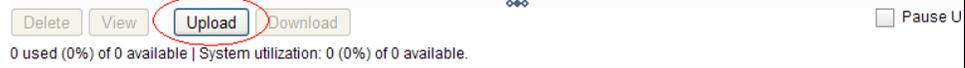
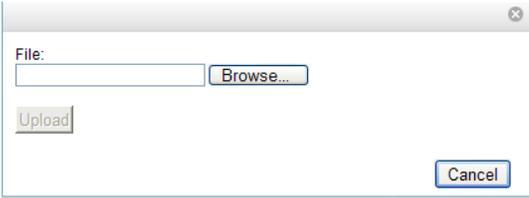
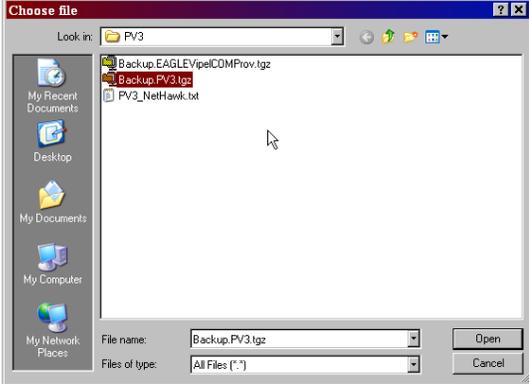
Procedure 2: Recovery Scenario 2

<p>16 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Stop Replication to the C-Level Servers of this Site.</p>	<p>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</p> <p style="text-align: center;"> Execute Appendix E. Inhibit A and B Level</p> <p style="text-align: center;"></p> <p>Replication on C-Level Servers</p>
<p>17 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover Active SOAM Server</p>	<p>Install the First SOAM server 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.</p> <p>Note: If you are using Netbackup, also execute step 10.</p>
<p>18 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Restart DSR application</p>	<p>Navigate to Main Menu->Status & Manage->Server,</p>  <p>Select the recovered Active SOAM server and click on Restart.</p> <p style="text-align: center;"> <input type="button" value="Stop"/> <input type="button" value="Restart"/> <input type="button" value="Reboot"/> <input type="button" value="NTP Sync"/> <input type="button" value="Report"/> </p>

Procedure 2: Recovery Scenario 2

19 <input type="checkbox"/>	NOAM VIP GUI: Set HA on Active SOAM	Navigate to Status & Manage -> HA  Click on Edit at the bottom of the screen Select the Active SOAM server, set it to Active Press OK
--------------------------------	--	---

Procedure 2: Recovery Scenario 2

<p>20 □</p>	<p>NOAM VIP GUI: Upload the backed up SOAM Database file</p>	<p>Navigate to Main Menu->Status & Manage->Files</p> <p>Select the Active SOAM server. The following screen will appear. Click on Upload as shown below and select the file “SO Provisioning and Configuration:” file backed up after initial installation and provisioning.</p>  <p>0 used (0%) of 0 available System utilization: 0 (0%) of 0 available.</p> <p>Click on Browse and Locate the backup file and click on Open as shown below.</p>   <p>Click on the Upload button.</p> <p>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.</p>
-----------------	---	--

Procedure 2: Recovery Scenario 2

21 <input type="checkbox"/>	Recovered SOAM GUI: Login	<p>Establish a GUI session on the recovered SOAM server. Open the web browser and enter a URL of:</p> <div data-bbox="492 365 1346 407" style="border: 1px solid black; padding: 2px;"><code>http://<Recovered_SOAM_IP_Address></code></div> <p>Login as the <i>guiadmin</i> user:</p> <div data-bbox="565 499 1349 1087" style="text-align: center;"></div>
--------------------------------	----------------------------------	---

Procedure 2: Recovery Scenario 2

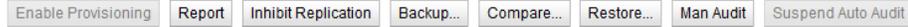
22



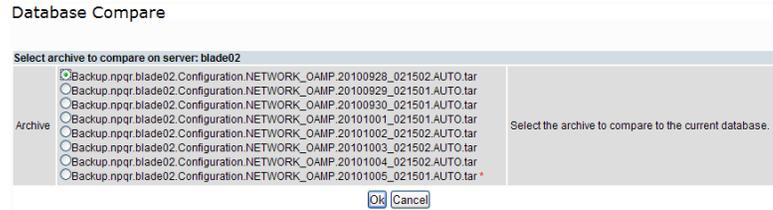
Recovered SOAM GUI:
Verify the Archive Contents and Database Compatibility

Click on **Main Menu->Status & Manage->Database**

Select the **Active SOAM** server and click on the **Compare**.



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.



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)**



Note: Archive Contents and Database Compatibilities must be the following:

- Archive Contents:** Configuration data
- Database Compatibility:** The databases are compatible.

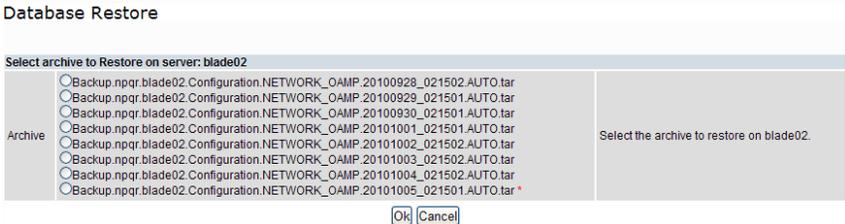
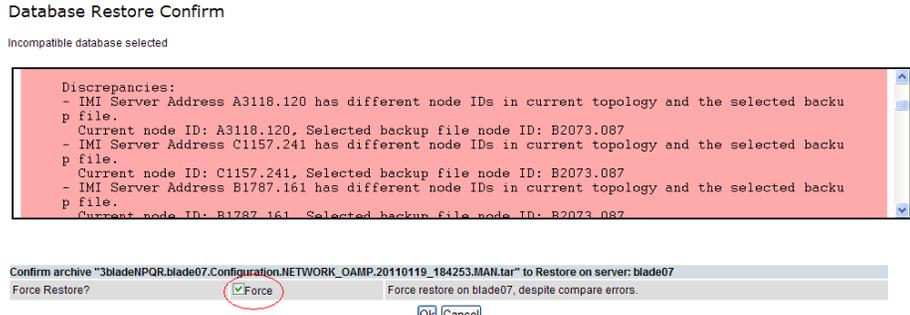
Note: The following is expected Output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM:

Topology Compatibility
THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.

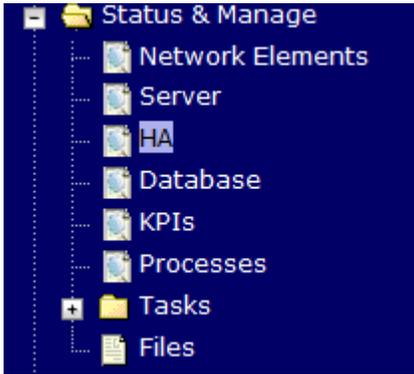
Note: We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility.

If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.

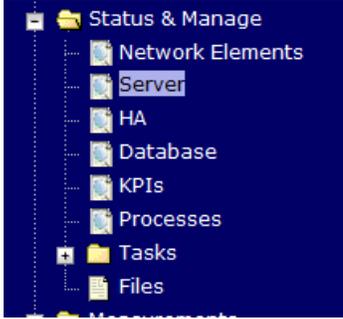
Procedure 2: Recovery Scenario 2

<p>23</p> <p><input type="checkbox"/></p>	<p>Recovered SOAM GUI: Restore the Database</p>	<p>Select the Active SOAM server, and click on Restore as shown below.</p> <p>The following screen will be displayed. Select the proper back up provisioning and configuration file.</p>  <p>Database Restore</p> <p>Select archive to Restore on server: blade02</p> <p>Archive</p> <ul style="list-style-type: none"> <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20100928_021502.AUTO.tar <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20100929_021501.AUTO.tar <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20100930_021501.AUTO.tar <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20101001_021501.AUTO.tar <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20101002_021502.AUTO.tar <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20101003_021502.AUTO.tar <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20101004_021502.AUTO.tar <input type="radio"/> Backup.npq: blade02.Configuration.NETWORK_OAMP.20101005_021501.AUTO.tar * <p><input type="button" value="OK"/> <input type="button" value="Cancel"/></p> <p>Click OK Button. The following confirmation screen will be displayed.</p> <p>If you get an error that the NodeIDs do not match. That is expected. If no other errors beside the NodeIDs are displayed, select the Force checkbox as shown above and Click OK to proceed with the DB restore.</p>  <p>Database Restore Confirm</p> <p>Incompatible database selected</p> <pre> Discrepancies: - IMI Server Address A3118.120 has different node IDs in current topology and the selected backup 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 backup 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 backup file. Current node ID: B1787.161, Selected backup file node ID: B2073.087 </pre> <p>Confirm archive "3bladeNPQR.blade07.Configuration.NETWORK_OAMP.20110119_184253.MAN.tar" to Restore on server: blade07</p> <p>Force Restore? <input checked="" type="checkbox"/> Force <input type="checkbox"/> Force restore on blade07, despite compare errors.</p> <p><input type="button" value="OK"/> <input type="button" value="Cancel"/></p> <p>Note: After the restore has started, the user will be logged out of XMI SOAM GUI since the restored Topology is old data.</p>
<p>24</p> <p><input type="checkbox"/></p>	<p>Recovered SOAM GUI: Monitor and Confirm database restoral</p>	<p>Wait for 5-10 minutes for the System to stabilize with the new topology:</p> <p>Monitor the Info tab for "Success". This will indicate that the backup is complete and the system is stabilized.</p> <p>Note: Do not pay attention to alarms until all the servers in the system are completely restored.</p> <p>Note: The Configuration and Maintenance information will be in the same state it was backed up during initial backup.</p>
<p>25</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover Remaining SOAM Servers</p>	<p>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.</p> <p>Note: If you are using Netbackup, also execute step 10.</p>

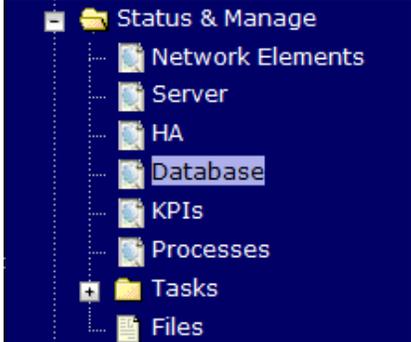
Procedure 2: Recovery Scenario 2

<p>26</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Set HA on SOAM Servers</p>	<p>Navigate to Status & Manage -> HA</p>  <p>Click on Edit at the bottom of the screen</p> <p>For each SOAM server whose Max Allowed HA Role is set to Standby, set it to Active</p> <p>Press OK</p>
<p>27</p> <p><input type="checkbox"/></p>	<p>Recovered Server: Sync NTP</p>	<p>1) Perform the following to retrieve the remote NTP server:</p> <pre data-bbox="488 982 1419 1314"> \$ 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 </pre> <p>2) Stop ntpd service:</p> <pre data-bbox="488 1409 1419 1446"> \$ sudo service ntpd stop </pre> <p>3) Sync the date to the ntp remote server:</p> <pre data-bbox="488 1541 1419 1579"> \$ sudo ntpdate <NTP remote server> </pre> <p>Note: The remote server below will be that of the one gathered in sub step 1.</p> <p>4) Start the ntp service:</p> <pre data-bbox="488 1766 1419 1803"> \$ sudo service ntpd start </pre>

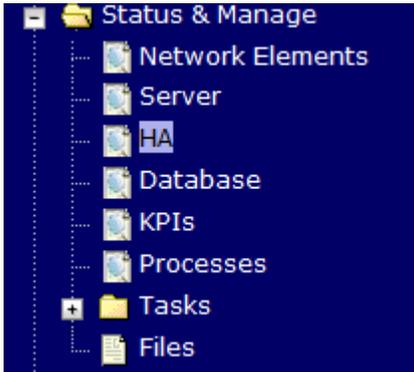
Procedure 2: Recovery Scenario 2

<p>28</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Restart DSR application</p>	<p>Navigate to Main Menu->Status & Manage->Server,</p>  <p>Select the recovered server and click on Restart.</p> 
<p>29</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Start Replication on working C-Level Servers</p>	<p>Un-Inhibit (<i>Start</i>) Replication to the working C-Level Servers which belong to the same site as of the failed SOAM servers.</p> <p>Execute Appendix F. Un-Inhibit A and B Level Replication on C-Level Servers</p> <p>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:</p> <ul style="list-style-type: none"> • 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 (<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>) <p>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”.</p> 

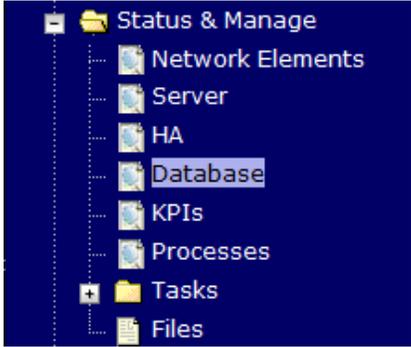
Procedure 2: Recovery Scenario 2

<p>30</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover the C-Level Server (DA-MP, SBRs, IPFE, SS7-MP)</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>Repeat this step for any remaining failed MP servers.</p>
<p>31</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Start replication on ALL C-Level Servers</p>	<p>Un-Inhibit (<i>Start</i>) Replication to the ALL C-Level Servers</p> <p>Navigate to Status & Manage -> Database</p>  <p>If the “<i>Repl Status</i>” is set to “Inhibited”, click on the Allow Replication button as shown below using the following order:</p> <ul style="list-style-type: none"> • 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/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>) <p>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”.</p> 

Procedure 2: Recovery Scenario 2

<p>32</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Set HA on all C-Level Servers</p>	<p>Navigate to Status & Manage -> HA</p>  <p>Click on Edit at the bottom of the screen</p> <p>For each server whose Max Allowed HA Role is set to Standby, set it to Active</p> <p>Press OK</p>
<p>33</p> <p><input type="checkbox"/></p>	<p>Active SOAM: Prepare recovered SOAM for optional feature activation (DSR 5.0/6.0/7.0)</p>	<p>For DSR 5.0/6.0/7.0: If DSR 7.1, skip this step</p> <p>Establish an SSH session to the Active SOAM, login as admusr.</p> <p>Execute the following command:</p> <pre style="border: 1px solid black; padding: 5px;">\$ irem DsrApplication where "name in ('RBAR', 'FABR', 'PCA', 'MD-IWF', 'DM-IWF', 'CPA', 'GLA')"</pre>
<p>34</p> <p><input type="checkbox"/></p>	<p>Active SOAM: Verify Preparation (DSR 5.0/6.0/7.0)</p>	<p>For DSR 5.0/6.0/7.0: If DSR 7.1, skip this step</p> <p>Execute the following command to verify preparation of optional feature activation:</p> <pre style="border: 1px solid black; padding: 5px;">\$ iqt -z -h -p -fname DsrApplication where "name in ('RBAR', 'FABR', 'PCA', 'MD-IWF', 'DM-IWF', 'CPA', 'GLA')"</pre> <p>Note: There should be no output of this command, if there is, verify the correct entry of the command in step 26.</p>
<p>35</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Perform key exchange between the active-NOAM and recovered servers.</p>	<p>Establish an SSH session to the Active NOAM, login as admusr.</p> <p>Execute the following command to perform a keyexchange from the active NOAM to each recovered server:</p> <pre style="border: 1px solid black; padding: 5px;">\$ keyexchange admusr@<Recovered Server Hostname></pre> <p>Note: If an export server is configured, perform this step.</p>

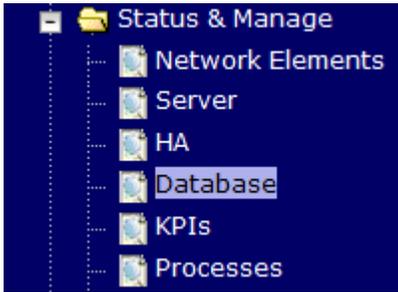
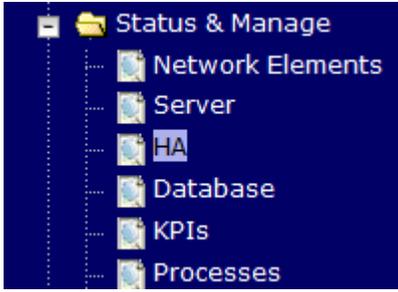
Procedure 2: Recovery Scenario 2

<p>36</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Activate Optional Features</p>	<p>Establish an SSH session to the active NOAM, login as admusr.</p> <p>Refer to section 1.5 Optional Features to activate any features that were previously activated.</p>
<p>37</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Fetch and Store the database Report for the Newly Restored Data and Save it</p>	<p>Navigate to Main Menu -> Status & Manage -> Database</p>  <p>Select the active NOAM server and click on the Report button at the bottom of the page. The following screen is displayed:</p> <p>Main Menu: Status & Manage -> Database [Report]</p> <pre> ===== d s r D a t a b a s e S t a t u s R e p o r t ===== 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: guadmin ===== 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 Alarms ----- None Maintenance in Progress ----- Backup operation success Replication Audit Status ----- Not found Service Information ----- ===== End of d s r D a t a b a s e S t a t u s R e p o r t ===== </pre> <p>Click on Save and save the report to your local machine.</p>

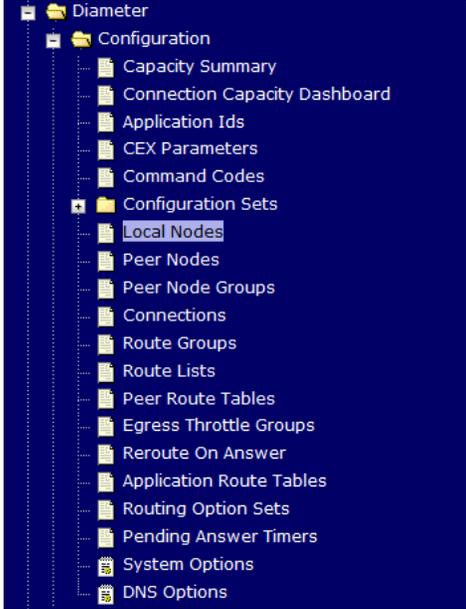
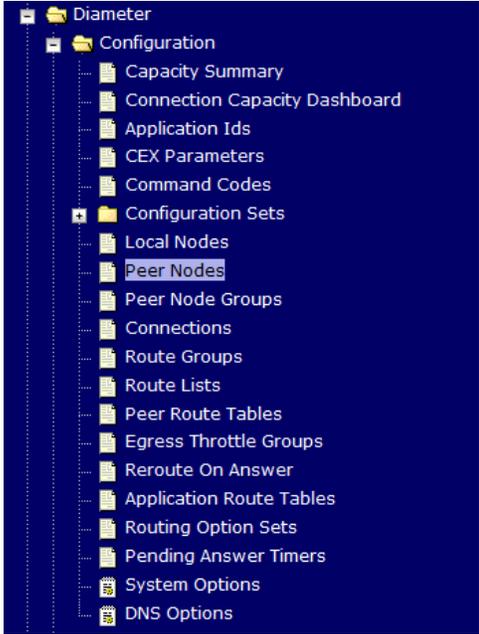
Procedure 2: Recovery Scenario 2

<p>38</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Verify Replication Between Servers.</p>	<p>Login to the Active NOAM via SSH terminal as root(5.0) or admusr(6.0+) user. Execute the following command:</p> <pre>\$ sudo irepstat -m</pre> <p>Output like below shall be generated:</p> <pre>-- 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 Oahu-SOAM-2 -- Active AB From Oahu-NOAM-2 Active 0 0.50 ^0.03%cpu 24B/s BB To Oahu-SOAM-1 Active 0 0.50 1%R 0.04%cpu 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</pre>
---	--	--

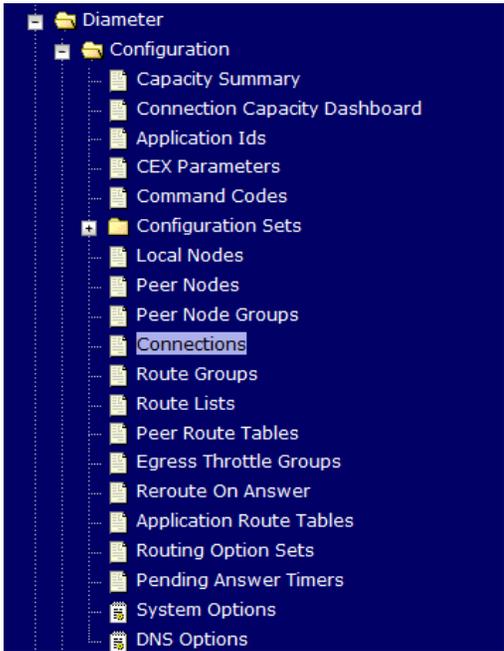
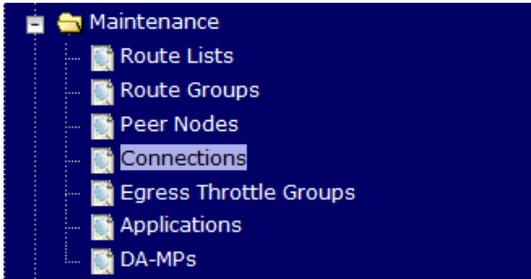
Procedure 2: Recovery Scenario 2

<p>39</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Verify the Database states</p>	<p>Click on Main Menu->Status and Manager->Database</p>  <p>Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below:</p> <table border="1" data-bbox="488 751 1438 957"> <thead> <tr> <th>Network Element</th> <th>Server</th> <th>Role</th> <th>OAM Max HA Role</th> <th>Application Max HA Role</th> <th>Status</th> <th>DB Level</th> <th>OAM Repl Status</th> <th>SIG Repl Status</th> <th>Repl Status</th> <th>Repl Audit Status</th> </tr> </thead> <tbody> <tr> <td>NO_10303</td> <td>NO2</td> <td>Network OAM&P</td> <td>Active</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutolnProg</td> </tr> <tr> <td>SO_10303</td> <td>PSBR</td> <td>MP</td> <td>Active</td> <td>Active</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>Normal</td> <td>Allowed</td> <td>AutolnProg</td> </tr> <tr> <td>SO_10303</td> <td>MP2</td> <td>MP</td> <td>Active</td> <td>Active</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>Normal</td> <td>Allowed</td> <td>AutolnProg</td> </tr> <tr> <td>SO_10303</td> <td>SO1</td> <td>System OAM</td> <td>Standby</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutolnProg</td> </tr> <tr> <td>NO_10303</td> <td>NO1</td> <td>Network OAM&P</td> <td>Standby</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutolnProg</td> </tr> <tr> <td>SO_10303</td> <td>IPFE</td> <td>MP</td> <td>Active</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>Normal</td> <td>Allowed</td> <td>AutolnProg</td> </tr> <tr> <td>SO_10303</td> <td>SO2</td> <td>System OAM</td> <td>Active</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutolnProg</td> </tr> </tbody> </table>	Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status	NO_10303	NO2	Network OAM&P	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg	SO_10303	PSBR	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutolnProg	SO_10303	MP2	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutolnProg	SO_10303	SO1	System OAM	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg	NO_10303	NO1	Network OAM&P	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg	SO_10303	IPFE	MP	Active	OOS	Normal	0	Normal	Normal	Allowed	AutolnProg	SO_10303	SO2	System OAM	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg
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	NO2	Network OAM&P	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg																																																																																
SO_10303	PSBR	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutolnProg																																																																																
SO_10303	MP2	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutolnProg																																																																																
SO_10303	SO1	System OAM	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg																																																																																
NO_10303	NO1	Network OAM&P	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg																																																																																
SO_10303	IPFE	MP	Active	OOS	Normal	0	Normal	Normal	Allowed	AutolnProg																																																																																
SO_10303	SO2	System OAM	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutolnProg																																																																																
<p>40</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Verify the HA Status</p>	<p>Click on Main Menu->Status and Manager->HA</p>  <p>Select the row for all of the servers Verify that the “HA Role” is either “Active” or “Standby”.</p> <table border="1" data-bbox="488 1482 1438 1656"> <thead> <tr> <th>Hostname</th> <th>OAM Max HA Role</th> <th>Application Max HA Role</th> <th>Max Allowed HA Role</th> <th>Mate Hostname List</th> <th>Network Element</th> <th>Server Role</th> <th>Active VIPs</th> </tr> </thead> <tbody> <tr> <td>NO2</td> <td>Active</td> <td>OOS</td> <td>Active</td> <td>NO1</td> <td>NO_10303</td> <td>Network OAM&P</td> <td>10.240.70.132</td> </tr> <tr> <td>SO1</td> <td>Standby</td> <td>OOS</td> <td>Active</td> <td>SO2</td> <td>SO_10303</td> <td>System OAM</td> <td></td> </tr> <tr> <td>SO2</td> <td>Active</td> <td>OOS</td> <td>Active</td> <td>SO1</td> <td>SO_10303</td> <td>System OAM</td> <td>10.240.70.133</td> </tr> <tr> <td>MP1</td> <td>Standby</td> <td>Active</td> <td>Active</td> <td>MP2</td> <td>SO_10303</td> <td>MP</td> <td></td> </tr> <tr> <td>MP2</td> <td>Active</td> <td>Active</td> <td>Active</td> <td>MP1</td> <td>SO_10303</td> <td>MP</td> <td></td> </tr> <tr> <td>IPFE</td> <td>Active</td> <td>OOS</td> <td>Active</td> <td></td> <td>SO_10303</td> <td>MP</td> <td></td> </tr> </tbody> </table>	Hostname	OAM Max HA Role	Application Max HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role	Active VIPs	NO2	Active	OOS	Active	NO1	NO_10303	Network OAM&P	10.240.70.132	SO1	Standby	OOS	Active	SO2	SO_10303	System OAM		SO2	Active	OOS	Active	SO1	SO_10303	System OAM	10.240.70.133	MP1	Standby	Active	Active	MP2	SO_10303	MP		MP2	Active	Active	Active	MP1	SO_10303	MP		IPFE	Active	OOS	Active		SO_10303	MP																																	
Hostname	OAM Max HA Role	Application Max HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role	Active VIPs																																																																																			
NO2	Active	OOS	Active	NO1	NO_10303	Network OAM&P	10.240.70.132																																																																																			
SO1	Standby	OOS	Active	SO2	SO_10303	System OAM																																																																																				
SO2	Active	OOS	Active	SO1	SO_10303	System OAM	10.240.70.133																																																																																			
MP1	Standby	Active	Active	MP2	SO_10303	MP																																																																																				
MP2	Active	Active	Active	MP1	SO_10303	MP																																																																																				
IPFE	Active	OOS	Active		SO_10303	MP																																																																																				

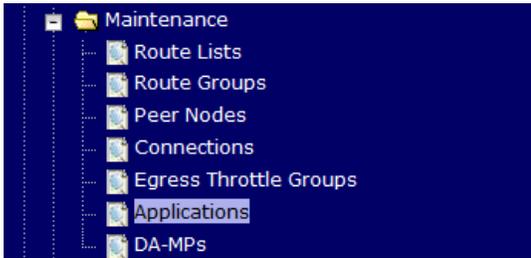
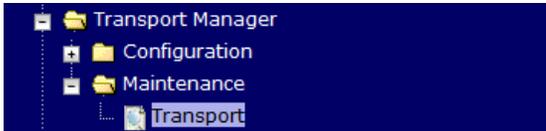
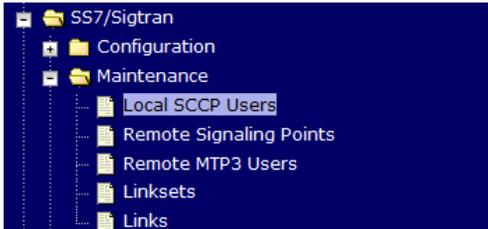
Procedure 2: Recovery Scenario 2

<p>41</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Verify the Local Node Info</p>	<p>Navigate to Main Menu->Diameter->Configuration->Local Node</p>  <p>Verify that all the local nodes are shown.</p>
<p>42</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Verify the Peer Node Info</p>	<p>Navigate to Main Menu->Diameter->Configuration->Peer Node</p>  <p>Verify that all the peer nodes are shown.</p>

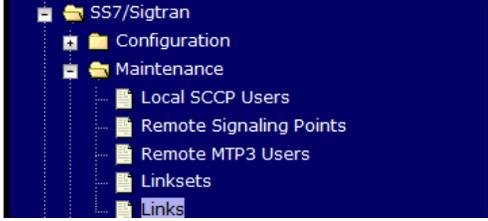
Procedure 2: Recovery Scenario 2

<p>43</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Verify the Connections Info</p>	<p>Navigate to Main Menu->Diameter->Configuration->Connections</p>  <p>Verify that all the connections are shown.</p>
<p>44</p> <p><input type="checkbox"/></p>	<p>MP Servers: Disable SCTP Auth Flag- DSR 7.1 Only</p>	<p>For DSR 7.1 Only: For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix in [17].</p> <p>Execute this procedure on all Failed MP Servers.</p>
<p>45</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Enable Connections if needed</p>	<p>Navigate to Main Menu->Diameter->Maintenance->Connections</p>  <p>Select each connection and click on the Enable button. Alternatively you can enable all the connections by selecting the EnableAll button.</p> <p> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="EnableAll"/> <input type="button" value="DisableAll"/> <input type="button" value="Diagnose Start"/> <input type="button" value="Diagnose End"/> <input type="button" value="SCTP STATISTICS"/> <input type="checkbox"/> Pause updates </p> <p>Verify that the Operational State is Available.</p>

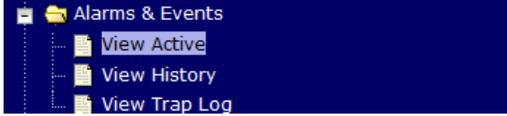
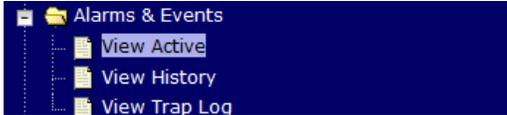
Procedure 2: Recovery Scenario 2

<p>46</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Enable Optional Features</p>	<p>Navigate to Main Menu -> Diameter -> Maintenance -> Applications</p>  <p>Select the optional feature application configured in step 29.</p> <p>Click the Enable button.</p> 
<p>47</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable Transports if Needed (Applicable ONLY for DSR 6.0+)</p>	<p>Navigate to Main Menu->Transport Manager -> Maintenance -> Transport</p>  <p>Select each transport and click on the Enable button</p>  <p>Verify that the Operational Status for each transport is Up.</p>
<p>48</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable MAPIWF application if needed (Applicable ONLY for DSR 6.0+)</p>	<p>Navigate to Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users</p>  <p>Click on the Enable button corresponding to MAPIWF Application Name.</p>  <p>Verify that the SSN Status is Enabled.</p>

Procedure 2: Recovery Scenario 2

<p>49</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable links if needed (Applicable ONLY for DSR 6.0+)</p>	<p>Navigate to Main Menu->SS7/Sigtran->Maintenance->Links</p>  <p>Click on Enable button for each link.</p>  <p>Verify that the Operational Status for each link is Up.</p>
<p>50</p> <p><input type="checkbox"/></p>	<p>Active NOAM: Verify Sync Split Scope Data (If POLICY AND CHARGING DRA is activated): 5.0/6.0 Only</p>	<p>If recovering a DSR 5.0/6.0 system and POLICY AND CHARGING DRA application is activated then execute this step.</p> <p>Note: If recovering a DSR 7.0+ system, DO NOT execute this step</p> <p>Login to the Active NOAM VIP via SSH terminal as root(5.0) or admusr(6.0+) user.</p> <p>Execute the following steps:</p> <p>Go to Appworks bin directory:</p> <pre>\$ sudo cd /usr/TKLC/appworks/bin/</pre> <p>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:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -reportonly</pre> <p>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.</p> <p>The “sync” option will modify the database:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -sync</pre> <p>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”:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -reportonly</pre>

Procedure 2: Recovery Scenario 2

<p>51 <input type="checkbox"/></p>	<p>SOAM VIP GUI: Examine All Alarms</p>	<p>Navigate to Main Menu->Alarms & Events->View Active</p>  <p>Examine all active alarms and refer to the on-line help on how to address them.</p> <p>If needed contact Appendix H. My Oracle Support (MOS).</p>
<p>52 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Examine All Alarms</p>	<p>Login to the NOAM VIP if not already logged in.</p> <p>Navigate to Main Menu->Alarms & Events->View Active</p>  <p>Examine all active alarms and refer to the on-line help on how to address them.</p> <p>If needed contact Appendix H. My Oracle Support (MOS).</p>
<p>53 <input type="checkbox"/></p>	<p>Backup and Archive All the Databases from the Recovered System</p>	<p>Execute Appendix A. DSR Database Backup to back up the Configuration databases:</p>

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.

Procedure 3: Recovery Scenario 3

S T E P #	<p>This procedure performs recovery if ALL NOAM servers are failed but 1 or more SOAM servers are intact. This includes any SOAM server that is in another location (spare SOAM server).</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Workarounds	Refer to Appendix G . Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
2 <input type="checkbox"/>	Gather Required Materials	Gather the documents and required materials listed in Section 3.1 Required Materials
3 <input type="checkbox"/>	RMS NOAM Failure	<p>If the failed server is a rack mount server based NOAM, execute this step; otherwise skip to the next step.</p> <ol style="list-style-type: none"> 1. HW vendor to replace the failed equipment 2. Execute the <i>"iLO Configuration Procedure"</i> 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. 5. 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. 6. If the failed NOAM is NOT co-hosted with the PMAC on the first rack mount server, execute <i>procedure "Configure TVOE on Additional RMS Servers(s)"</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.

Procedure 3: Recovery Scenario 3

<p>4 <input type="checkbox"/></p>	<p>HP-Class Blade Failure</p>	<p>If the failed server is an HP C-Class Blade, execute this step; otherwise skip to the next step.</p> <ol style="list-style-type: none"> 1. HW vendor to replace the failed equipment 1. Execute procedure “<i>Confirm/Update blade Server BIOS Settings</i>” – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 2. Execute procedure “<i>Configure Blade Server iLO Password for Administrator Account</i>” – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 3. Perform any needed firmware upgrades – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 4. 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.
<p>5 <input type="checkbox"/></p>	<p>Configure TVOE on Server Blades</p>	<p>For NOAMs on TVOE server Blades and SOAMs, execute procedure “<i>Configure TVOE on Server Blades</i>” - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.</p>
<p>6 <input type="checkbox"/></p>	<p>Create VMs</p>	<p>For NOAMs, execute procedure “<i>Create NOAM Guest VMs</i>” - Refer to Table 5 for the applicable DSR software installation and configuration reference.</p> <p>For SOAMs, execute procedure “<i>Create SOAM Guest VMs</i>” - Refer to Table 5 for the applicable DSR software installation and configuration reference.</p>
<p>7 <input type="checkbox"/></p>	<p>IPM Failed Guest/Servers</p>	<p>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.</p>
<p>8 <input type="checkbox"/></p>	<p>Install DSR application on Failed Guests/Servers</p>	<p>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.</p>
<p>9 <input type="checkbox"/></p>	<p>Repeat for Remaining Failed Servers</p>	<p>If necessary, repeat steps 1-7 for all remaining failed servers.</p>
<p>10 <input type="checkbox"/></p>	<p>Install NetBackup Client (Optional)</p>	<p>If NetBackup is used execute procedure “<i>Install NetBackup Client (Optional)</i>” - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.</p>

Procedure 3: Recovery Scenario 3

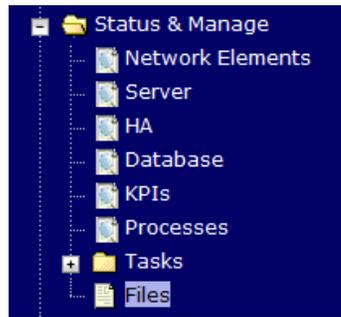
<p>11 <input type="checkbox"/></p>	<p>Obtain Latest Database Backup and Network Configuration Data.</p>	<p>Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources.</p> <p>From required materials list in Section 3.1 Required Materials; use site survey documents and Network Element report (if available), to determine network configuration data.</p>
<p>12 <input type="checkbox"/></p>	<p>Execute DSR Installation Procedure for the First NOAM</p>	<p>Verify the networking data for Network Elements</p> <p>Note: Use the backup copy of network configuration data and site surveys (Step 2)</p> <p>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.</p> <p>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</p>
<p>13 <input type="checkbox"/></p>	<p>NOAM GUI: Login</p>	<p>Login to the NOAM GUI as the <i>guiadmin</i> user:</p> 

Procedure 3: Recovery Scenario 3

14
□

NOAM GUI:
Upload the
Backed up
Database File

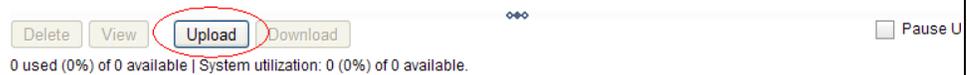
Browse to **Main Menu->Status & Manage->Files**



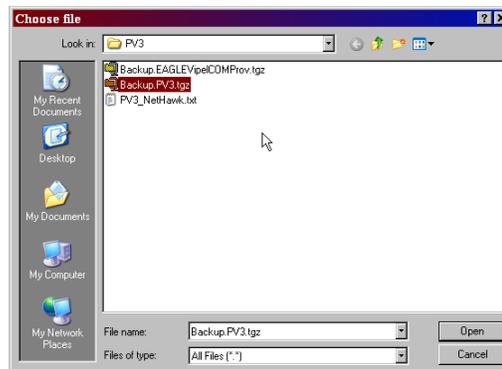
Select the Active NOAM server. The following screen will appear:

File Name	Size	Type	Timestamp
Backup.dsr.Cpa1-NO.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 *“NO Provisioning and Configuration:”* file backed up after initial installation and provisioning.



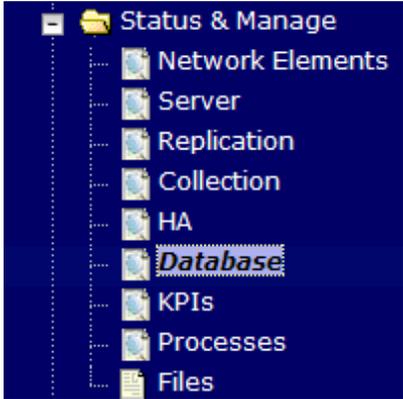
Click on **Browse** and locate the backup file and click on Open as shown below.



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.

Procedure 3: Recovery Scenario 3

15 <input type="checkbox"/>	NOAM GUI: Disable Provisioning	<p>Click on Main Menu->Status & Manage->Database</p>  <p>Disable Provisioning by clicking on Disable Provisioning button at the bottom of the screen as shown below.</p>  <p>A confirmation window will appear, press OK to disable Provisioning.</p>  <p>The message <i>"Warning Code 002"</i> will appear.</p>
--------------------------------	---	--

Procedure 3: Recovery Scenario 3

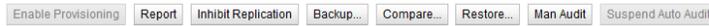
16



NOAM GUI:
Verify the Archive Contents and Database Compatibility

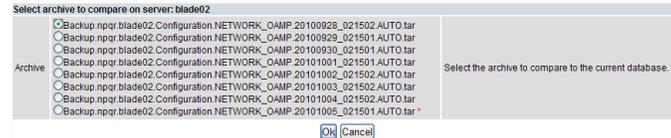
Click on **Main Menu->Status & Manage->Database**

Select the **Active NOAM** server and click on the **Compare**.



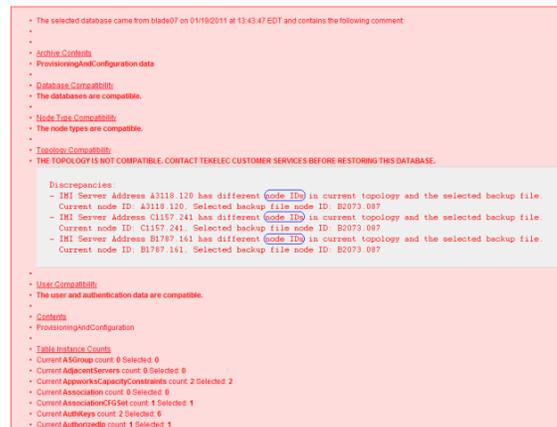
The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 13** of this procedure.

Database Compare



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)**



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:

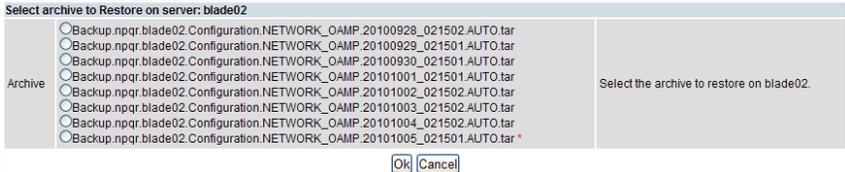
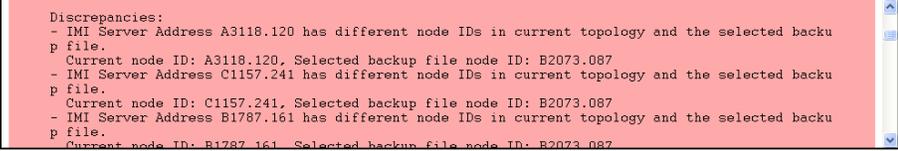
Topology Compatibility

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.

Procedure 3: Recovery Scenario 3

<p>17</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Restore the Database</p>	<p>Select the Active NOAM server, and click on Restore as shown below.</p> <p>The following screen will be displayed. Select the proper back up provisioning and configuration file.</p> <p>Database Restore</p>  <p>Click OK Button. The following confirmation screen will be displayed.</p> <p>If you get an error that the NodeIDs do not match. That is expected. If no other errors beside the NodeIDs are displayed, select the Force checkbox as shown above and Click OK to proceed with the DB restore.</p> <p>Database Restore Confirm</p> <p>Incompatible database selected</p>   <p>Note: After the restore has started, the user will be logged out of XMI NO GUI since the restored Topology is old data.</p>
---	---	---

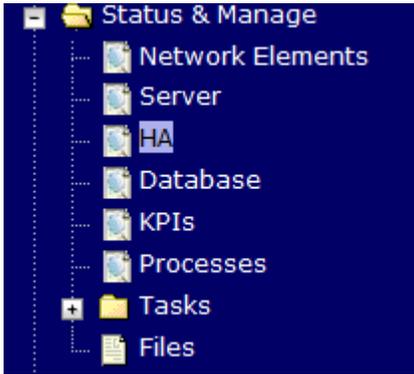
Procedure 3: Recovery Scenario 3

<p>18</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 10px auto;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the <i>guiadmin</i> user:</p> 
<p>19</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Monitor and Confirm database restoral</p>	<p>Wait for 5-10 minutes for the System to stabilize with the new topology:</p> <p>Monitor the Info tab for “Success”. This will indicate that the backup is complete and the system is stabilized.</p> <p>Following alarms must be ignored for NOAM and MP Servers until all the Servers are configured:</p> <p>Alarms with Type Column as “REPL”, “COLL”, “HA” (with mate NOAM), “DB” (about Provisioning Manually Disabled)</p> <p>Note: Do not pay attention to alarms until all the servers in the system are completely restored.</p> <p>Note: The Configuration and Maintenance information will be in the same state it was backed up during initial backup.</p>
<p>20</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Login</p>	<p>Login to the recovered Active NOAM via SSH terminal as root (5.0) or admusr(6.0+) user.</p>

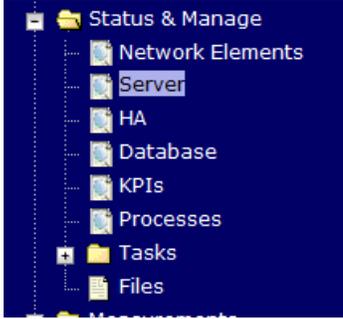
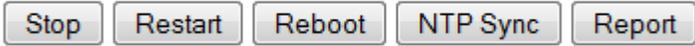
Procedure 3: Recovery Scenario 3

<p>21</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Restore /etc/hosts/ File of the Active NOAM (DSR 5.0/6.0/7.0 ONLY)</p>	<p>IF DSR 7.1, SKIP THIS STEP</p> <p>Execute the following command:</p> <pre>\$ sudo AppWorks AppWorks_AppWorks updateServerAliases <NOAM Host Name></pre>
<p>22</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Re-enable Provisioning</p>	<p>Navigate to Main Menu->Status & Manage->Database</p>  <p>Click on the Enable Provisioning. A pop-up window will appear to confirm as shown below, press OK.</p> 
<p>23</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover Standby NOAM</p>	<p>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.</p> <p>Note: Execute step 7 if Netbackup is used.</p> <p>If NetBackup is used, execute procedure “<i>Install NetBackup Client</i>” - Refer to Table 5 for the applicable DSR software installation and configuration reference.</p> <p>Note: If Topology or nodeld alarms are persistent after the database restore, refer to Appendix G. Workarounds for Issues not fixed in this Release</p>
<p>24</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover the Failed SOAM Servers</p>	<p>Recover the remaining SOAM servers (standby, spare) by repeating the following steps for each SOAM server:</p> <ol style="list-style-type: none"> 1. Install the remaining SOAM servers by executing reference Procedure “<i>Configure the SOAM Servers</i>”, 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. 2. If you are using Netbackup, execute procedure “<i>Install Netbackup Client</i>” - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.

Procedure 3: Recovery Scenario 3

<p>25</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Set HA on all C-Level Servers</p>	<p>Navigate to Status & Manage -> HA</p>  <p>Click on Edit at the bottom of the screen</p> <p>For each server whose Max Allowed HA Role is set to Standby, set it to Active</p> <p>Press OK</p>
<p>26</p> <p><input type="checkbox"/></p>	<p>Recovered Server: Login</p>	<p>Establish an SSH to the recovered server's XML address:</p>
<p>27</p> <p><input type="checkbox"/></p>	<p>Recovered Server: Sync NTP</p>	<p>1) Perform the following to retrieve the remote NTP server:</p> <pre data-bbox="488 1073 1419 1402"> \$ 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 </pre> <p>2) Stop ntpd service:</p> <pre data-bbox="488 1493 1419 1535"> \$ sudo service ntpd stop </pre> <p>3) Sync the date to the ntp remote server:</p> <pre data-bbox="488 1625 1419 1667"> \$ sudo ntpdate <NTP remote server> </pre> <p>Note: The remote server below will be that of the one gathered in sub step 1.</p> <p>4) Start the ntp service:</p> <pre data-bbox="488 1818 1419 1860"> \$ sudo service ntpd start </pre>

Procedure 3: Recovery Scenario 3

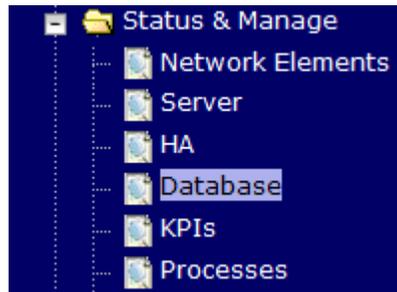
<p>28</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Restart DSR application</p>	<p>Navigate to Main Menu->Status & Manage->Server,</p>  <p>Select each recovered server and click on Restart.</p> 
<p>29</p> <p><input type="checkbox"/></p>	<p>Active SOAM: Prepare recovered SOAM for optional feature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

Procedure 3: Recovery Scenario 3

33

NOAM VIP GUI:
Fetch and Store
the database
Report for the
Newly Restored
Data and Save it

Navigate to **Main Menu -> Status & Manage -> Database**



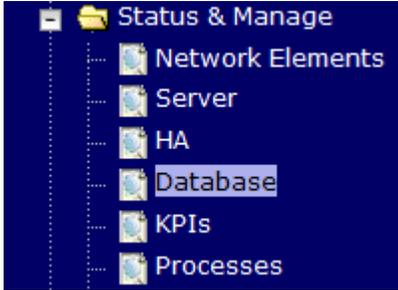
Select the **active** NOAM server and click on the **Report** button at the bottom of the page. The following screen is displayed:

Main Menu: Status & Manage -> Database [Report]

```
-----  
d s r   D a t a b a s e   S t a t u s   R e p o r t  
-----  
Report Generated: Wed Aug 19 16:49:08 2015 EDT  
From: Network OAMsP on host Oahu-NOAM-2  
Report Version: 7.1.0.0.0-71.19.0  
User: guladmin  
-----  
  
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  
-----  
Alarms  
-----  
None  
-----  
Maintenance in Progress  
-----  
Backup operation success  
-----  
Replication Audit Status  
-----  
Not found  
-----  
Service Information  
-----  
-----  
End of d s r   D a t a b a s e   S t a t u s   R e p o r t  
-----
```

Click on **Save** and save the report to your local machine.

Procedure 3: Recovery Scenario 3

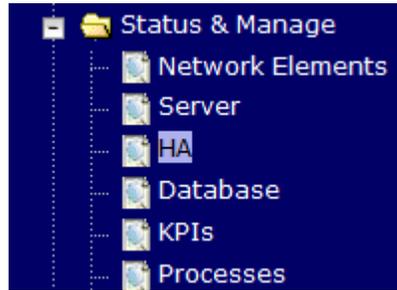
<p>34</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Verify Replication Between Servers.</p>	<p>Login to the Active NOAM via SSH terminal as root(5.0) or admusr(6.0+) user. Execute the following command:</p> <pre>\$ sudo irepstat -m</pre> <p>Output like below shall be generated:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- ----- RDU06-MP1 -- Stby BC From RDU06-S01 Active 0 0.50 ^0.17%cpu 42B/s A=none CC From RDU06-MP2 Active 0 0.10 ^0.17 0.88%cpu 32B/s A=none RDU06-MP2 -- Active BC From RDU06-S01 Active 0 0.50 ^0.10%cpu 33B/s A=none CC To RDU06-MP1 Active 0 0.10 0.08%cpu 20B/s A=none RDU06-N01 -- Active AB To RDU06-S01 Active 0 0.50 1%R 0.03%cpu 21B/s RDU06-S01 -- Active AB From RDU06-N01 Active 0 0.50 ^0.04%cpu 24B/s BC To RDU06-MP1 Active 0 0.50 1%R 0.04%cpu 21B/s BC To RDU06-MP2 Active 0 0.50 1%R 0.07%cpu 21B/s</pre>																																																																																								
<p>35</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Verify the Database states</p>	<p>Click on Main Menu->Status and Manager->Database</p>  <p>Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below:</p> <table border="1" data-bbox="488 1478 1433 1682"> <thead> <tr> <th>Network Element</th> <th>Server</th> <th>Role</th> <th>OAM Max HA Role</th> <th>Application Max HA Role</th> <th>Status</th> <th>DB Level</th> <th>OAM Repl Status</th> <th>SIG Repl Status</th> <th>Repl Status</th> <th>Repl Audit Status</th> </tr> </thead> <tbody> <tr> <td>NO_10303</td> <td>NO2</td> <td>Network OAM&P</td> <td>Active</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutoInProg</td> </tr> <tr> <td>SO_10303</td> <td>PSBR</td> <td>MP</td> <td>Active</td> <td>Active</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>Normal</td> <td>Allowed</td> <td>AutoInProg</td> </tr> <tr> <td>SO_10303</td> <td>MP2</td> <td>MP</td> <td>Active</td> <td>Active</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>Normal</td> <td>Allowed</td> <td>AutoInProg</td> </tr> <tr> <td>SO_10303</td> <td>S01</td> <td>System OAM</td> <td>Standby</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutoInProg</td> </tr> <tr> <td>NO_10303</td> <td>NO1</td> <td>Network OAM&P</td> <td>Standby</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutoInProg</td> </tr> <tr> <td>SO_10303</td> <td>JPFE</td> <td>MP</td> <td>Active</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>Normal</td> <td>Allowed</td> <td>AutoInProg</td> </tr> <tr> <td>SO_10303</td> <td>S02</td> <td>System OAM</td> <td>Active</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutoInProg</td> </tr> </tbody> </table>	Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status	NO_10303	NO2	Network OAM&P	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg	SO_10303	PSBR	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg	SO_10303	MP2	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg	SO_10303	S01	System OAM	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg	NO_10303	NO1	Network OAM&P	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg	SO_10303	JPFE	MP	Active	OOS	Normal	0	Normal	Normal	Allowed	AutoInProg	SO_10303	S02	System OAM	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg
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	NO2	Network OAM&P	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg																																																																																
SO_10303	PSBR	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg																																																																																
SO_10303	MP2	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg																																																																																
SO_10303	S01	System OAM	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg																																																																																
NO_10303	NO1	Network OAM&P	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg																																																																																
SO_10303	JPFE	MP	Active	OOS	Normal	0	Normal	Normal	Allowed	AutoInProg																																																																																
SO_10303	S02	System OAM	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg																																																																																

Procedure 3: Recovery Scenario 3

36

NOAM VIP GUI:
Verify the HA
Status

Click on **Main Menu->Status and Manage->HA**



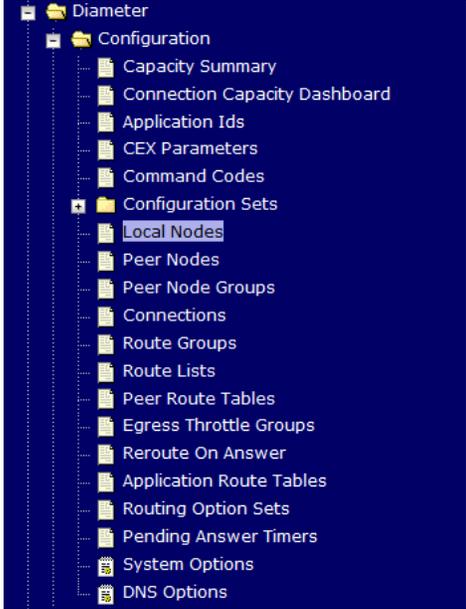
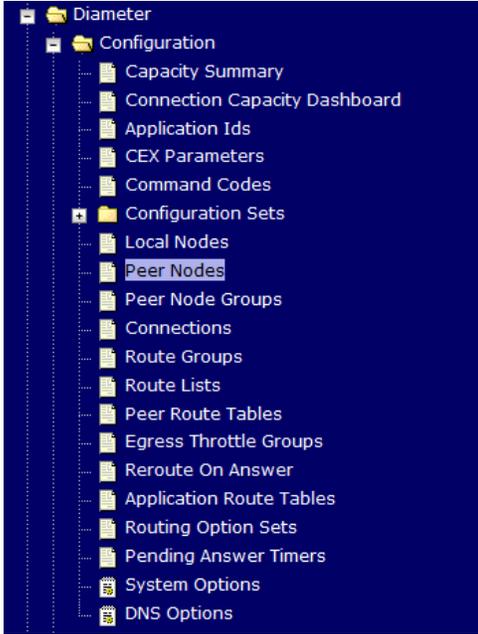
Select the row for all of the servers
Verify that the “HA Role” is either “Active” or “Standby”.

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

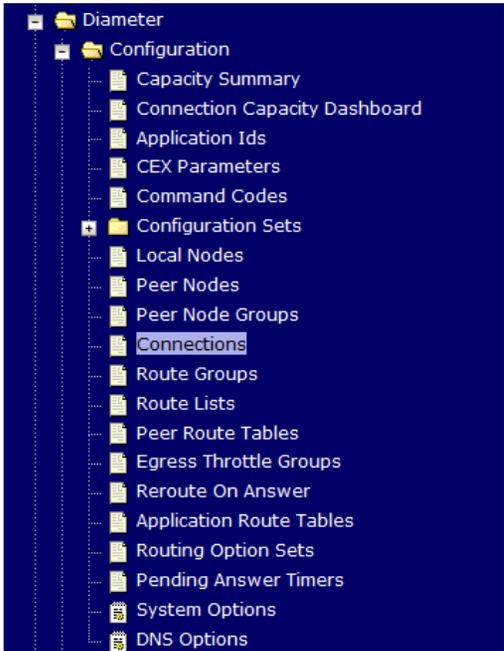
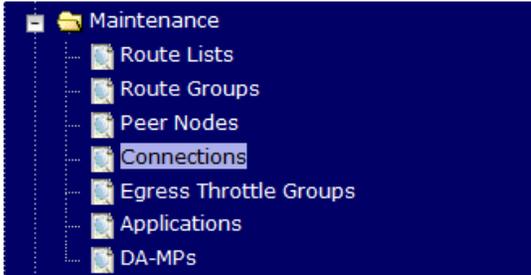
Procedure 3: Recovery Scenario 3

37 <input type="checkbox"/>	Active NOAM: Verify Sync Split Scope Data (If POLICY AND CHARGING DRA is activated): 5.0/6.0 Only	<p>If recovering a DSR 5.0/6.0 system and POLICY AND CHARGING DRA application is activated then execute this step.</p> <p>Note: If recovering a DSR 7.0+ system, DO NOT execute this step</p> <p>Login to the Active NOAM VIP via SSH terminal as root(5.0) or admusr(6.0+) user.</p> <p>Execute the following steps:</p> <p>Go to Appworks bin directory:</p> <pre>\$ sudo cd /usr/TKLC/appworks/bin/</pre> <p>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:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -reportonly</pre> <p>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.</p> <p>The “sync” option will modify the database:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -sync</pre> <p>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”:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -reportonly</pre>
--------------------------------	--	---

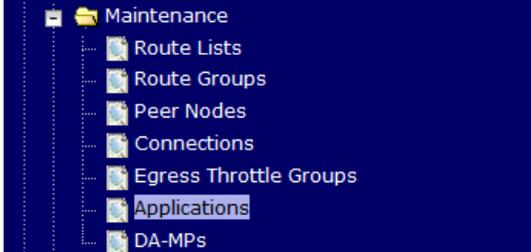
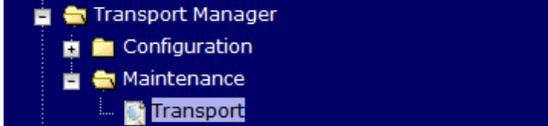
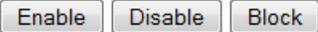
Procedure 3: Recovery Scenario 3

<p>38</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Verify the Local Node Info</p>	<p>Navigate to Main Menu->Diameter->Configuration->Local Node</p>  <p>Verify that all the local nodes are shown.</p>
<p>39</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Verify the Peer Node Info</p>	<p>Navigate to Main Menu->Diameter->Configuration->Peer Node</p>  <p>Verify that all the peer nodes are shown.</p>

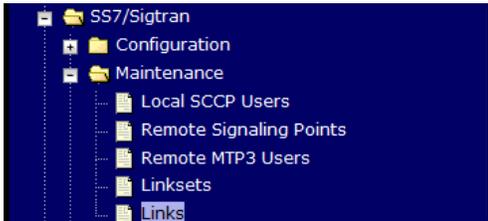
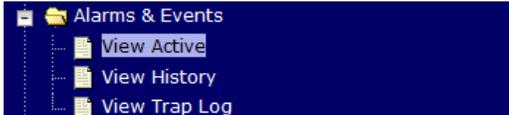
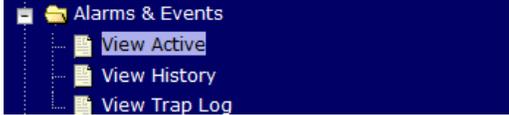
Procedure 3: Recovery Scenario 3

<p>40</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Verify the Connections Info</p>	<p>Navigate to Main Menu->Diameter->Configuration->Connections</p>  <p>Verify that all the connections are shown.</p>
<p>41</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Enable Connections if needed</p>	<p>Navigate to Main Menu->Diameter->Maintenance->Connections</p>  <p>Select each connection and click on the Enable button. Alternatively you can enable all the connections by selecting the EnableAll button.</p>  <p>Verify that the Operational State is Available.</p>

Procedure 3: Recovery Scenario 3

<p>42</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Enable Optional Features</p>	<p>Navigate to Main Menu -> Diameter -> Maintenance -> Applications</p>  <p>Select the optional feature application configured in step 31.</p> <p>Click the Enable button.</p> 
<p>43</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable Transports if Needed (Applicable ONLY for DSR 6.0+)</p>	<p>Navigate to Main Menu->Transport Manager -> Maintenance -> Transport</p>  <p>Select each transport and click on the Enable button</p>  <p>Verify that the Operational Status for each transport is Up.</p>
<p>44</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable MAPIWF application if needed (Applicable ONLY for DSR 6.0+)</p>	<p>Navigate to Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users</p>  <p>Click on the Enable button corresponding to MAPIWF Application Name.</p>  <p>Verify that the SSN Status is Enabled.</p>

Procedure 3: Recovery Scenario 3

<p>45</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable links if needed (Applicable ONLY for DSR 6.0+)</p>	<p>Navigate to Main Menu->SS7/Sigtran->Maintenance->Links</p>  <p>Click on Enable button for each link.</p>  <p>Verify that the Operational Status for each link is Up.</p>
<p>46</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Examine All Alarms</p>	<p>Navigate to Main Menu->Alarms & Events->View Active</p>  <p>Examine all active alarms and refer to the on-line help on how to address them.</p> <p>If needed contact Appendix H. My Oracle Support (MOS).</p>
<p>47</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Examine All Alarms</p>	<p>Login to the NOAM VIP if not already logged in.</p> <p>Navigate to Main Menu->Alarms & Events->View Active</p>  <p>Examine all active alarms and refer to the on-line help on how to address them.</p> <p>If needed contact Appendix H. My Oracle Support (MOS).</p>
<p>48</p> <p><input type="checkbox"/></p>	<p>Restore GUI Usernames and Passwords</p>	<p>If applicable, Execute steps in Section 6.0 to recover the user and group information restored.</p>
<p>49</p> <p><input type="checkbox"/></p>	<p>Backup and Archive All the Databases from the Recovered System</p>	<p>Execute Appendix A. DSR Database Backup to back up the Configuration databases:</p>

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.

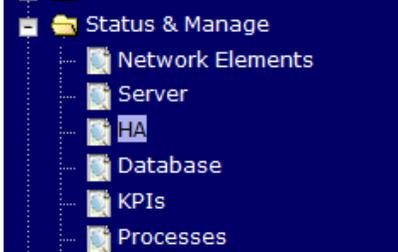
The database is intact at the active NOAM server and does not require restoration at the SO and MP servers.

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

Procedure 4: Recovery Scenario 4

<p>S T E P #</p>	<p>This procedure performs recovery if at least 1 NOAM server is intact and available and 1 SOAM server is intact and available.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>Workarounds</p>	<p>Refer to Appendix G. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.</p>
<p>2 <input type="checkbox"/></p>	<p>Gather Required Materials</p>	<p>Gather the documents and required materials listed in Section 3.1 Required Materials</p>
<p>3 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>http://<Primary_NOAM_VIP_IP_Address></p> </div> <p>Login as the <i>guiadmin</i> user:</p> <div style="text-align: center; margin: 20px 0;">  </div> <div style="text-align: center; margin: 10px 0;"> <p>Oracle System Login Fri Mar 20 12:29:52 2015 EDT</p> <hr style="width: 50%; margin: 0 auto;"/> </div> <div style="text-align: center; margin: 20px 0;"> <div style="border: 1px solid gray; padding: 10px; width: fit-content; margin: 0 auto;"> <p>Log In Enter your username and password to log in</p> <p>Username: <input type="text" value="guiadmin"/></p> <p>Password: <input type="password" value="••••••"/></p> <p><input type="checkbox"/> Change password</p> <p><input type="button" value="Log In"/></p> </div> </div> <p style="text-align: center; font-size: small;">Welcome to the Oracle System Login.</p> <p style="text-align: center; font-size: x-small;">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.</p> <hr style="width: 50%; margin: 0 auto;"/> <p style="text-align: center; font-size: x-small;">Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</p>

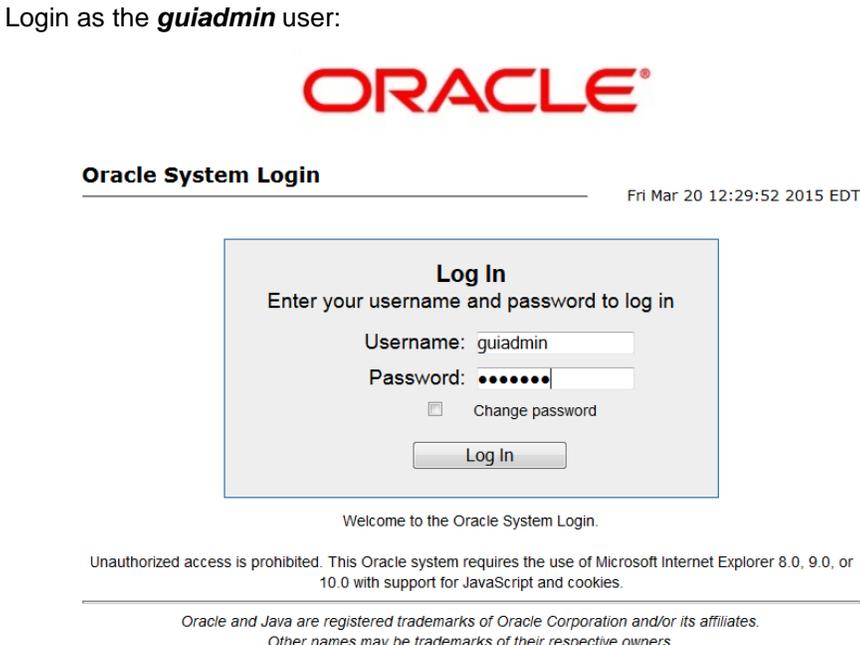
Procedure 4: Recovery Scenario 4

<p>4</p> <p><input type="checkbox"/></p>	<p>Active NOAM: Set Failed Servers to Standby</p>	<p>Navigate to Main Menu -> Status & Manage -> HA</p>  <p>Select Edit</p> <p>Set the Max Allowed HA Role drop down box to Standby for the failed servers.</p> <p>Select Ok</p> 
<p>5</p> <p><input type="checkbox"/></p>	<p>RMS NOAM Failure</p>	<ol style="list-style-type: none"> 1. HW vendor to replace the failed equipment 2. Execute the <i>“iLO Configuration Procedure”</i> 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. 5. 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. 6. If the failed NOAM is NOT co-hosted with the PMAC on the first rack mount server, execute <i>procedure “Configure TVOE on Additional RMS Servers(s)”</i> - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.

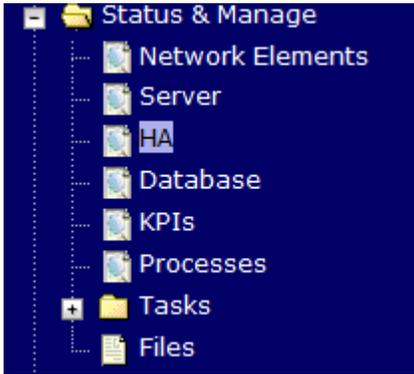
Procedure 4: Recovery Scenario 4

<p>6 <input type="checkbox"/></p>	<p>HP-Class Blade Failure</p>	<p>If the failed server is an HP C-Class Blade, execute this step; otherwise skip to the next step.</p> <ol style="list-style-type: none"> 1. HW vendor to replace the failed equipment 2. Execute procedure “<i>Confirm/Update blade Server BIOS Settings</i>” – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 3. Execute procedure “<i>Configure Blade Server iLO Password for Administrator Account</i>” – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference. 4. Perform any needed firmware upgrades – Refer to Table 4: DSR Base Hardware Installation Reference Table for the applicable DSR base hardware installation reference 5. For NOAM/SOAM TVOE Host 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.
<p>7 <input type="checkbox"/></p>	<p>Configure TVOE on Server Blades</p>	<p>For NOAMs on TVOE server Blades and SOAMs, execute procedure “<i>Configure TVOE on Server Blades</i>” - Refer to Table 5 for the applicable DSR software installation/configuration guide reference.</p>
<p>8 <input type="checkbox"/></p>	<p>Create VMs</p>	<p>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.</p> <p>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.</p>
<p>9 <input type="checkbox"/></p>	<p>IPM Failed Guest/Servers</p>	<p>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.</p>
<p>10 <input type="checkbox"/></p>	<p>Install DSR application on Failed Guests/Servers</p>	<p>Install the DSR application on the failed guests/server by executing procedure “<i>Install Application Software on Blades</i>” - Refer to Table 5: DSR Software Installation/Configuration Reference Table for the applicable DSR software installation/configuration guide reference.</p>
<p>11 <input type="checkbox"/></p>	<p>Repeat for Remaining Failed Servers</p>	<p>If necessary, repeat steps 1-7 for all remaining failed servers.</p>

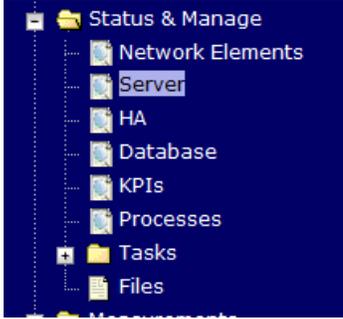
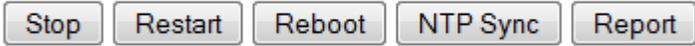
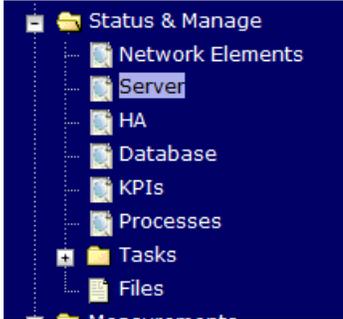
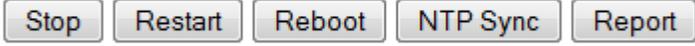
Procedure 4: Recovery Scenario 4

<p>12 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 10px auto;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the <i>guiadmin</i> user:</p> 
<p>13 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover Standby NOAM if needed</p>	<p>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.</p> <p>Note: Execute step 7 if Netbackup is used.</p> <p>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 guide reference.</p>
<p>14 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover the Failed SOAM Servers if needed</p>	<p>If the failed server is an SOAM, recover the remaining SOAM servers (standby, spare) by repeating the following steps for each SOAM server:</p> <ol style="list-style-type: none"> 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 DSR software installation/configuration guide reference.

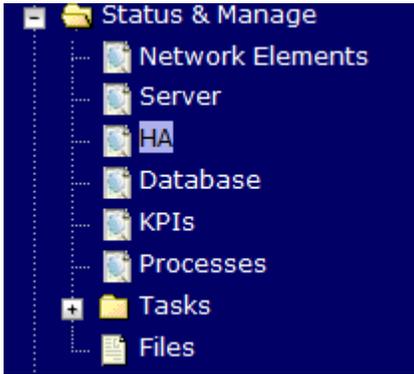
Procedure 4: Recovery Scenario 4

<p>15</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Set HA on Recovered Servers</p>	<p>Navigate to Status & Manage -> HA</p>  <p>Click on Edit at the bottom of the screen</p> <p>For each server whose Max Allowed HA Role is set to Standby, set it to Active</p> <p>Press OK</p>
<p>16</p> <p><input type="checkbox"/></p>	<p>Recovered Server: Login</p>	<p>Establish an SSH to the recovered server's XML address:</p>
<p>17</p> <p><input type="checkbox"/></p>	<p>Recovered Server: Sync NTP</p>	<p>1) Perform the following to retrieve the remote NTP server:</p> <pre data-bbox="488 1073 1419 1402"> \$ 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 </pre> <p>2) Stop ntpd service:</p> <pre data-bbox="488 1493 1419 1535"> \$ sudo service ntpd stop </pre> <p>3) Sync the date to the ntp remote server:</p> <pre data-bbox="488 1625 1419 1667"> \$ sudo ntpdate <NTP remote server> </pre> <p>Note: The remote server below will be that of the one gathered in sub step 1.</p> <p>4) Start the ntp service:</p> <pre data-bbox="488 1818 1419 1860"> \$ sudo service ntpd start </pre>

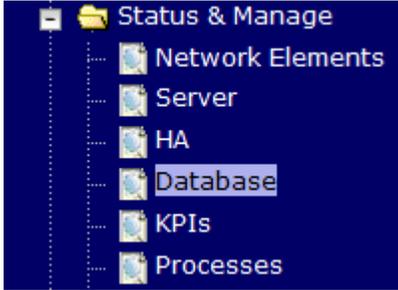
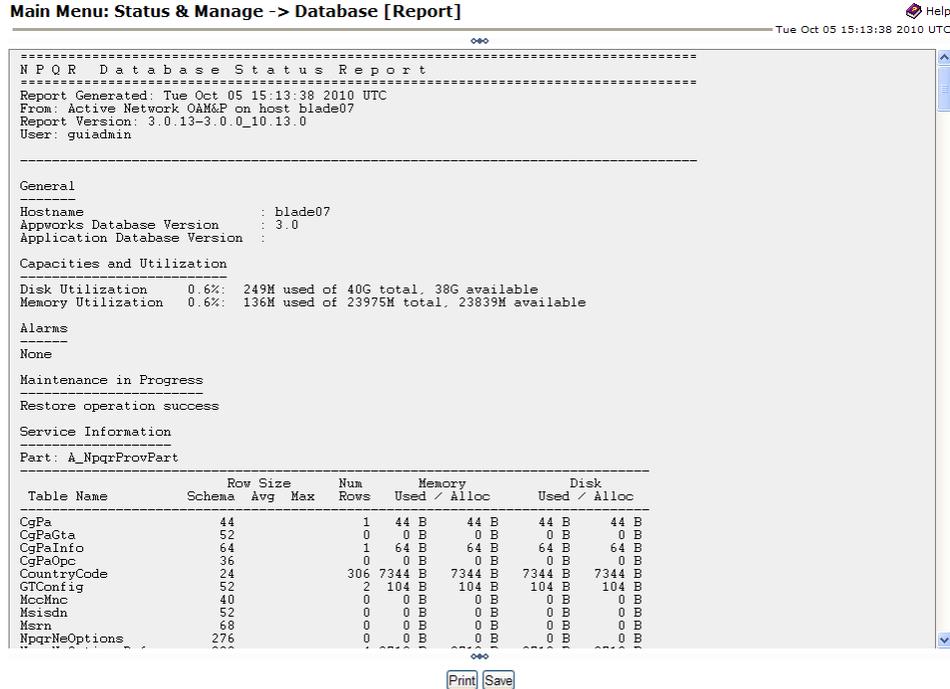
Procedure 4: Recovery Scenario 4

<p>18 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Restart DSR application</p>	<p>Navigate to Main Menu->Status & Manage->Server,</p>  <p>Select the recovered server and click on Restart.</p> 
<p>19 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover the C-Level Server (DA-MP, SBRs, IPFE, SS7-MP)</p>	<p>Execute procedure “<i>Configure MP Blades Servers</i>”, 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.</p> <p>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.</p> <p>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.</p> <p>Repeat this step for any remaining failed MP servers.</p>
<p>20 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Restart DSR Application on recovered C-Level Servers.</p>	<p>Navigate to Main Menu->Status & Manage->Server</p>  <p>Select the recovered servers and click on Restart.</p> 

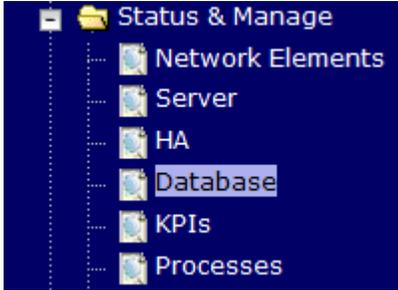
Procedure 4: Recovery Scenario 4

<p>21</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Set HA on all C-Level Servers</p>	<p>Navigate to Status & Manage -> HA</p>  <p>Click on Edit at the bottom of the screen</p> <p>For each server whose Max Allowed HA Role is set to Standby, set it to Active</p> <p>Press OK</p>
<p>22</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Login</p>	<p>Login to the recovered Active NOAM via SSH terminal as root (5.0) or admusr(6.0+) user.</p>
<p>23</p> <p><input type="checkbox"/></p>	<p>Active SOAM: Prepare recovered SOAM for optional feature activation (DSR 5.0/6.0/7.0)</p>	<p>For DSR 5.0/6.0/7.0: If DSR 7.1, skip this step</p> <p>Establish an SSH session to the Active SOAM, login as admusr.</p> <p>Execute the following command:</p> <pre style="border: 1px solid black; padding: 5px;">\$ irem DsrApplication where "name in ('RBAR', 'FABR', 'PCA', 'MD-IWF', 'DM-IWF', 'CPA', 'GLA')"</pre>
<p>24</p> <p><input type="checkbox"/></p>	<p>Active SOAM: Verify Preparation (DSR 5.0/6.0/7.0)</p>	<p>For DSR 5.0/6.0/7.0: If DSR 7.1, skip this step.</p> <p>Execute the following command to verify preparation of optional feature activation:</p> <pre style="border: 1px solid black; padding: 5px;">\$ iqt -z -h -p -fname DsrApplication where "name in ('RBAR', 'FABR', 'PCA', 'MD-IWF', 'DM-IWF', 'CPA', 'GLA')"</pre> <p>Note: There should be no output of this command, if there is, verify the correct entry of the command in step 22.</p>
<p>25</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Perform key exchange between the active-NOAM and recovered servers.</p>	<p>Establish an SSH session to the Active NOAM, login as admusr.</p> <p>Execute the following command to perform a keyexchange from the active NOAM to each recovered server:</p> <pre style="border: 1px solid black; padding: 5px;">\$ keyexchange admusr@<Recovered Server Hostname></pre>

Procedure 4: Recovery Scenario 4

<p>26</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Activate Optional Features</p>	<p>Establish an SSH session to the active NOAM, login as admusr.</p> <p>Refer to section 1.5 Optional Features to activate any features that were previously activated.</p>
<p>27</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Fetch and Store the database Report for the Newly Restored Data and Save it</p>	<p>Navigate to Configuration-> Server -> Database</p>  <p>Select the active NOAM server and click on the Report button at the bottom of the page. The following screen is displayed:</p>  <p>Click on Save and save the report to your local machine.</p>

Procedure 4: Recovery Scenario 4

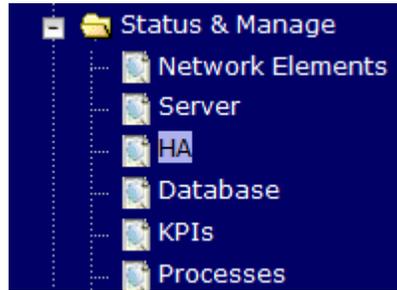
<p>28</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Verify Replication Between Servers.</p>	<p>Login to the Active NOAM via SSH terminal as root(5.0) or admusr(6.0+) user. Execute the following command:</p> <pre style="background-color: #f0f0f0; padding: 10px;">\$ sudo irepstat -m</pre> <p>Output like below shall be generated:</p> <pre style="background-color: #f0f0f0; padding: 10px;">-- Policy 0 ActStb [DbReplication] ----- ----- RDU06-MP1 -- Stby BC From RDU06-S01 Active 0 0.50 ^0.17%cpu 42B/s A=none CC From RDU06-MP2 Active 0 0.10 ^0.17 0.88%cpu 32B/s A=none RDU06-MP2 -- Active BC From RDU06-S01 Active 0 0.50 ^0.10%cpu 33B/s A=none CC To RDU06-MP1 Active 0 0.10 0.08%cpu 20B/s A=none RDU06-N01 -- Active AB To RDU06-S01 Active 0 0.50 1%R 0.03%cpu 21B/s RDU06-S01 -- Active AB From RDU06-N01 Active 0 0.50 ^0.04%cpu 24B/s BC To RDU06-MP1 Active 0 0.50 1%R 0.04%cpu 21B/s BC To RDU06-MP2 Active 0 0.50 1%R 0.07%cpu 21B/s</pre>																																																																																								
<p>29</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Verify the Database states</p>	<p>Click on Main Menu->Status and Manager->Database</p>  <p>Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below:</p> <table border="1" data-bbox="488 1478 1433 1682"> <thead> <tr> <th>Network Element</th> <th>Server</th> <th>Role</th> <th>OAM Max HA Role</th> <th>Application Max HA Role</th> <th>Status</th> <th>DB Level</th> <th>OAM Repl Status</th> <th>SIG Repl Status</th> <th>Repl Status</th> <th>Repl Audit Status</th> </tr> </thead> <tbody> <tr> <td>NO_10303</td> <td>NO2</td> <td>Network OAM&P</td> <td>Active</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutoInProg</td> </tr> <tr> <td>SO_10303</td> <td>PSBR</td> <td>MP</td> <td>Active</td> <td>Active</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>Normal</td> <td>Allowed</td> <td>AutoInProg</td> </tr> <tr> <td>SO_10303</td> <td>MP2</td> <td>MP</td> <td>Active</td> <td>Active</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>Normal</td> <td>Allowed</td> <td>AutoInProg</td> </tr> <tr> <td>SO_10303</td> <td>S01</td> <td>System OAM</td> <td>Standby</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutoInProg</td> </tr> <tr> <td>NO_10303</td> <td>NO1</td> <td>Network OAM&P</td> <td>Standby</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutoInProg</td> </tr> <tr> <td>SO_10303</td> <td>JPFE</td> <td>MP</td> <td>Active</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>Normal</td> <td>Allowed</td> <td>AutoInProg</td> </tr> <tr> <td>SO_10303</td> <td>S02</td> <td>System OAM</td> <td>Active</td> <td>OOS</td> <td>Normal</td> <td>0</td> <td>Normal</td> <td>NotApplicabl</td> <td>Allowed</td> <td>AutoInProg</td> </tr> </tbody> </table>	Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status	NO_10303	NO2	Network OAM&P	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg	SO_10303	PSBR	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg	SO_10303	MP2	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg	SO_10303	S01	System OAM	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg	NO_10303	NO1	Network OAM&P	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg	SO_10303	JPFE	MP	Active	OOS	Normal	0	Normal	Normal	Allowed	AutoInProg	SO_10303	S02	System OAM	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg
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	NO2	Network OAM&P	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg																																																																																
SO_10303	PSBR	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg																																																																																
SO_10303	MP2	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg																																																																																
SO_10303	S01	System OAM	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg																																																																																
NO_10303	NO1	Network OAM&P	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg																																																																																
SO_10303	JPFE	MP	Active	OOS	Normal	0	Normal	Normal	Allowed	AutoInProg																																																																																
SO_10303	S02	System OAM	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg																																																																																

Procedure 4: Recovery Scenario 4

30

NOAM VIP GUI:
Verify the HA
Status

Click on **Main Menu->Status and Manage->HA**



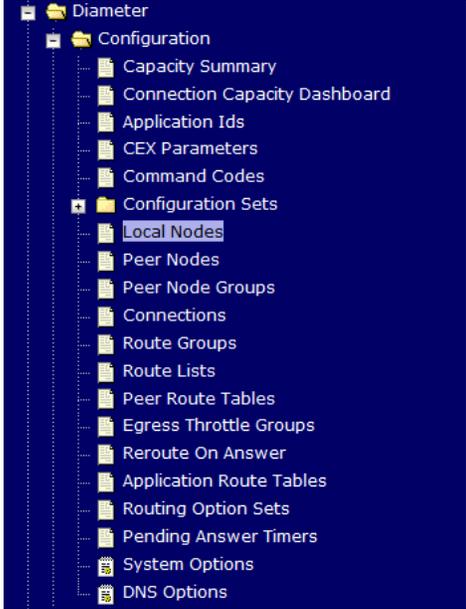
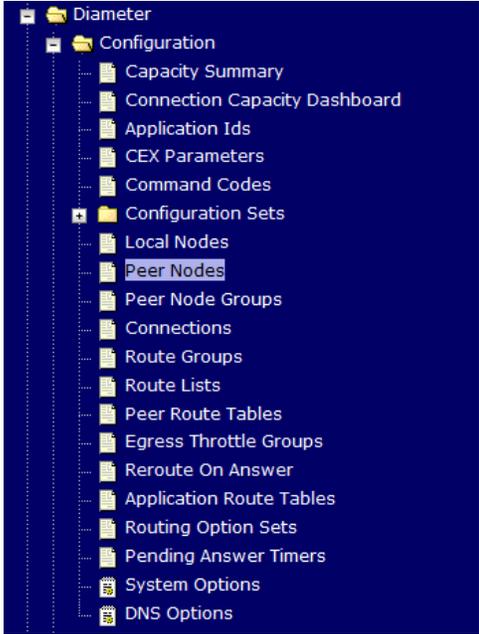
Select the row for all of the servers
Verify that the “HA Role” is either “Active” or “Standby”.

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

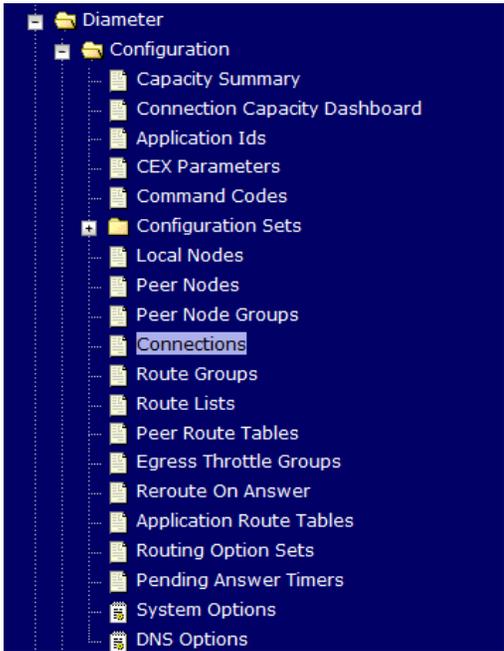
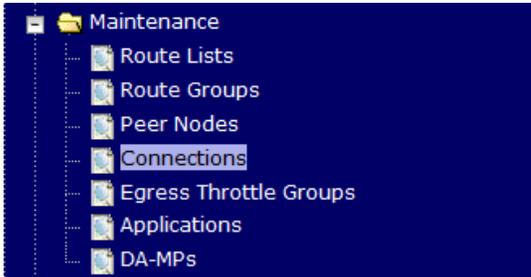
Procedure 4: Recovery Scenario 4

31 <input type="checkbox"/>	Active NOAM: Verify Sync Split Scope Data (If POLICY AND CHARGING DRA is activated): 5.0/6.0 Only	<p>If recovering a DSR 5.0/6.0 system and POLICY AND CHARGING DRA application is activated then execute this step.</p> <p>Note: If recovering a DSR 7.0+ system, DO NOT execute this step</p> <p>Login to the Active NOAM VIP via SSH terminal as root(5.0) or admusr(6.0+) user.</p> <p>Execute the following steps:</p> <p>Go to Appworks bin directory:</p> <pre>\$ sudo cd /usr/TKLC/appworks/bin/</pre> <p>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:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -reportonly</pre> <p>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.</p> <p>The “sync” option will modify the database:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -sync</pre> <p>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”:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -reportonly</pre>
--------------------------------	--	---

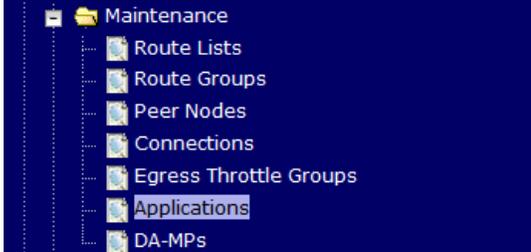
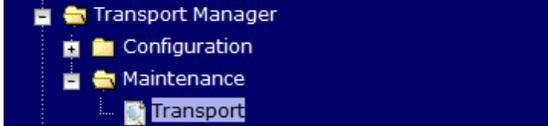
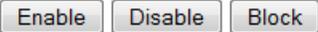
Procedure 4: Recovery Scenario 4

<p>32</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Verify the Local Node Info</p>	<p>Navigate to Main Menu->Diameter->Configuration->Local Node</p>  <p>Verify that all the local nodes are shown.</p>
<p>33</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Verify the Peer Node Info</p>	<p>Navigate to Main Menu->Diameter->Configuration->Peer Node</p>  <p>Verify that all the peer nodes are shown.</p>

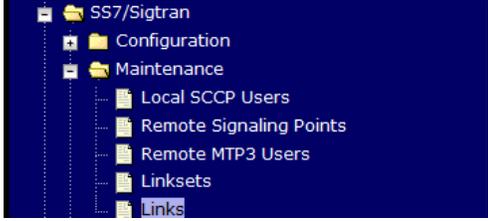
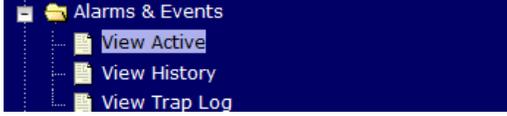
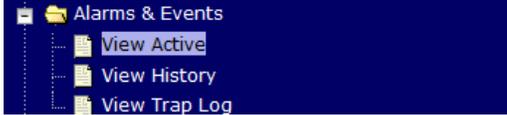
Procedure 4: Recovery Scenario 4

<p>34</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Verify the Connections Info</p>	<p>Navigate to Main Menu->Diameter->Configuration->Connections</p>  <p>Verify that all the connections are shown.</p>
<p>35</p> <p><input type="checkbox"/></p>	<p>MP Servers: Disable SCTP Auth Flag- DSR 7.1 Only</p>	<p>For DSR 7.1 Only: For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix in [17].</p> <p>Execute this procedure on all Failed MP Servers.</p>
<p>36</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Enable Connections if needed</p>	<p>Navigate to Main Menu->Diameter->Maintenance->Connections</p>  <p>Select each connection and click on the Enable button.</p> <p>Alternatively you can enable all the connections by selecting the EnableAll button.</p>  <p>Verify that the Operational State is Available.</p>

Procedure 4: Recovery Scenario 4

<p>37</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Enable Optional Features</p>	<p>Navigate to Main Menu -> Diameter -> Maintenance -> Applications</p>  <p>Select the optional feature application configured in step 22.</p> <p>Click the Enable button.</p> 
<p>38</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable Transports if Needed (Applicable ONLY for DSR 6.0+)</p>	<p>Navigate to Main Menu->Transport Manager -> Maintenance -> Transport</p>  <p>Select each transport and click on the Enable button</p>  <p>Verify that the Operational Status for each transport is Up.</p>
<p>39</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable MAPIWF application if needed (Applicable ONLY for DSR 6.0+)</p>	<p>Navigate to Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users</p>  <p>Click on the Enable button corresponding to MAPIWF Application Name.</p>  <p>Verify that the SSN Status is Enabled.</p>

Procedure 4: Recovery Scenario 4

<p>40</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable links if needed (Applicable ONLY for DSR 6.0+)</p>	<p>Navigate to Main Menu->SS7/Sigtran->Maintenance->Links</p>  <p>Click on Enable button for each link.</p>  <p>Verify that the Operational Status for each link is Up.</p>
<p>41</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Examine All Alarms</p>	<p>Navigate to Main Menu->Alarms & Events->View Active</p>  <p>Examine all active alarms and refer to the on-line help on how to address them.</p> <p>If needed contact Appendix H. My Oracle Support (MOS).</p>
<p>42</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Examine All Alarms</p>	<p>Login to the NOAM VIP if not already logged in.</p> <p>Navigate to Main Menu->Alarms & Events->View Active</p>  <p>Examine all active alarms and refer to the on-line help on how to address them.</p> <p>If needed contact Appendix H. My Oracle Support (MOS).</p>
<p>43</p> <p><input type="checkbox"/></p>	<p>Restart oampAgent if Needed</p>	<p>Note: If alarm “10012: The responder for a monitored table failed to respond to a table change” is raised, the oampAgent needs to be restarted.</p> <p>Establish an SSH session to each server that has the alarm. Login as root (5.0) or admusr (6.0+)</p> <p>Execute the following commands:</p> <pre> \$ sudo pm.set off oampAgent \$ sudo pm.set on oampAgent </pre>

Procedure 4: Recovery Scenario 4

44 <input type="checkbox"/>	Backup and Archive All the Databases from the Recovered System	Execute Appendix A. DSR Database Backup to back up the Configuration databases:
--------------------------------	---	--

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 is intact at the active NOAM server and does not require restoration at the SOAM and MP servers.

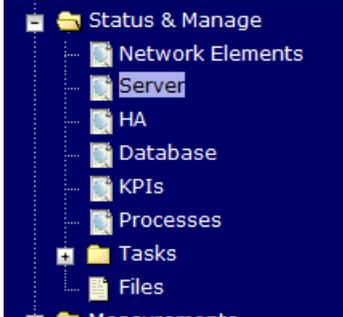
Procedure 5: Recovery Scenario 5

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

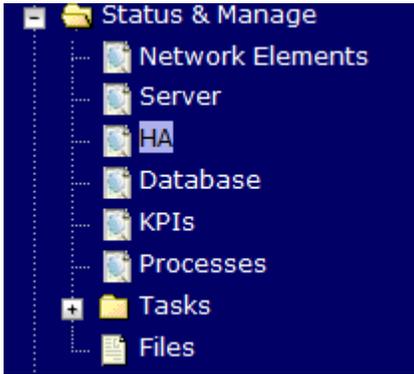
Procedure 5: Recovery Scenario 5

4 <input type="checkbox"/>	Recover System	<p>If ALL SOAM servers have failed, execute Procedure 2</p> <p>If ALL NOAM servers have failed, execute the following steps:</p> <ol style="list-style-type: none">1) Procedure 4: <i>Steps 3-7, 8-10</i>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 admusr user, exchange SSH keys for admusr 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 admusr user of the PMAC server. <pre>\$ keyexchange admusr@<Recovered_PMAC_IP Address></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 admusr user, exchange SSH keys for admusr 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 admusr user of the VM guest. <pre>\$ keyexchange admusr@<Recovered_VM_control_IP Address></pre> Note: if keyexchange fails, edit /home/admusr/.ssh/known_hosts and remove blank lines, and retry the keyexchange commands.4) Procedure 4: <i>12-13(For each NOAM))</i>
-------------------------------	-----------------------	--

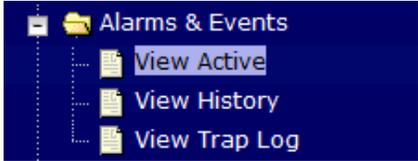
Procedure 5: Recovery Scenario 5

<p>5</p> <p><input type="checkbox"/></p>	<p>Perform Key exchange between Active NOAM and Recovered NOAMs</p>	<p>Perform a keyexchange between the newly active NOAM and the recovered NOAM servers:</p> <p>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 servers using the keyexchange utility, using the host names of the recovered NOAMs.</p> <p>When prompted for the password, enter the password for the <i>admusr</i> user of the recovered NOAM servers.</p> <pre style="border: 1px solid black; padding: 5px; width: fit-content;">\$ keyexchange admusr@<Recovered_NOAM Hostname></pre>
<p>6</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Restart DSR application</p>	<p>Navigate to Main Menu->Status & Manage->Server,</p>  <p>Select each recovered NOAM server and click on Restart.</p> <div style="display: flex; justify-content: center; gap: 10px;"> Stop Restart Reboot NTP Sync Report </div>

Procedure 5: Recovery Scenario 5

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

Procedure 5: Recovery Scenario 5

<p>10</p> <p><input type="checkbox"/></p>	<p>Recovered Active NOAM: Activate Optional Features</p>	<p>Establish an SSH session to the Active NOAM, login as admusr.</p> <p>If PCA was previously activated, execute the following commands:</p> <pre style="border: 1px solid black; padding: 5px;">\$ cd /usr/TKLC/dsr/prod/maint/loaders/activate \$./load.pcaActivateStandByAsScoped</pre> <p>If MAP-Diameter IWF was previously activated, execute the following commands:</p> <pre style="border: 1px solid black; padding: 5px;">\$ cd /usr/TKLC/dsr/prod/maint/loaders/activate \$./load.mapinterworkingActivateAsourced</pre>
<p>11</p> <p><input type="checkbox"/></p>	<p>Recovered Standby NOAM: Prepare and Activate Recovered Standby NOAM for Optional Feature Activation.</p>	<p>Repeat Steps 5-7 for the preparing and activating previously activated features on the recovered Standby NOAM.</p>
<p>12</p> <p><input type="checkbox"/></p>	<p>Switch DR NOAM Back to Secondary</p>	<p>Once the system have been recovered:</p> <p>Execute Appendix D. Returning a Recovered Site to Primary to have the recovered NOAM become primary again.</p>
<p>13</p> <p><input type="checkbox"/></p>	<p>Recovered Servers: Verify Alarms</p>	<p>Navigate to Main Menu -> Alarms & Events -> View Active</p>  <p>Verify the recovered servers are not contributing to any active alarms (Replication, Topology misconfiguration, database impairments, NTP, etc.)</p>

5.1.6 Recovery Scenario 6 (Database Recovery)

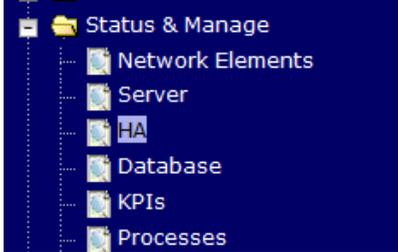
5.1.6.1 Recovery Scenario 6: Case 1

For a partial outage with

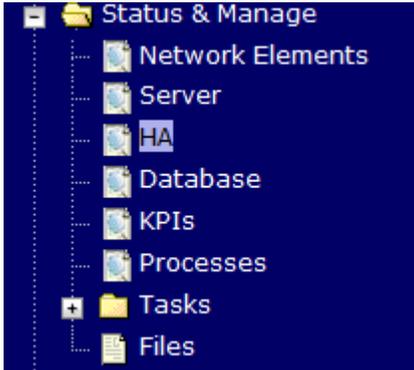
- Server having a corrupted database
- Replication channel from parent is inhibited because of upgrade activity or
- Server is in a different release then that of its Active parent because of upgrade activity.
- Verify that the Server Runtime backup files, performed at the start of the upgrade, are present in /var/TKLC/db/filemgmt area in the following format
 - Backup.DSR.HPC02-NO2.FullDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2
 - 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 T E P #	<p>This procedure performs recovery if database is corrupted in the system</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Workarounds	Refer to Appendix G . Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
2 <input type="checkbox"/>	NOAM VIP GUI: Set Failed Servers to Standby	<p>Navigate to Main Menu -> Status & Manage -> HA</p>  <p>Select Edit</p> <p>Set the Max Allowed HA Role drop down box to Standby for the failed servers.</p> <p>Select Ok</p> <div style="text-align: center;"> <input type="button" value="Ok"/> <input type="button" value="Cancel"/> </div>

Procedure 6: Recovery Scenario 6 (Case 1)

<p>3 <input type="checkbox"/></p>	<p>Server in Question: Login</p>	<p>Establish an SSH session to the server in question. Login as root(5.0) or admusr(6.0+) user.</p>
<p>4 <input type="checkbox"/></p>	<p>Server in Question: Change runlevel to 3</p>	<p>Execute the following command to bring the system to runlevel 3.</p> <pre>\$ sudo init 3</pre>
<p>5 <input type="checkbox"/></p>	<p>Server in Question: Recover System</p>	<p>Execute the following command and follow the instructions appearing the console prompt</p> <pre>\$ sudo /usr/TKLC/appworks/sbin/backout_restore</pre>
<p>6 <input type="checkbox"/></p>	<p>Server in Question: Change runlevel to 4</p>	<p>Execute the following command to bring the system back to runlevel 4.</p> <pre>\$ sudo init 6</pre>
<p>7 <input type="checkbox"/></p>	<p>Server in Question: Verify the server</p>	<p>Execute the following command to verify if the processes are up and running</p> <pre>\$ sudo pm.getprocs</pre>
<p>8 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Set Failed Servers to Active</p>	<p>Navigate to Status & Manage -> HA</p>  <p>Click on Edit at the bottom of the screen</p> <p>For each failed server whose Max Allowed HA Role is set to Standby, set it to Active</p> <p>Press OK</p>

Procedure 6: Recovery Scenario 6 (Case 1)

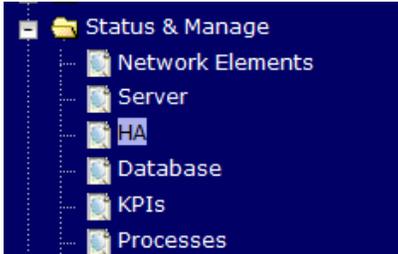
<p>9</p> <p><input type="checkbox"/></p>	<p>Active NOAM: Verify Sync Split Scope Data (If POLICY AND CHARGING DRA is activated): 5.0/6.0 Only</p>	<p>If recovering a DSR 5.0/6.0 system and POLICY AND CHARGING DRA application is activated then execute this step.</p> <p>Note: If recovering a DSR 7.0+ system, DO NOT execute this step</p> <p>Login to the Active NOAM VIP via SSH terminal as root(5.0) or admusr(6.0+) user.</p> <p>Execute the following steps:</p> <p>Go to Appworks bin directory:</p> <pre>\$ sudo cd /usr/TKLC/appworks/bin/</pre> <p>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:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -reportonly</pre> <p>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.</p> <p>The “sync” option will modify the database:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -sync</pre> <p>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”:</p> <pre>\$ sudo ./syncPcrfReferencesAfterRestore.sh -reportonly</pre>
<p>10</p> <p><input type="checkbox"/></p>	<p>Backup and Archive All the Databases from the Recovered System</p>	<p>Execute Appendix A. DSR Database Backup to back up the Configuration databases:</p>

5.1.6.2 Recovery Scenario 6: Case 2

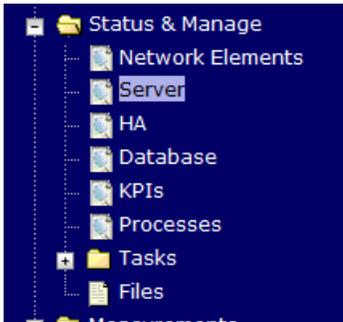
For a partial outage with

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

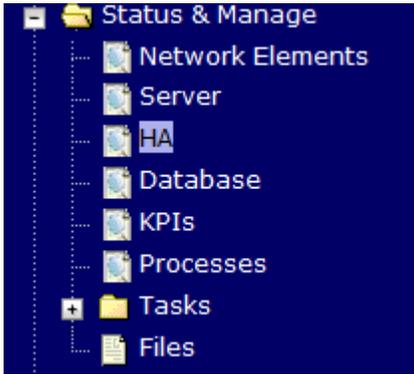
Procedure 7: Recovery Scenario 6 (Case 2)

S T E P #	<p>This procedure performs recovery if database got corrupted in the system and system is in the state to get replicated</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Workarounds	Refer to Appendix G . Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
2 <input type="checkbox"/>	NOAM VIP GUI: Set Failed Servers to Standby	<p>Navigate to Main Menu -> Status & Manage -> HA</p>  <p>Select Edit</p> <p>Set the Max Allowed HA Role drop down box to Standby for the failed servers.</p> <p>Select Ok</p> 
3 <input type="checkbox"/>	Server in Question: Login	Establish an SSH session to the server in question. Login as root(5.0) or admusr(6.0+) user.
4 <input type="checkbox"/>	Server in Question: Take Server out of Service	<p>Execute the following command to take the server out of service.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo bash -l \$ sudo prod.clobber</pre>

Procedure 7: Recovery Scenario 6 (Case 2)

<p>5</p> <p><input type="checkbox"/></p>	<p>Server in Question: Take Server to DbUp State and Start the Application</p>	<p>Execute the following commands to take the server to Dbup and start the DSR application:</p> <pre>\$ sudo bash -l \$ sudo prod.start</pre>
<p>6</p> <p><input type="checkbox"/></p>	<p>Server in Question: Verify the Server State</p>	<p>Execute the following commands to verify the processes are up and running:</p> <pre>\$ sudo pm.getprocs</pre> <p>Execute the following command to verify if replication channels are up and running:</p> <pre>\$ sudo irepstat</pre> <p>Execute the following command to verify if merging channels are up and running:</p> <pre>\$ sudo inetmstat</pre>
<p>7</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Restart DSR application</p>	<p>Navigate to Main Menu->Status & Manage->Server,</p>  <p>Select each recovered server and click on Restart.</p> <p> <input type="button" value="Stop"/> <input type="button" value="Restart"/> <input type="button" value="Reboot"/> <input type="button" value="NTP Sync"/> <input type="button" value="Report"/> </p>

Procedure 7: Recovery Scenario 6 (Case 2)

<p>8</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Set Failed Servers to Active</p>	<p>Navigate to Status & Manage -> HA</p>  <p>Click on Edit at the bottom of the screen</p> <p>For each failed server whose Max Allowed HA Role is set to Standby, set it to Active</p> <p>Press OK</p>
<p>9</p> <p><input type="checkbox"/></p>	<p>Backup and Archive All the Databases from the Recovered System</p>	<p>Execute Appendix A. DSR Database Backup to back up the Configuration databases:</p>

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.

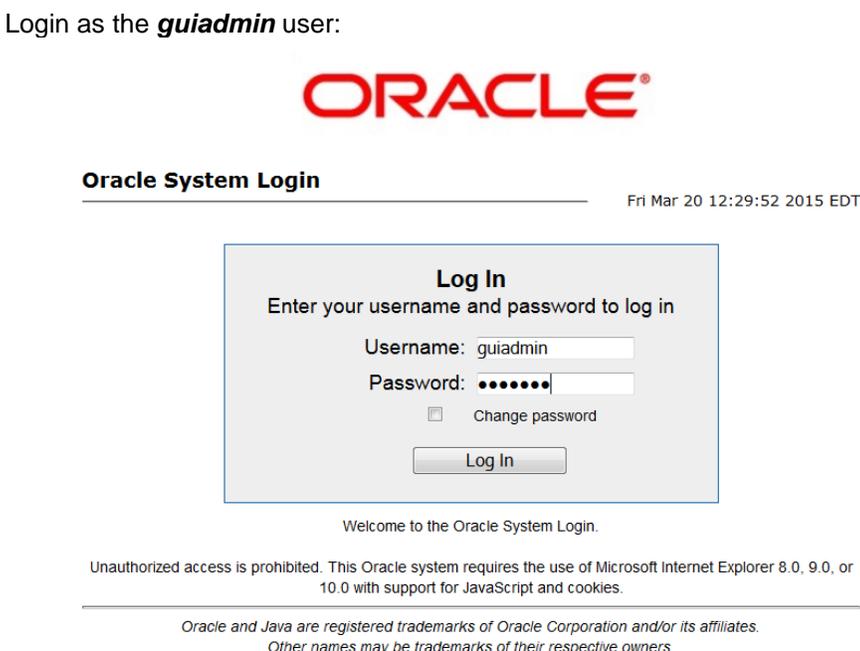
6.1 Restoring a Deleted User

<p>- User 'testuser' exists in the selected backup file but not in the current database.</p>
--

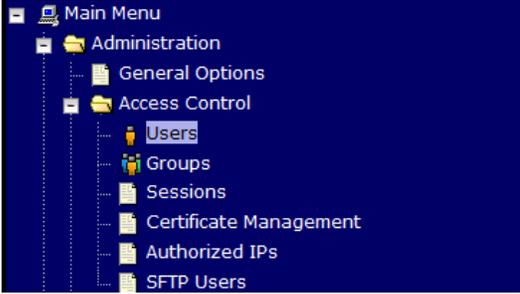
These users were removed prior to creation of the backup and archive file. They will be reintroduced by system restoration of that file.

6.2 Keeping a Restored user

Procedure 8: Keep Restored User

S T E P #	<p>Perform this procedure to keep users that will be restored by system restoration.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	<p>Before Restoration: Notify Affected Users Before Restoration</p>	<p>Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.</p>
2 <input type="checkbox"/>	<p>After Restoration: Login to the NOAM VIP</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 10px auto;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the <i>guiadmin</i> user:</p> <div style="text-align: center; margin: 20px 0;">  </div>

Procedure 8: Keep Restored User

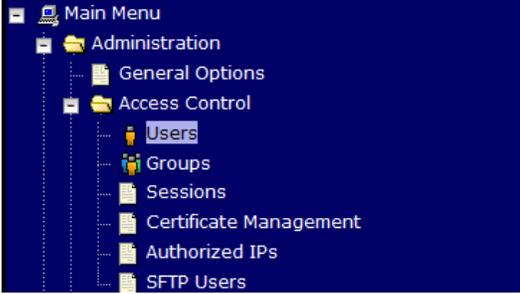
<p>3</p> <p>□</p>	<p>After Restoration: Reset User Passwords</p>	<p>Navigate to Administration -> Access Control -> Users</p>  <p>Select the user</p> <p>Click the Change Password button</p>  <p>Enter a new password</p>  <p>Click the Continue button</p>
-------------------	---	---

6.3 Removing a Restored User

Procedure 9: Remove the Restored User

S T E P #	<p>Perform this procedure to remove users that will be restored by system restoration</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>
<p>1</p> <p><input type="checkbox"/></p>	<p>After Restoration: Login to the NOAM VIP</p> <p>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:</p> <div data-bbox="492 705 1346 747" style="border: 1px solid black; padding: 2px;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the <i>guiadmin</i> user:</p> 

Procedure 9: Remove the Restored User

<p>2</p> <p>□</p>	<p>After Restoration: Reset User Passwords</p>	<p>Navigate to Administration -> Access Control -> Users</p>  <p>Select the user</p> <p>Click the Delete button</p>  <p>Delete selected users?</p>  <p>Click the OK button to confirm.</p>
-------------------	---	--

6.4 Restoring a Modified User

These users have had a password change prior to creation of the backup and archive file. They 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. They 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.

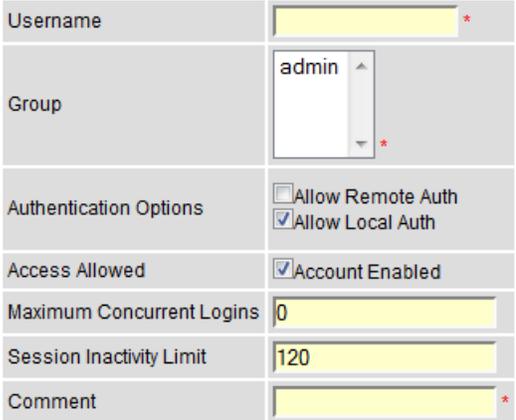
Procedure 10: Restoring an Archive that does not Contain a Current User

S T E P #	Perform this procedure to remove users that will be restored by system restoration	
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
	If this procedure fails, contact Appendix H . My Oracle Support (MOS) and ask for assistance.	
1 <input type="checkbox"/>	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 <input type="checkbox"/>	Before Restoration: Login to the NOAM VIP	<p>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:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the <i>guiadmin</i> user:</p> <div style="text-align: center;">  </div>

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

<p>3</p> <p><input type="checkbox"/></p>	<p>Before Restoration: Record user settings</p>	<p>Navigate to Administration -> Access Control -> Users</p>  <p>Under each affected user, record the following:</p> <ul style="list-style-type: none"> • Username, • Account status • Remote Auth • Local Auth • Concurrent Logins Allowed • Inactivity Limit • Comment • Groups
<p>4</p> <p><input type="checkbox"/></p>	<p>After Restoration: Login</p>	<p>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:</p> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px auto;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user:</p>  <p>Welcome to the Oracle System Login.</p> <p>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.</p> <p><small>Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</small></p>

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

<p>5</p> <p>☐</p>	<p>After Restoration: Recreate affected user</p>	<p>Navigate to Administration -> Access Control -> Users</p>  <p>Click Insert</p>  <p>Recreate the user using the data collected in Step 3.</p>  <p>Click Ok</p> 
<p>6</p> <p>☐</p>	<p>After Restoration: Repeat for Additional Users</p>	<p>Repeat Step 5 to recreate additional users.</p>
<p>7</p> <p>☐</p>	<p>After Restoration: Reset the Passwords</p>	<p>See Procedure 8 for resetting passwords for a user.</p>

7.0 IDIH Disaster Recovery

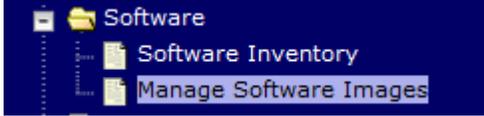
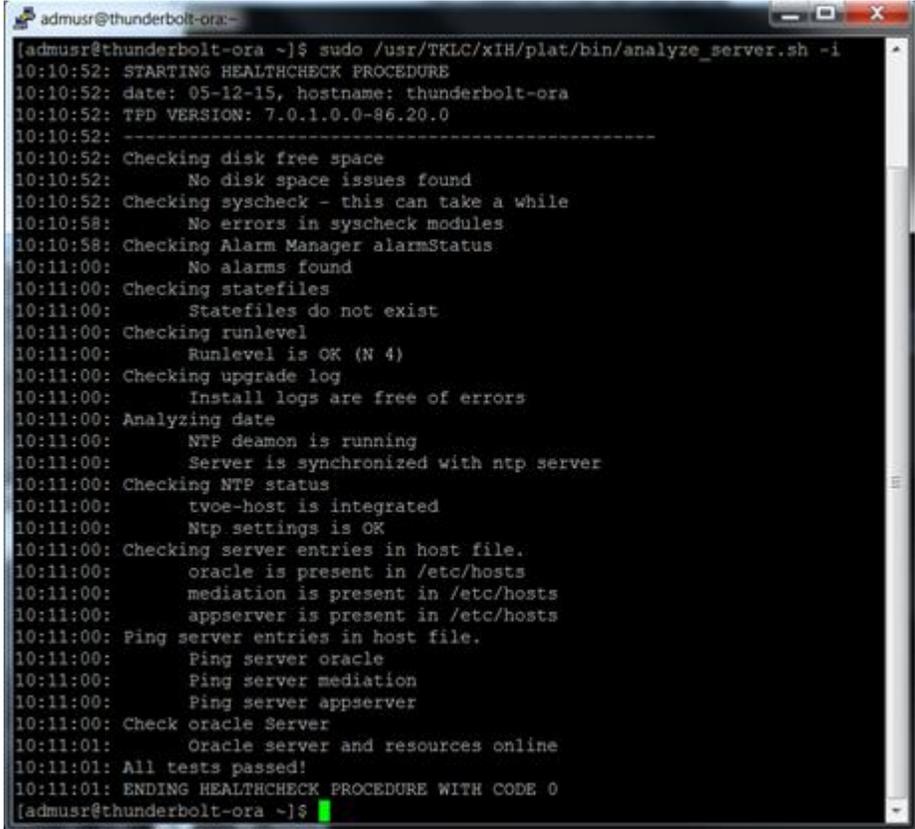
The fdconfig xml file you use for disaster recovery is different from the one used for fresh installation. The one for disaster recovery has hostname-**upgrade_xx-xx-xx.xml** file format. It took out the oracle server installation part since for disaster recovery it is not needed.

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.

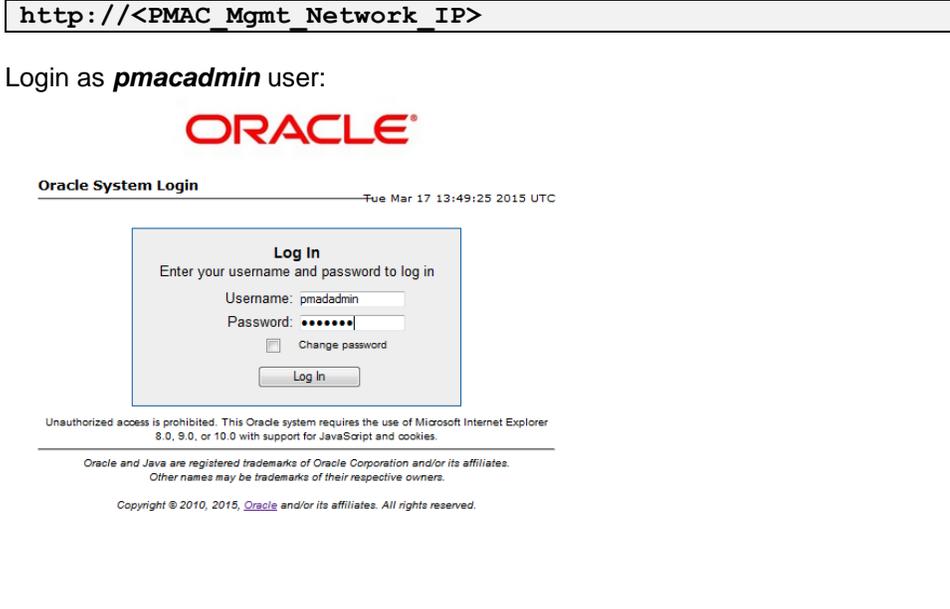
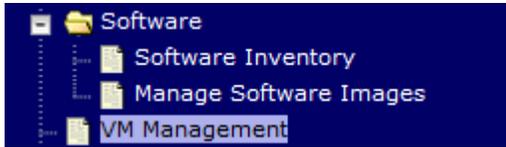
Procedure 11: IDIH Disaster Recovery Preparation

S T E P #	<p>This procedure performs disaster recovery preparation steps for the IDIH.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	PMAC GUI: Login	<p>Open web browser and enter:</p> <p>http://<PMAC Mgmt Network IP></p> <p>Login as <i>pmacadmin</i> user:</p> 

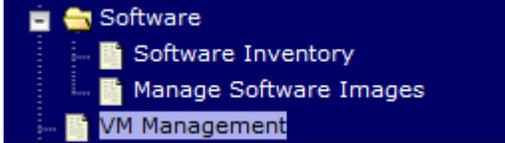
Procedure 11: IDIH Disaster Recovery Preparation

<p>2</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Verify necessary IDIH images are available</p>	<p>Navigate to Main Menu -> Software -> Manage Software Images</p>  <p>Verify the current IDIH TVOE, TPD, Oracle, Application and Mediation images are listed.</p> <p>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</p>
<p>3</p> <p><input type="checkbox"/></p>	<p>Oracle Guest: Login</p>	<p>Establish an SSH session to the Oracle guest, login as admusr.</p>
<p>4</p> <p><input type="checkbox"/></p>	<p>Oracle Guest: Perform Database Health check</p>	<p>Execute the following command to perform a database health check:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i</pre> <p>Output:</p> 

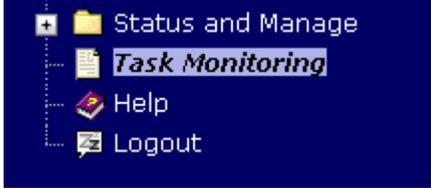
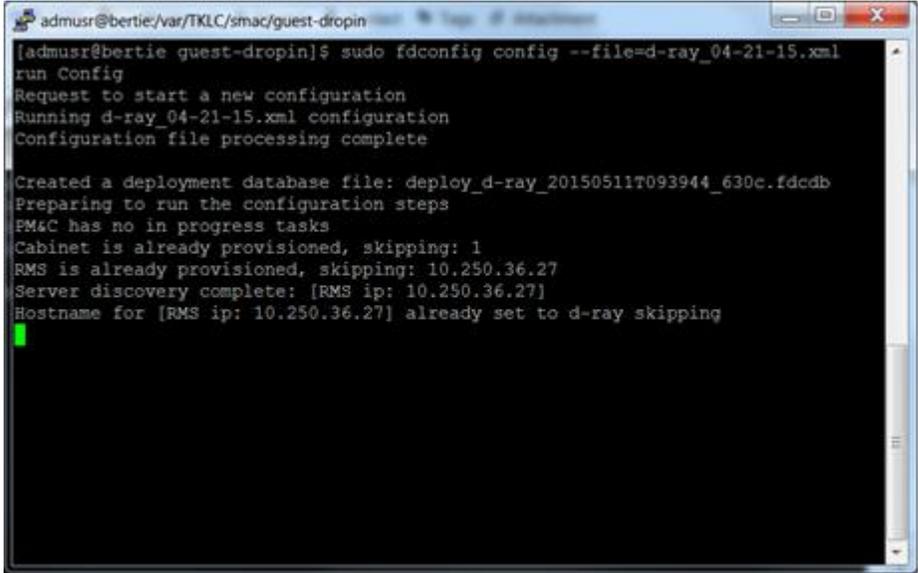
Procedure 12: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

<p>S T E P #</p>	<p>This procedure performs disaster recovery for the IDIH by re-installing the mediation and application servers.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>
<p>1 <input type="checkbox"/></p>	<p>PMAC GUI: Login</p> <p>Open web browser and enter:</p> <p>http://<PMAC Mgmt Network IP></p> <p>Login as <i>pmacadmin</i> user:</p> 
<p>2 <input type="checkbox"/></p>	<p>Remove existing Application Server</p> <p>Navigate to Main Menu -> VM Management</p>  <p>Select the application guest,</p> <p>Click on the Delete button.</p> 

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

<p>3</p> <p><input type="checkbox"/></p>	<p>Remove existing Mediation Server</p>	<p>Navigate to Main Menu -> VM Management</p>  <p>Select the Mediation guest,</p> <p>Click on the Delete button.</p> 
<p>4</p> <p><input type="checkbox"/></p>	<p>PMAC: Establish SSH session and Login</p>	<p>Establish an SSH session to the PMAC, login as admusr.</p>
<p>5</p> <p><input type="checkbox"/></p>	<p>PMAC: Re-install the Mediation and Application Servers</p>	<p>Execute the following command (Enter your upgrade file) :</p> <pre data-bbox="488 915 1419 1035"> \$ cd /var/TKLC/smac/guest-dropin \$ sudo fdconfig config -file=<hostname-upgrade_XX-XX-XX>.xml </pre>  <p>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.</p>

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

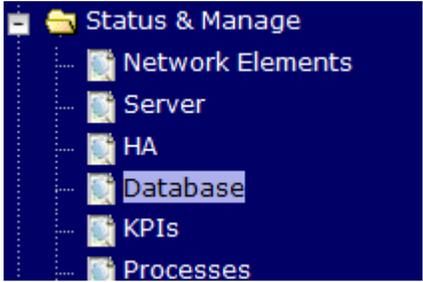
<p>6</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Monitor the Configuration</p>	<p>If not already done so, establish a GUI session on the PMAC server.</p> <p>Navigate to Main Menu -> Task Monitoring</p>  <p>Monitor the IDIH configuration to completion.</p> <p>Alternatively, you can monitor the fdconfig status through the command line after executing the fdconfig command:</p> <p>Example:</p> 
--	---	--

Appendix A. DSR Database Backup

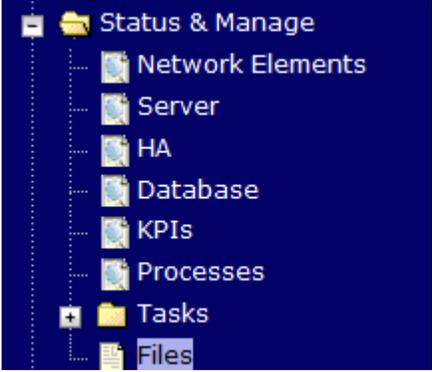
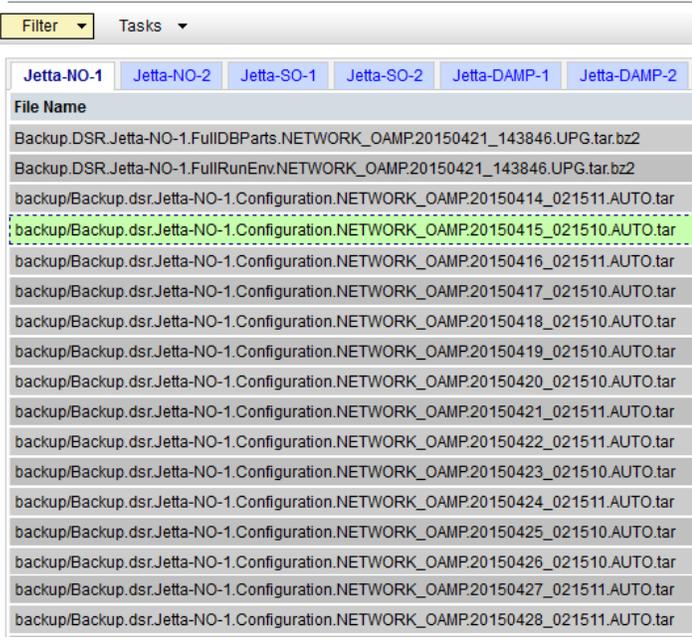
Procedure 13: Restoring an Archive that does not Contain a Current User

<p>S T E P #</p>	<p>The intent of this procedure is to back up the provision and configuration information from an NOAM or SOAM server after the disaster recovery is complete</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>NOAM/SOAM VIP: Login</p>	<p>Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server.</p> <p>Open the web browser and enter a URL of:</p> <div data-bbox="492 751 1346 793" style="border: 1px solid black; padding: 2px;"> <p>http://<Primary_NOAM/SOAM_VIP_IP_Address></p> </div> <p>Login as the <i>guiadmin</i> user:</p> <div data-bbox="475 877 1438 1476" style="text-align: center;">  <p>The screenshot shows the Oracle System Login interface. At the top is the Oracle logo in red. Below it, the text 'Oracle System Login' is displayed, followed by a horizontal line and the date 'Fri Mar 20 12:29:52 2015 EDT'. A central box titled 'Log In' contains the instruction 'Enter your username and password to log in'. Below this are two input fields: 'Username: guiadmin' and 'Password: ●●●●●●'. There is a checkbox labeled 'Change password' and a 'Log In' button. At the bottom of the screenshot, it says '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.', and a footer with trademark information: 'Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.'</p> </div>

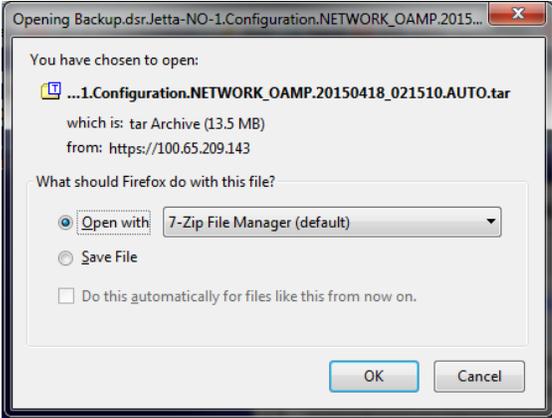
Procedure 13: Restoring an Archive that does not Contain a Current User

<p>2</p> <p><input type="checkbox"/></p>	<p>NOAM/SOAM VIP: Backup Configuration Data for the System</p>	<p>Navigate to Main Menu -> Status & Manage -> Database</p>  <p>Select the Active NOAM Server and Click on Backup button</p>  <p>Make sure that the checkboxes next to "Configuration" is checked.</p> <p>Database Backup</p> <table border="1" data-bbox="500 835 1317 1129"> <thead> <tr> <th>Field</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Server: Jetta-NO-1</td> <td></td> </tr> <tr> <td>Select data for backup</td> <td> <input type="checkbox"/> Provisioning <input checked="" type="checkbox"/> Configuration </td> </tr> <tr> <td>Compression</td> <td> <input type="radio"/> gzip <input checked="" type="radio"/> bzip2 <input type="radio"/> none * </td> </tr> <tr> <td>Archive Name</td> <td>Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150428_093111.*</td> </tr> <tr> <td>Comment</td> <td><input type="text"/></td> </tr> </tbody> </table> <p style="text-align: right;"><input type="button" value="Ok"/> <input type="button" value="Cancel"/></p> <p>Enter a filename for the backup and press OK</p>	Field	Value	Server: Jetta-NO-1		Select data for backup	<input type="checkbox"/> Provisioning <input checked="" type="checkbox"/> Configuration	Compression	<input type="radio"/> gzip <input checked="" type="radio"/> bzip2 <input type="radio"/> none *	Archive Name	Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150428_093111.*	Comment	<input type="text"/>
Field	Value													
Server: Jetta-NO-1														
Select data for backup	<input type="checkbox"/> Provisioning <input checked="" type="checkbox"/> Configuration													
Compression	<input type="radio"/> gzip <input checked="" type="radio"/> bzip2 <input type="radio"/> none *													
Archive Name	Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150428_093111.*													
Comment	<input type="text"/>													

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

<p>3</p> <p><input type="checkbox"/></p>	<p>NOAM/SOAM VIP: Verify the backup file existence.</p>	<p>Navigate to Main Menu -> Status & Manage -> Files</p>  <p>Main Menu: Status & Manage -> Files</p>  <p>Select the Active NOAM or SOAM tab.</p> <p>The files on this server will be displayed. Verify the existence of the backup file.</p>
--	--	---

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

<p>4</p> <p><input type="checkbox"/></p>	<p>NOAM/SOAM VIP: Download the file to a local machine.</p>	<p>From the previous step, choose the backup file.</p> <p>Select the Download button</p>  <p>Select OK to confirm the download.</p> 
<p>5</p> <p><input type="checkbox"/></p>	<p>Upload the Image to Secure Location</p>	<p>Transfer the backed up image saved in the previous step to a secure location where the Server Backup files are fetched in case of system disaster recovery.</p>
<p>6</p> <p><input type="checkbox"/></p>	<p>Backup Active SOAM</p>	<p>Repeat Steps 2 through 5 to back up the Active SOAM</p>

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 E P #	<p>The intent of this procedure is to recover a failed Aggregation (4948E / 4948E-F) Switch.</p> <p>Prerequisites for this procedure are:</p> <ul style="list-style-type: none"> • 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 • Rack Mount position of the failed switch <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <input type="checkbox"/>	<p>Recover failed Aggregation Switches: Cisco 4948E/4948E-F</p>	<p>Login to the PMAC via SSH as root(5.0) or admusr(6.0+)</p> <p>Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell:</p> <pre style="border: 1px solid black; padding: 5px; display: inline-block;">sudo ssh-keygen -R <4948_switch_ip></pre> <p>Refer to procedure “<i>Replace a failed 4948/4948E/4948E-F switch (c-Class system) (netConfig)</i>” to replace a failed Aggregation switch. - Refer to Table 7: Platform Configuration Reference Table for the applicable platform configuration reference.</p> <p>Note: You will need a copy of the HP Misc Firmware DVD or ISO (<i>or firmware file obtained from the appropriate hardware vendor</i>) 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.</p>

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

<p>S T E P #</p>	<p>The intent of this procedure is to recover a failed Enclosure (3020) Switch.</p> <p>Prerequisites for this procedure are:</p> <ul style="list-style-type: none"> • 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 <p>Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
<p>1 <input type="checkbox"/></p>	<p>Recover failed Enclosure Switch: Cisco 3020</p>	<p>Login to the PMAC via SSH as root(5.0) or admusr(6.0+)</p> <p>Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell:</p> <pre style="border: 1px solid black; padding: 5px; display: inline-block;">sudo ssh-keygen -R <enclosure_switch_ip></pre> <p>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.</p> <p>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.</p>

Procedure 16: Recovering a Failed Enclosure Switch (HP 6120XG)

S T E P #	<p>The intent of this procedure is to recover a failed Enclosure (6120XG) Switch.</p> <p>Prerequisites for this procedure are:</p> <ul style="list-style-type: none"> • A copy of the networking xml configuration files • IP address and hostname of the failed switch • Interconnect Bay position of the enclosure switch <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	<p>Recover failed Enclosure Switch: HP 6120XG</p>	<p>Login to the PMAC via SSH as root(5.0) or admusr(6.0+)</p> <p>Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>sudo ssh-keygen -R <enclosure_switch_ip></pre> </div> <p>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.</p> <p>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.</p>

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

S T E P #	<p>The intent of this procedure is to recover a failed Enclosure (6125XLG/6125G) Switch.</p> <p>Prerequisites for this procedure are:</p> <ul style="list-style-type: none"> • A copy of the networking xml configuration files <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	<p>Recover failed Enclosure Switch: HP 6125XLG/6125G</p>	<p>Login to the PMAC via SSH as root(5.0) or admusr(6.0+)</p> <p>Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>sudo ssh-keygen -R <enclosure_switch_ip></pre> </div> <p>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.</p> <p>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.</p>

Procedure 18: Recovering a Failed Enclosure OA

S T E P #	The intent of this procedure is to recover a failed Enclosure Onboard Administrator. 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 <input type="checkbox"/>	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.

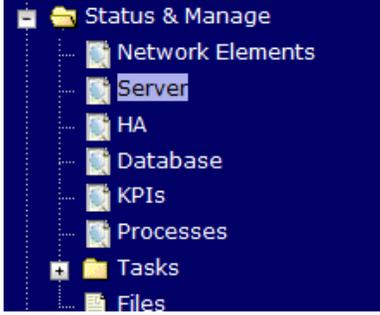
Preconditions:

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

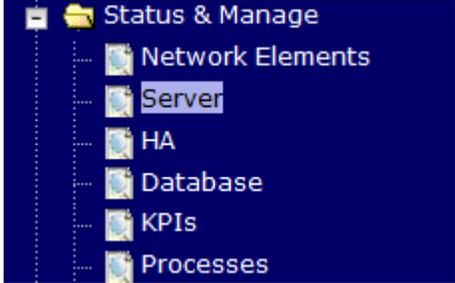
Procedure 19: Switching a DR NOAM Site to Primary

S T E P #	<p>The intent of this procedure is to switch a DR site to Primary.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>DR-NOAM VIP: Login</p>	<p>Establish a GUI session on the DR-NOAM server by using the VIP IP address of the DR-NOAM.</p> <p>Open the web browser and enter a URL of:</p> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px auto;"> <p><code>http://<Primary_DR_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the <i>guiadmin</i> user:</p> <div style="text-align: center;">  </div>

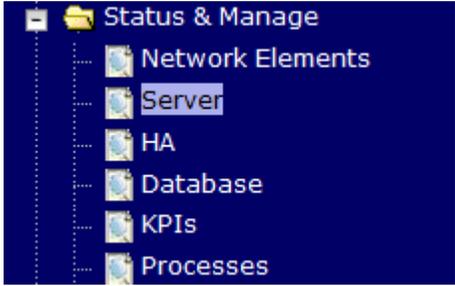
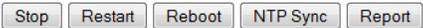
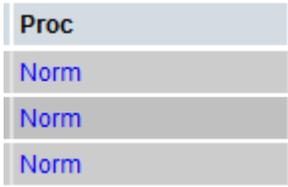
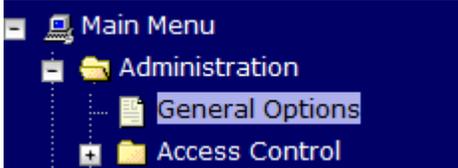
Procedure 19: Switching a DR NOAM Site to Primary

<p>2</p> <p><input type="checkbox"/></p>	<p>DR-NOAM VIP: Disable DSR Application on DR-NOAM Servers</p>	<p>Navigate to Main Menu -> Status & Manage -> Server</p>  <p>Select the row that has the Active DR-NOAM server.</p> <p>Select the Stop button.</p>  <p>Note: At this time, HA switch over causes an automatic logout.</p>
<p>3</p> <p><input type="checkbox"/></p>	<p>DR-NOAM VIP: Login</p>	<p>Establish a GUI session on the DR-NOAM server by using the VIP IP address of the DR-NOAM.</p> <p>Open the web browser and enter a URL of:</p> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px auto;"> <p><code>http://<Primary_DR_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user:</p> 

Procedure 19: Switching a DR NOAM Site to Primary

4 <input type="checkbox"/>	DR-NOAM VIP: Repeat	Repeat step 2 to disable the DSR application on the now active DR NOAM. Note: The DSR application should now be stopped on all DR-NOAMs.								
5 <input type="checkbox"/>	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 <input type="checkbox"/>	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 <input type="checkbox"/>	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: <pre>\$ sudo top.myrole</pre> System generates several replication and collection alarms as replication/collection links to/from former Primary NOAM servers becomes inactive.								
8 <input type="checkbox"/>	Primary DR-NOAM: Verify Replication	Navigate to Main Menu -> Status & Manage -> Server  It may take several minutes for replication; afterward the “ DB ” and “ Reporting Status ” columns should show “ Normal ”. <table border="1" data-bbox="488 1541 943 1688"> <thead> <tr> <th>DB</th> <th>Reporting Status</th> </tr> </thead> <tbody> <tr> <td>Norm</td> <td>Norm</td> </tr> <tr> <td>Norm</td> <td>Norm</td> </tr> <tr> <td>Norm</td> <td>Norm</td> </tr> </tbody> </table>	DB	Reporting Status	Norm	Norm	Norm	Norm	Norm	Norm
DB	Reporting Status									
Norm	Norm									
Norm	Norm									
Norm	Norm									

Procedure 19: Switching a DR NOAM Site to Primary

<p>9</p> <p><input type="checkbox"/></p>	<p>New Primary NOAM: Re-enable the application.</p>	<p>Navigate to Main Menu -> Status & Manage -> Server</p>  <p>Select the row that has the active New-Primary NOAM server.</p> <p>Click the Restart button and then click the OK button.</p>  <p>Verify that “PROC” column now shows “Norm”.</p>  <p>Provisioning can now resume to the VIP of the new-Primary DSR.</p>
<p>10</p> <p><input type="checkbox"/></p>	<p>New Primary NOAM: Decrease the Durability Admin status</p>	<p>Lower the durability admin status to (NOAM pair) to exclude former-Primary NOAM servers from the provisioning database durability.</p> <p>A value greater than 2 must be adjusted downward.</p> <p>Navigate to Main Menu -> Administration -> General Options</p>  <p>Set “cm.idb.durableAdminState” to 2 (NOAM pair)</p>  <p>Click the OK button</p>

Procedure 19: Switching a DR NOAM Site to Primary

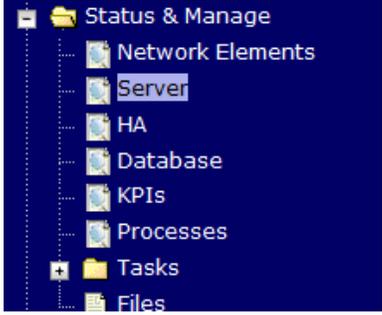
11	New Primary NOAM: Repeat for standby of new-primary NOAM Server	Repeat steps 8-9 for standby of the new-Primary NOAM server.
----	--	---

Appendix D. Returning a Recovered Site to Primary

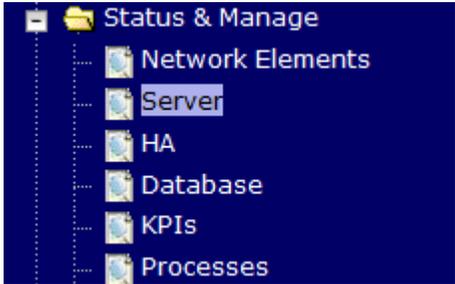
Procedure 20: Returning a Recovered Site to Primary

S T E P #	<p>The intent of this procedure is to return a recovered site to primary.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
1	<p>Primary NOAM VIP: Login</p>	<p>Establish a GUI session on the primary NOAM server by using the VIP IP address of the primary NOAM.</p> <p>Open the web browser and enter a URL of:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the <i>guiadmin</i> user:</p> <div style="text-align: center;">  <p>The screenshot shows the Oracle System Login interface. At the top is the Oracle logo. Below it is the text 'Oracle System Login' followed by a horizontal line and the date 'Fri Mar 20 12:29:52 2015 EDT'. In the center is a 'Log In' box with the heading 'Log In' and the instruction 'Enter your username and password to log in'. Inside this box are fields for 'Username: guiadmin' and 'Password: ●●●●●●', a 'Change password' checkbox, and a 'Log In' button. Below the box is the text 'Welcome to the Oracle System Login.' At the bottom, there is a disclaimer: '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.' and a footer: 'Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.'</p> </div>

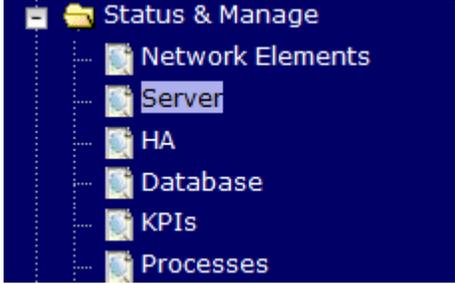
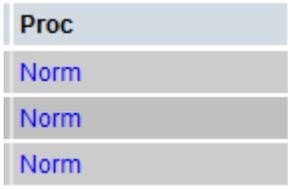
Procedure 20: Returning a Recovered Site to Primary

<p>2</p> <p><input type="checkbox"/></p>	<p>Primary NOAM VIP: Disable DSR Application on DR-NOAM Servers</p>	<p>Navigate to Main Menu -> Status & Manage -> Server</p>  <p>Select the row that has the Active DR-NOAM server.</p> <p>Select the Stop button.</p>  <p>Note: At this time, HA switch over causes an automatic logout.</p>
<p>3</p> <p><input type="checkbox"/></p>	<p>Primary NOAM VIP: Login</p>	<p>Establish a GUI session on the primary NOAM server by using the VIP IP address of the NOAM.</p> <p>Open the web browser and enter a URL of:</p> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px auto;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user:</p>  <p>Welcome to the Oracle System Login.</p> <p>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.</p> <p><small>Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</small></p>

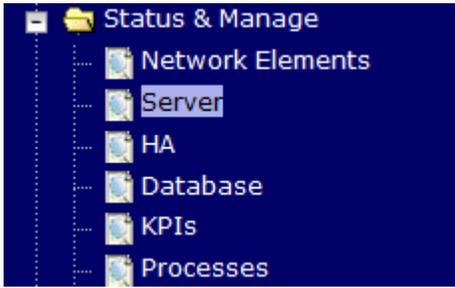
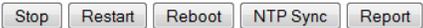
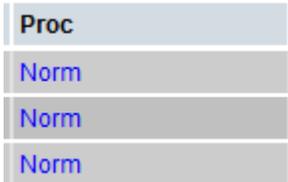
Procedure 20: Returning a Recovered Site to Primary

<p>4 <input type="checkbox"/></p>	<p>Primary NOAM VIP: Repeat</p>	<p>Repeat step 2 to disable the DSR application on the now active DR NOAM. Note: The DSR application should now be stopped on all DR-NOAMs.</p>								
<p>5 <input type="checkbox"/></p>	<p>Primary NOAM VIP: Verify DSR application is stopped.</p>	<p>Verify that “PROC” column on both DR DSR servers show “Man” indicating that application is manually stopped</p>								
<p>6 <input type="checkbox"/></p>	<p>Primary NOAM VIP: Establish an SSH session</p>	<p>Login via SSH to the physical IP of the chosen primary DR-NOAM server as root(5.0) or admusr(6.0+) user.</p>								
<p>7 <input type="checkbox"/></p>	<p>Primary NOAM VIP: Change Role to Secondary</p>	<p>Execute the command</p> <pre style="border: 1px solid black; padding: 2px;">\$ sudo top.setSecondary</pre> <p>Note: This step makes the primary NOAM to revert to DR-NOAM</p> <p>Execute the following command to verify the role was changed to secondary:</p> <pre style="border: 1px solid black; padding: 2px;">\$ sudo top.myrole</pre>								
<p>8 <input type="checkbox"/></p>	<p>New DR-NOAM VIP: Verify Replication</p>	<p>Navigate to Main Menu -> Status & Manage -> Server</p>  <p>It may take several minutes for replication; afterward the “DB” and “Reporting Status” columns should show “Normal”.</p> <table border="1" data-bbox="488 1430 943 1577"> <thead> <tr> <th>DB</th> <th>Reporting Status</th> </tr> </thead> <tbody> <tr> <td>Norm</td> <td>Norm</td> </tr> <tr> <td>Norm</td> <td>Norm</td> </tr> <tr> <td>Norm</td> <td>Norm</td> </tr> </tbody> </table>	DB	Reporting Status	Norm	Norm	Norm	Norm	Norm	Norm
DB	Reporting Status									
Norm	Norm									
Norm	Norm									
Norm	Norm									

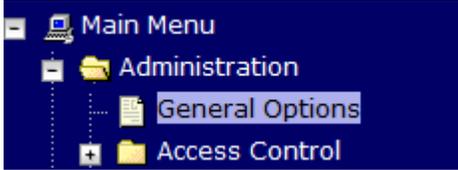
Procedure 20: Returning a Recovered Site to Primary

<p>9</p> <p><input type="checkbox"/></p>	<p>New DR-NOAM VIP: Re-enable the application.</p>	<p>Navigate to Main Menu -> Status & Manage -> Server</p>  <p>Select the row that has the formerly Primary NOAM server.</p> <p>Click the Restart button and then click the OK button.</p>  <p>Verify that “PROC” column now shows “Norm”.</p> 
<p>10</p> <p><input type="checkbox"/></p>	<p>To-Be-Primary NOAM VIP: Establish an SSH session</p>	<p>Login via SSH to the physical IP of the chosen primary DR-NOAM server as root(5.0) or admusr(6.0+) user.</p>
<p>11</p> <p><input type="checkbox"/></p>	<p>To-Be-Primary DSR NOAM VIP: Set To-be-Primary DSR NOAM to Primary</p>	<p>Execute the following command:</p> <pre>\$ sudo top.setPrimary</pre> <p>Note: This step makes the DSR take over as the Primary.</p> <p>Execute the command to verify the server role was changed to Primary:</p> <pre>\$ sudo top.myrole</pre> <p>System generates several replication and collection alarms as replication/collection links to/from former Primary NOAM servers becomes inactive.</p>

Procedure 20: Returning a Recovered Site to Primary

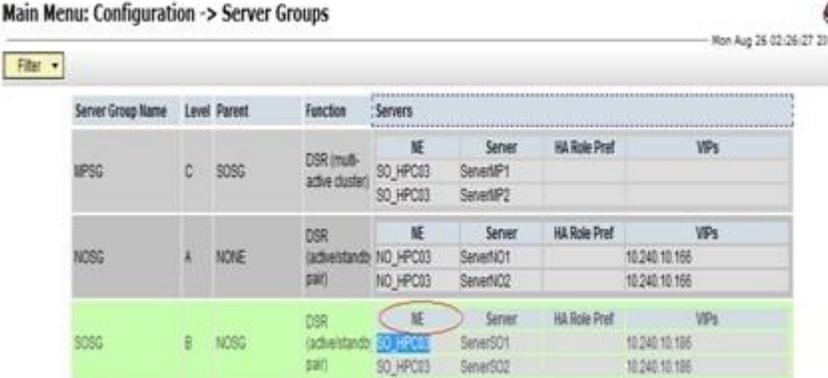
<p>12</p> <p><input type="checkbox"/></p>	<p>New Primary NOAM VIP: Re-enable the application.</p>	<p>Navigate to Main Menu -> Status & Manage -> Server</p>  <p>Select the row that has the active New-Primary NOAM server.</p> <p>Click the Restart button and then click the OK button.</p>  <p>Verify that “PROC” column now shows “Norm”.</p> 
<p>13</p> <p><input type="checkbox"/></p>	<p>New Primary NOAM VIP: Repeat on Second Recovered NOAM</p>	<p>Repeat Step 12 on the second recovered NOAM.</p> <p>Provisioning can now resume to the VIP of the new-Primary DSR.</p>
<p>14</p> <p><input type="checkbox"/></p>	<p>New Primary DSR NOAM VIP: Verify Replication</p>	<p>Monitor Main Menu -> Status & Manage -> Server screen at new-Primary DSR.</p> <p>It may take several minutes for replication; afterward the “DB” and “Reporting Status” columns should show “Normal”</p> <p>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:</p> <p>For DSR 5.0:</p> <pre>\$ pm.kill inetmerge</pre> <p>For DSR 6.0/7.0/7.1:</p> <pre>\$ sudo pm.kill inetmerge</pre>

Procedure 20: Returning a Recovered Site to Primary

16 <input type="checkbox"/>	New Primary NOAM VIP: Set Durability admin status to include DR-NOAM (Optional)	<p>If you reduced the durability status in procedure 19, raise durability admin status to its former value (NOAM + DRNOAM)</p> <p>Navigate to Main Menu -> Administration -> General Options</p>  <p>Set "durableAdminState" to 3(NO DRNOAM)</p>  <p>Click the OK button</p> <p>Now new DRNOAM DSR servers are part of provisioning database durability.</p>
--------------------------------	--	---

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

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

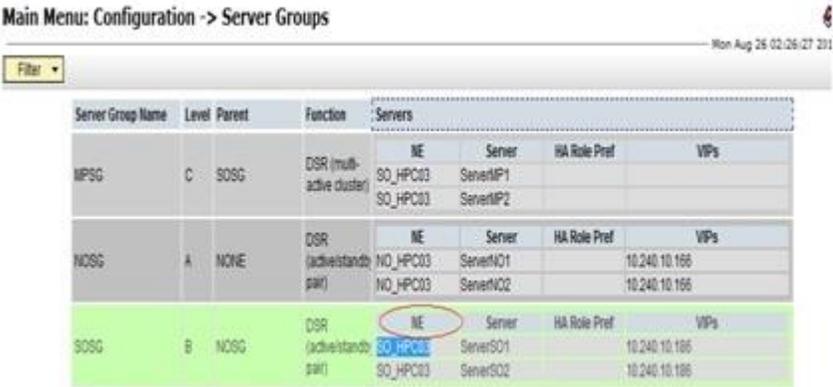
S T E P #	<p>The intent of this procedure is to inhibit A and B level replication on all C Level servers of this site</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix H. My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Active NOAM: Login	<p>Login to the Active NOAM server via SSH as root(5.0) or admusr(6.0+) user.</p>
2 <input type="checkbox"/>	Active NOAM: Inhibit replication on all C level Servers	<p>Execute the following command:</p> <pre style="border: 1px solid black; padding: 5px;">\$ for i in \$(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<SOAM Site_NE name of the site>'); do iset -finhibitRepPlans='A B' NodeInfo where "nodeName='\$i'; done</pre> <p>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.</p> <p>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.</p> 

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

3 <input type="checkbox"/>	Active NOAM: Verify Replication has been Inhibited.	<p>After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.</p> <p>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':</p> <p>Perform the following command:</p> <pre>\$ sudo iqt NodeInfo</pre> <p>Expected output:</p> <table border="1"><thead><tr><th>nodeId</th><th>nodeName</th><th>hostName</th><th>nodeCapability</th><th>inhibitRepPlans</th><th>siteId</th></tr></thead><tbody><tr><td>excludeTables</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>A1386.099</td><td>NO1</td><td>NO1</td><td>Active</td><td></td><td>NO_HPC03</td></tr><tr><td>B1754.109</td><td>SO1</td><td>SO1</td><td>Active</td><td></td><td>SO_HPC03</td></tr><tr><td>C2254.131</td><td>MP2</td><td>MP2</td><td>Active</td><td>A B</td><td>SO_HPC03</td></tr><tr><td>C2254.233</td><td>MP1</td><td>MP1</td><td>Active</td><td>A B</td><td>SO_HPC03</td></tr></tbody></table>	nodeId	nodeName	hostName	nodeCapability	inhibitRepPlans	siteId	excludeTables						A1386.099	NO1	NO1	Active		NO_HPC03	B1754.109	SO1	SO1	Active		SO_HPC03	C2254.131	MP2	MP2	Active	A B	SO_HPC03	C2254.233	MP1	MP1	Active	A B	SO_HPC03
nodeId	nodeName	hostName	nodeCapability	inhibitRepPlans	siteId																																	
excludeTables																																						
A1386.099	NO1	NO1	Active		NO_HPC03																																	
B1754.109	SO1	SO1	Active		SO_HPC03																																	
C2254.131	MP2	MP2	Active	A B	SO_HPC03																																	
C2254.233	MP1	MP1	Active	A B	SO_HPC03																																	

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

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

S T E P #	The intent of this procedure is to Un-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 step number. If this procedure fails, contact Appendix H . My Oracle Support (MOS) and ask for assistance.
1 <input type="checkbox"/>	Active NOAM: Login	Login to the Active NOAM server via SSH as root(5.0) or admusr(6.0+) user.
2 <input type="checkbox"/>	Active NOAM: Un-Inhibit replication on all C level Servers	Execute the following command: <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>\$ for i in \$(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<SOAM_Site_NE_namee>'); do iset -finhibitRepPlans='' NodeInfo where "nodeName='<i>\$i</i>'; done</pre> </div> <p>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.</p> <p>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.</p> 

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

3 <input type="checkbox"/>	Active NOAM: Verify Replication has been Inhibited.	<p>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.</p> <p>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':</p> <p>Perform the following command:</p> <pre>\$ sudo iqt NodeInfo</pre> <p>Expected output:</p> <table border="1"><thead><tr><th>nodeId</th><th>nodeName</th><th>hostName</th><th>nodeCapability</th><th>inhibitRepPlans</th><th>siteId</th><th>excludeTables</th></tr></thead><tbody><tr><td>A1386.099</td><td>NO1</td><td>NO1</td><td>Active</td><td></td><td>NO_HPC03</td><td></td></tr><tr><td>B1754.109</td><td>SO1</td><td>SO1</td><td>Active</td><td></td><td>SO_HPC03</td><td></td></tr><tr><td>C2254.131</td><td>MP2</td><td>MP2</td><td>Active</td><td></td><td>SO_HPC03</td><td></td></tr><tr><td>C2254.233</td><td>MP1</td><td>MP1</td><td>Active</td><td></td><td>SO_HPC03</td><td></td></tr></tbody></table>	nodeId	nodeName	hostName	nodeCapability	inhibitRepPlans	siteId	excludeTables	A1386.099	NO1	NO1	Active		NO_HPC03		B1754.109	SO1	SO1	Active		SO_HPC03		C2254.131	MP2	MP2	Active		SO_HPC03		C2254.233	MP1	MP1	Active		SO_HPC03	
nodeId	nodeName	hostName	nodeCapability	inhibitRepPlans	siteId	excludeTables																															
A1386.099	NO1	NO1	Active		NO_HPC03																																
B1754.109	SO1	SO1	Active		SO_HPC03																																
C2254.131	MP2	MP2	Active		SO_HPC03																																
C2254.233	MP1	MP1	Active		SO_HPC03																																

Appendix G. Workarounds for Issues not fixed in this Release

Issue	Associated PR	Workaround
Inetmerge alarm after force restore	222826	<p>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:</p>
Incorrect NodeID		<pre data-bbox="951 579 1425 680" style="border: 1px solid black; padding: 5px;">\$ top.myrole myNodeId=A3603.215 myMasterCapable=true</pre> <p>Then update the clusterId field in RecognizedAuthority table to have the same clustered from the above command:</p> <pre data-bbox="951 867 1425 1087" style="border: 1px solid black; padding: 5px;">\$ ivi RecognizedAuthority e.g. iload -ha -xU -frecNum -fclusterId -ftimestamp RecognizedAuthority \ <<'!!!!' 0 A3603 1436913769646 !!!!</pre>
Inetsync alarms after performing disaster recovery	222828	<p>Restart the Inetsync service on all affected servers using the following commands:</p> <pre data-bbox="951 1245 1425 1318" style="border: 1px solid black; padding: 5px;">\$ pm.set off inetsync \$ pm.set on inetsync</pre>
Active NO /etc/hosts file does not contain server aliases after force restore done. Note: This is no longer needed in DSR 7.1	222829,234357	<p>Release 5.0:</p> <p>From the recovered NOAM server command line, execute:</p> <pre data-bbox="951 1539 1425 1633" style="border: 1px solid black; padding: 5px;">\$ AppWorks AppWorks_AppWorks updateServerAliases <NO Host Name></pre>
Active NO cannot communicate with other Servers		

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

Appendix H. My Oracle Support (MOS)

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

When calling, there are multiple layers of menu 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.