

Oracle® Communications
Diameter Signaling Router
DSR C-Class Disaster Recovery Guide
Release 7.2/7.3
E69612 Revision 02

July 2016

ORACLE®

Copyright © 2016 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, except as set forth in an applicable agreement between you and Oracle.



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	5
List of Tables	5
List of Figures.....	6
1.0 Introduction.....	6
1.1 Purpose and Scope	6
1.2 References	7
1.3 Acronyms.....	8
1.4 Terminology.....	9
1.5 Optional Features	10
2.0 General Description	11
2.1 Complete Server Outage (All Servers).....	12
2.2 Partial server outage with one NOAM server intact and both SOAMs failed	12
2.3 Partial server outage with both NOAM servers failed and one SOAM server intact.....	12
2.4 Partial server outage with NOAM and one SOAM server intact.....	12
2.5 Partial Service outage with corrupt database.....	12
3.0 Procedure Overview.....	13
3.1 Required Materials	13
3.2 Disaster Recovery Strategy.....	14
4.0 Procedure Preparation	16
5.0 Disaster Recovery Procedure	18
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)	55
5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact)	87
5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)	111
5.1.5 Recovery Scenario 5 (Both NOAM servers failed with DR-NOAM available)	131
5.1.6 Recovery Scenario 6 (Database Recovery)	141
6.0 Resolving User Credential Issues after Database Restore.....	152
6.1 Restoring a Deleted User	152

6.2 Keeping a Restored user.....	153
6.3 Removing a Restored User	155
6.4 Restoring a Modified User	157
6.5 Restoring an Archive that does not contain a Current User	158
11. IDIH Disaster Recovery.....	161
Appendix A: DSR Database Backup.....	166
Appendix B: Recovering/Replacing Failed 3 rd Party Components (Switches, OAs)	171
Appendix C: Switching DR NOAM Site to Primary	175
Appendix D: Returning a Recovered Site to Primary.....	179
Appendix E: Inhibit A and B Level Replication on C-Level Servers.....	184
Appendix F: Un-Inhibit A and B Level Replication on C-Level Servers	186
Appendix G: Workarounds for Issues not fixed in this Release.....	188
Appendix H: Restore TVOE Configuration from Backup Media	189
Appendix I: Restore PMAC from Backup Media	193
Appendix J: Configure TVOE Hosts.....	202
Appendix K: Create NOAM/SOAM Virtual Machines.....	215
Appendix L: My Oracle Support (MOS)	223

List of Procedures

Procedure 1: Recovery Scenario 1	20
Procedure 2: Recovery Scenario 2	56
Procedure 3: Recovery Scenario 3	88
Procedure 4: Recovery Scenario 4	112
Procedure 5: Recovery Scenario 5	132
Procedure 6: Recovery Scenario 6 (Case 1)	141
Procedure 7: Recovery Scenario 6 (Case 2)	146
Procedure 8: Keep Restored User	153
Procedure 9: Remove the Restored User	155
Procedure 10: Restoring an Archive that does not Contain a Current User	158
Procedure 11: IDIH Disaster Recovery Preparation	161
Procedure 12: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)	163
Procedure 13: DSR Database Backup	166
Procedure 14: Recovering a Failed Aggregation Switch (Cisco 4948E/4948E-F)	171
Procedure 15: Recovering a Failed Enclosure Switch (Cisco 3020)	172
Procedure 16: Recovering a Failed Enclosure Switch (HP 6120XG , HP 6125XLG, HP 6125G)	173
Procedure 17: Recovering a Failed Enclosure OA	174
Procedure 18: Switching a DR NOAM Site to Primary	175
Procedure 19: Returning a Recovered Site to Primary	179
Procedure 20: Inhibit A and B Level Replication on C-Level Servers	184
Procedure 21: Un-Inhibit A and B Level Replication on C-Level Servers	186
Procedure 22: Restore TVOE Configuration from Backup Media	189
Procedure 23: Restore PMAC from Backup Media	193
Procedure 24: Restore PMAC from Backup Server	196
Procedure 25: Configure TVOE	202
Procedure 26: Create NOAM Guest VMs	215
Procedure 27: Create SOAM Guest VMs	219

List of Tables

Table 1 Acronyms	8
Table 2 Terminology	9
Table 3 Optional Features	10
Table 4. 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 7.2/7.3. 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 7.2/7.3. 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.

1.2 References

- [1] TPD Initial Product Manufacture, E54521-01
- [2] Platform 6.7/7.0 Configuration Procedure Reference, E53486
- [3] CPA Feature Activation Procedure, E58663
- [4] DSR Mediation Feature Activation Procedure, E58661
- [5] DSR FABR Feature Activation Procedure, E58664
- [6] DSR RBAR Feature Activation Procedure, E58665
- [7] DSR MAP-Diameter IWF Feature Activation Procedure, E58666
- [8] DSR 7.2/7.3 Software Installation and Configuration Procedure Part 2/2, E69409
- [9] DSR GLA Feature Activation Procedure, E58659
- [10] DSR 7.1/7.2/7.3 Hardware and Software Installation, E53488
- [11] PM&C 5.7/6.0 Disaster Recovery Guide, E54388
- [12] SDS 7.1/7.2/7.3 Disaster Recovery Guide. E59145
- [13] DSR 7.2/7.3 PCA Activation and Configuration, E67989
- [14] DSR DTLS Feature Activation Procedure, E67867

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 MAP-Diameter IWF Feature Activation Procedure, E58666
Policy and Charging Application (PCA)	DSR 7.2/7.3 PCA Activation and Configuration Procedure, E67989

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

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 (E69612-01) and hardcopies of all documents in the reference list
2. Hardcopy of all NAPD performed at the initial installation and network configuration of this 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 7.2/7.3 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*)
15. Latest RADIUS shared secret encryption key file backup (DpiKf.bin.encr)
16. List of activated and enabled features

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.

Note: Starting in DSR 7.2, NOAMs are now deployed using the fast deployment tool from the PMAC. In scenarios where both NOAMs are failed, this fast deployment file will be used. In scenarios where only one NOAM is failed, the fast deployment file is NOT used.

SUDO

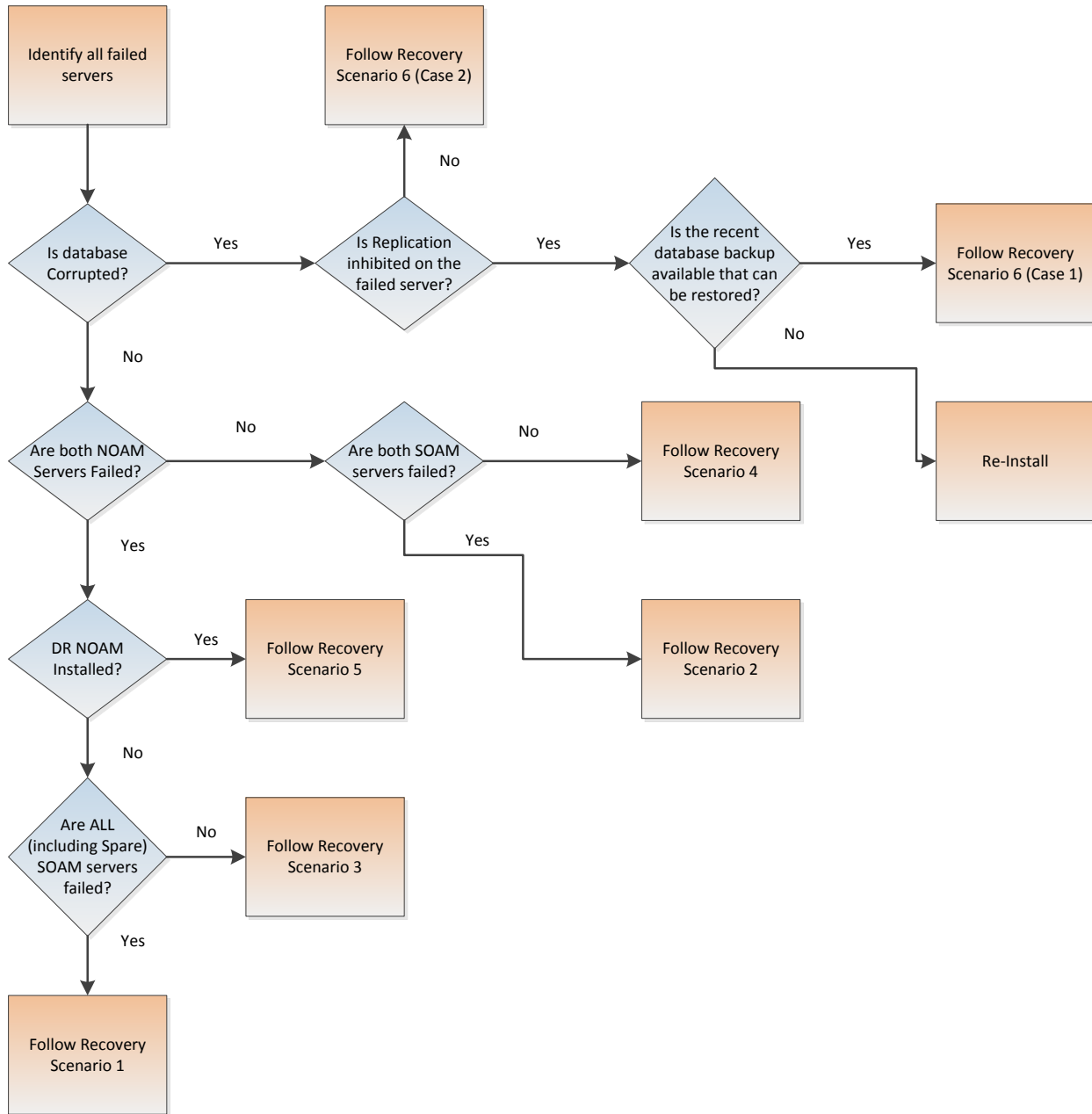
As a non-root user (***admusr***), many commands (*when run as admusr*) now require the use of '***sudo***'.

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 4**. Recovery Scenarios).
5. Execute appropriate recovery procedures (listed in **Table 4**. 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 4**. 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 4. 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 5.1.2 Recovery Scenario 2 (Partial Server Outage with one NOAM server intact and ALL SOAMs failed)
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 L: 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 ORACLE SUPPORT prime. Based on ORACLE SUPPORT'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 major activities are summarized as follows:

Recover Base Hardware and Software for all rack mount servers and blades:

- Recover the base hardware. (By replacing the hardware and executing hardware configuration procedures) - Reference [10] for the DSR base hardware installation procedure.

Recover the **NOAM** servers by recovering executing the fast deployment xml file.

- Recover the NOAM database
- Reconfigure the DSR application

Recover the **SOAM** servers by recovering base hardware/software and/or VM image:

- Recover the SOAM database
- Reconfigure the DSR Application

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

- Reconfigure the signaling interface and routes on the MPs, the DSR software will automatically reconfigure the signaling interface from the recovered database.
- Reference [8] 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. **Section 0** for IDIH disaster recovery and [12] for SDS 7.2/7.3 disaster recovery


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 Server 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 L: 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"/>	Replace Failed Equipment	HW vendor to replace the failed equipment
4 <input type="checkbox"/>	Recover PMAC and PMAC TVOE Host: Configure BIOS Settings and Update Firmware	<ol style="list-style-type: none"> 1. Configure and verify the BIOS settings by executing procedure “<i>Configure the RMS and Blade Server BIOS Settings</i>” from reference [10] 2. Verify and/or upgrade server firmware by executing procedure “<i>Upgrade Management Server Firmware</i>” from reference[10] Note: As indicated in [10], repeat for additional rack mount servers if equipped.
5 <input type="checkbox"/>	PMAC, TVOE Hosts, and Switch Recovery: Backups Available	<p>This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> 1. Restore the PMAC TVOE host backup by executing Appendix H: Restore TVOE Configuration from Backup Media <p>Restore the PMAC backup by executing</p> <ol style="list-style-type: none"> 2. Appendix I: Restore PMAC from Backup 3. Recover failed OAs, aggregation and enclosure switches, refer to Appendix B: Recovering/Replacing Failed 3rd Party Components (Switches, OAs)to recover failed OAs, aggregation, and enclosure switches 4. Verify/Update Blade server firmware by executing section “<i>Server Blades Installation Preparation</i>” from reference [10]. 5. Execute Install TVOE on ALL failed TVOE servers as needed by executing section “<i>Install TVOE on Blade Servers</i>” from reference [10]. 6. Restore the TVOE backup by executing Appendix H: Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers. <p style="text-align: center;">Proceed to Step 7</p>

Procedure 1: Recovery Scenario 1

<p>6 <input type="checkbox"/></p>	<p>PMAC, TVOE Hosts, and Switch Recovery: Backups NOT Available</p>	<p>This step assumes that TVOE and PMAC backups NOT are available, if the TVOE and PMAC have already been restored, skip this step</p> <ol style="list-style-type: none"> 1. Execute section “<i>Configure and IPM Management Server</i>” from reference [10]. 2. Execute section “<i>Install PM&C</i>” from reference [10]. 3. Execute section “<i>Configure Aggregation Switches</i>” from reference [10] to recover Cisco 4948 aggregation switches if needed. 4. Execute section “<i>Configure PM&C Application</i>” from reference [10]. 5. Execute section “<i>HP C-7000 Enclosure Configuration</i>” from reference [10] to recover and configure any failed OAs if needed. 6. Execute section “<i>Enclosure and Blades Setup</i>” from reference [10]. 7. Execute section “<i>Configure Enclosure Switches</i>” from reference [10] to recover enclosure switches if needed. 8. Verify/Update Blade server firmware by executing section “<i>Server Blades Installation Preparation</i>” from reference [10]. 9. Install and configure TVOE on failed rack mount servers by executing section “<i>Installing TVOE on Rack Mount Server(s)</i>” from reference [10]. 10. Install and configure TVOE on failed TVOE blade servers by executing section “<i>Install TVOE on Blade Servers</i>” from reference [10]. <p style="text-align: center;">Proceed to Next Step</p>
<p>7 <input type="checkbox"/></p>	<p>Execute Fast Deployment File for NOAMs</p>	<p>The backup fdconfig file used during the initial DSR 7.2/7.3 installation, this file will be available on the PMAC if a database backup was restored on the PMAC.</p> <p>If a backup fast deployment xml is NOT available, execute procedure “<i>Configure NOAM Servers</i>” from reference [8].</p> <p>If a backup fast deployment xml is already present on the PMAC, execute the following procedure:</p> <ol style="list-style-type: none"> 1) Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade has been performed since initial installation). 2) Execute the following commands: <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <pre>\$ cd /usr/TKLC/smac/etc \$ screen \$ sudo fdconfig config --file=<Created_FD_File>.xml</pre> </div>

Procedure 1: Recovery Scenario 1

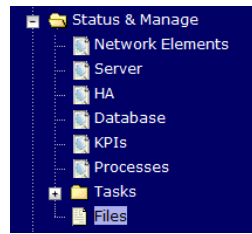
<p>8 <input type="checkbox"/></p>	<p>Obtain Latest Database Backup and Network Configuration Data.</p>	<ol style="list-style-type: none"> 1. Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. 2. Obtain most recent "RADIUS shared secret encryption key" file DpiKf.bin.encr from external backup sources. (Only when the RADIUS Key Revocation MOP has been executed on the system) <p>Note: Shared secret encryption key file needs to be handled by someone authorized to handle shared secrets information.</p> <p>Note: From required materials list in Section 3.1 <i>Required Materials</i>; use site survey documents and Network Element report (if available), to determine network configuration data.</p>
<p>9 <input type="checkbox"/></p>	<p>Execute DSR Installation Procedure for the First NOAM</p>	<ol style="list-style-type: none"> 1. Configure the first NOAM server by executing procedure "Configure the First NOAM NE and Server" from reference [8]. 2. Configure the NOAM server group by executing procedure "Configure the NOAM Server Group" from reference [8]. <p>Note: Use the backup copy of network configuration data and site surveys (Step 2)</p>
<p>10 <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

11
□

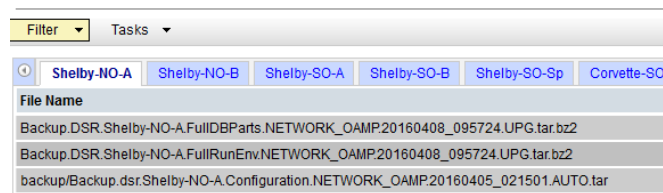
NOAM GUI:
Upload the
Backed up
Database File

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

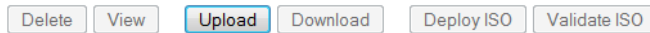


Select the Active NOAM server. The following screen will appear:

Main Menu: Status & Manage -> Files

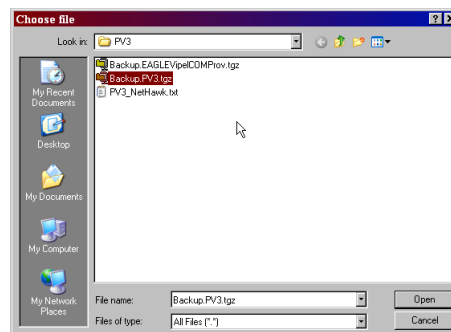
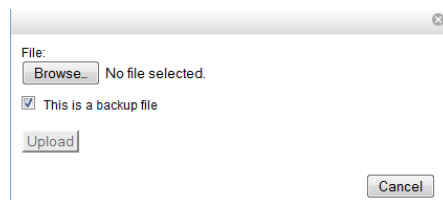


Click on **Upload** as shown below and select the file *“NO Provisioning and Configuration:”* file backed up after initial installation and provisioning.



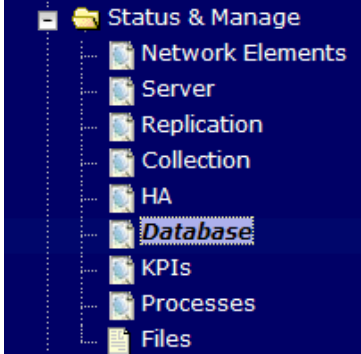

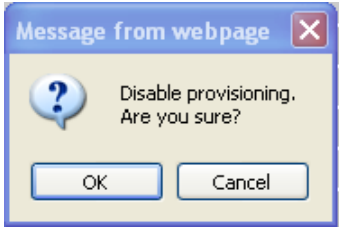
1 GB used (3.00%) of 34 GB available | System utilization: 1.8 GB (5.24%) of 34 GB available.

1. Click on **Browse** and locate the backup file
2. Check **This is a backup file** Box
3. 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

12 <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

13



NOAM GUI:
Verify the Archive Contents and Database Compatibility

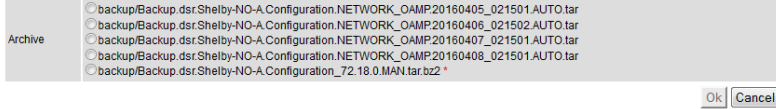
Select the **Active NOAM** server and click on the **Compare**.



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.

Database Compare

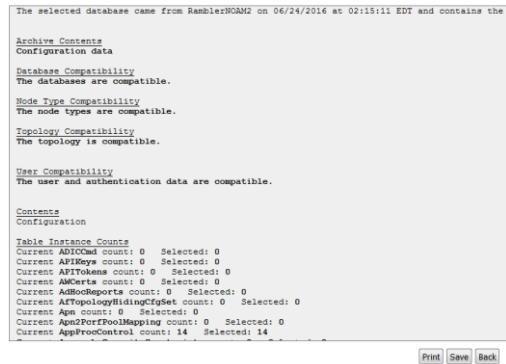
Select archive to compare on server: Shelby-NO-A



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 L: My Oracle Support (MOS)** and ask for assistance.

Database Archive Compare



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: USER AND AUTHENTICATION DATA may not be compatible

Note: These compatibility errors do not have an impact on the database restore.


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.

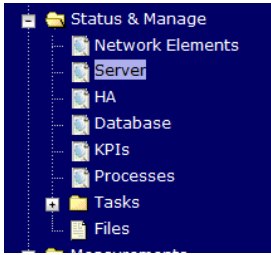
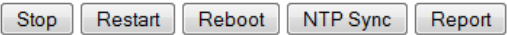
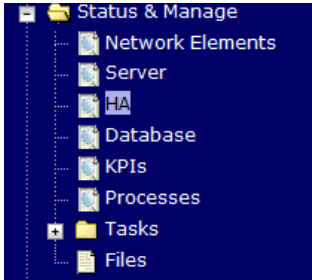
Procedure 1: Recovery Scenario 1

<p>14</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Restore the Database</p>	<p>Click on Main Menu->Status & Manage->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 data-bbox="487 462 1429 651"><p>Database Restore</p><p>Select archive to Restore on server: Shelby-NO-A</p><p>Archive</p><ul style="list-style-type: none"><input type="radio"/> backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP20160405_021501.AUTO.tar<input type="radio"/> backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP20160406_021502.AUTO.tar<input type="radio"/> backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP20160407_021501.AUTO.tar<input type="radio"/> backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP20160408_021501.AUTO.tar<input type="radio"/> backup/Backup.dsr.Shelby-NO-A.Configuration_72.18.0.MAN.tar.bz2 *<p>Ok 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 data-bbox="487 871 1429 1197"><p>Database Restore Confirm</p><p>Incompatible database selected</p><div data-bbox="495 934 1396 1102"><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><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 Force restore on blade07, despite compare errors.</p><p>Ok Cancel</p></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>
---	---	---

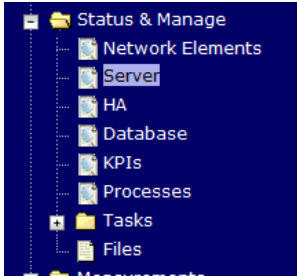
Procedure 1: Recovery Scenario 1

<p>15</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>16</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 restore 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>17</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Login</p>	<p>Login to the recovered Active NOAM via SSH terminal as <i>admusr</i> user.</p>

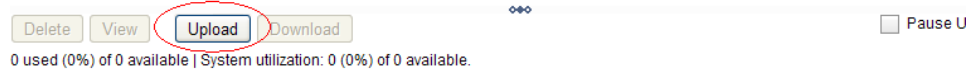
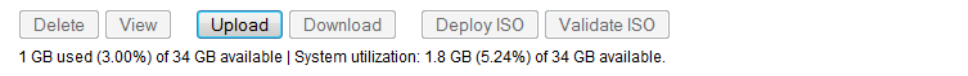
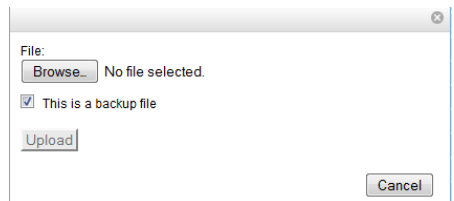
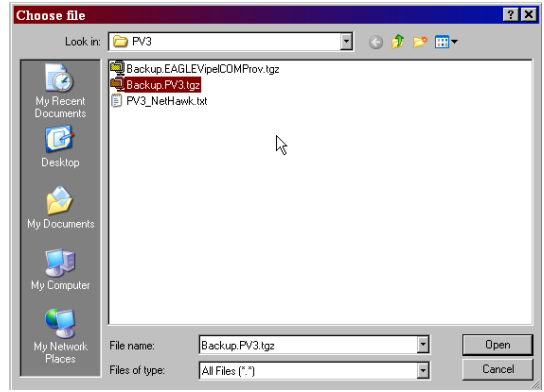
Procedure 1: Recovery Scenario 1

<p>18</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover Standby NOAM</p>	<p>1. Install the second NOAM server by executing procedure “<i>Configure the Second NOAM Server</i>”, steps 3-5, 7 from reference [8].</p> <p>Note: Execute step 6 if NetBackup is used.</p> <p>2. If NetBackup is used, execute procedure “<i>Install NetBackup Client</i>” from reference [8].</p>
<p>19</p> <p><input type="checkbox"/></p>	<p>Active NOAM: Correct the RecognizedAuth ority table</p>	<p>Establish an SSH session to the active NOAM, login as admusr.</p> <p>Execute the following command:</p> <pre style="background-color: #f0f0f0; padding: 5px;">\$ sudo top.setPrimary - Using my cluster: A1789 - New Primary Timestamp: 11/09/15 20:21:43.418 - Updating A1789.022: <DSR_NOAM_B_hostname> - Updating A1789.144: <DSR_NOAM_A_hostname></pre>
<p>20</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 standby NOAM server and click on Restart.</p> 
<p>21</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>


Procedure 1: Recovery Scenario 1

<p>25</p> <p><input type="checkbox"/></p>	<p>Create and IPM SOAM VMs</p>	<ol style="list-style-type: none"> 1. Execute procedure “<i>Create SOAM Guest VMs</i>” for the failed SOAM VMs and MP blades from reference [8]. 2. Execute procedure “<i>IPM Blades and VMs</i>” for the failed SOAM VMs and MP blades from reference [8]. 3. Execute procedure “<i>Install the Application</i>” for the failed SOAM VMs and MP blades from reference [8].
<p>26</p> <p><input type="checkbox"/></p>	<p>Recover Active SOAM Server</p>	<ol style="list-style-type: none"> 1. Execute procedure “Configure the SOAM Servers”, steps 1-3, and 5-8 from reference [8]. <p>Note: If you are using NetBackup, also execute step 10</p> <ol style="list-style-type: none"> 2. If you are using NetBackup, execute procedure “<i>Install NetBackup Client</i>” from reference [8].
<p>27</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 Active SOAM 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 1: Recovery Scenario 1

<p>28</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>0 used (0%) of 0 available System utilization: 0 (0%) of 0 available.</p>  <p>1 GB used (3.00%) of 34 GB available System utilization: 1.8 GB (5.24%) of 34 GB available.</p> <ol style="list-style-type: none"> 1. Click on Browse and locate the backup file 2. Check This is a backup file Box 3. Click on Open as shown below.   <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

29 <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="492 367 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

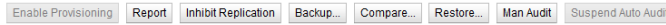
30

Recovered SOAM GUI:

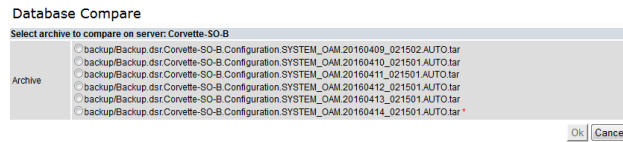
Verify the Archive Contents and Database Compatibility

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 L: 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.

Topology Compatibility

THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID

Note: USER AND AUTHENTICATION DATA may not be compatible

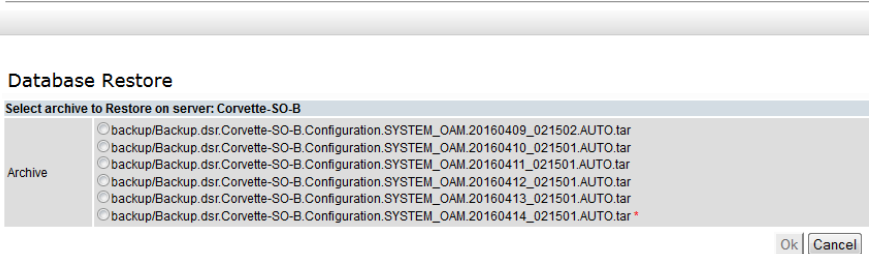
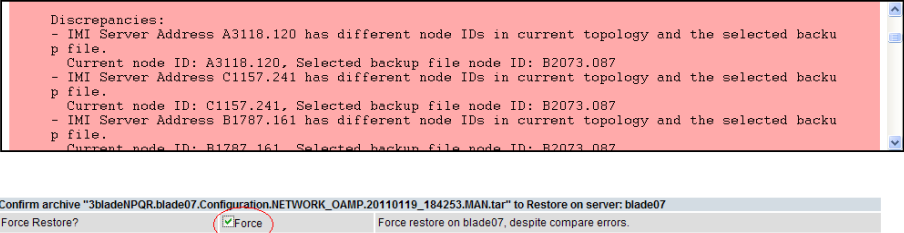
Note: These compatibility errors do not have an impact on the database restore.

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


E69612-02

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

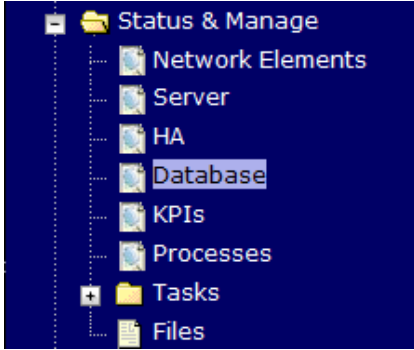
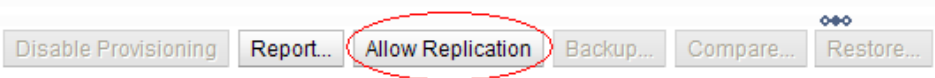
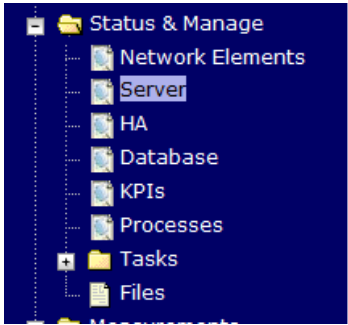
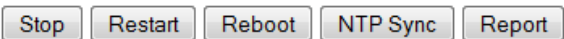
Procedure 1: Recovery Scenario 1

<p>31</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>Main Menu: Status & Manage -> Database [Restore]</p>  <p>Database Restore</p> <p>Select archive to Restore on server: Corvette-SO-B</p> <p>Archive</p> <ul style="list-style-type: none"> <input type="radio"/> backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160409_021502.AUTO.tar <input type="radio"/> backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160410_021501.AUTO.tar <input type="radio"/> backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160411_021501.AUTO.tar <input type="radio"/> backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160412_021501.AUTO.tar <input type="radio"/> backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160413_021501.AUTO.tar <input checked="" type="radio"/> backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160414_021501.AUTO.tar * <p>Ok 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 Force restore on blade07, despite compare errors.</p> <p>Ok 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>32</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 restore 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>

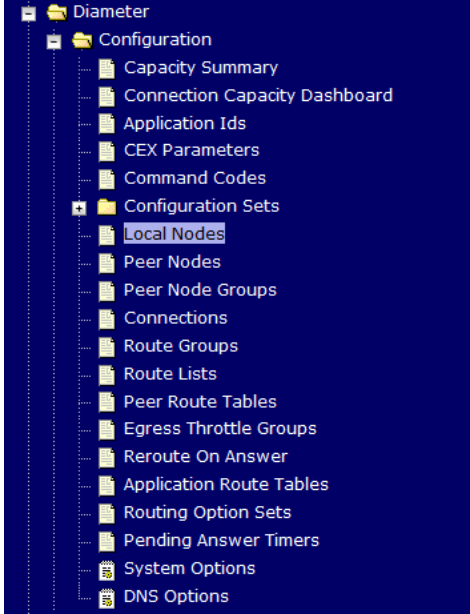
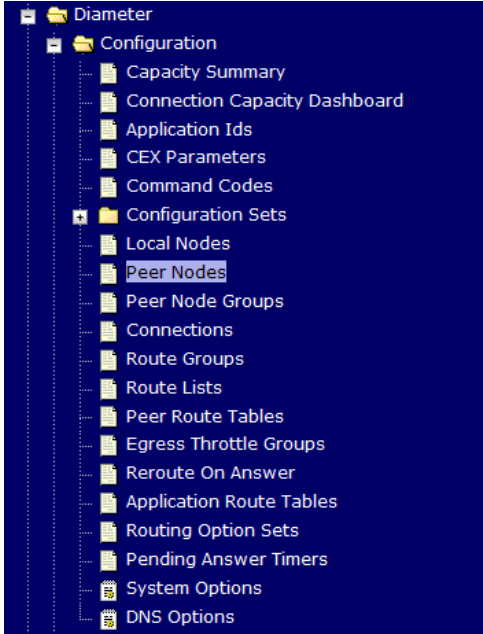
Procedure 1: Recovery Scenario 1

<p>33 □</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; margin: 5px 0;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>Login as the <i>guiadmin</i> user:</p> 
<p>34 □</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. Execute procedure “Configure the SOAM Servers”, steps 1-3, and 5-8 from reference [8]. <p>Note: If you are using NetBackup, also execute step 10</p> <ol style="list-style-type: none"> 2. If you are using NetBackup, execute procedure “Install NetBackup Client” from reference [8].

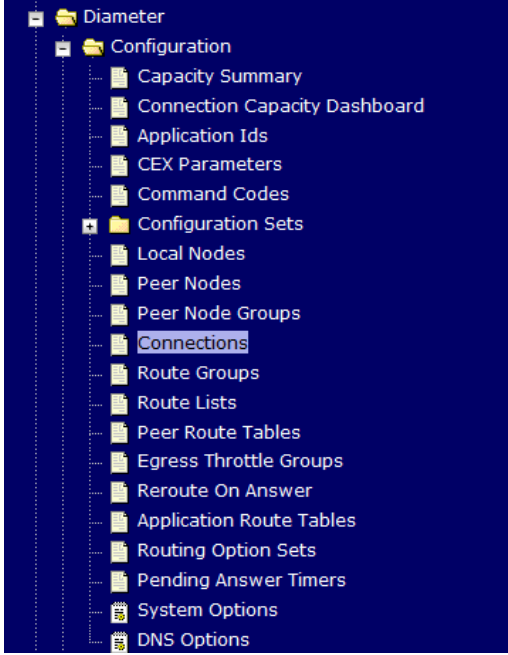
Procedure 1: Recovery Scenario 1

<p>35</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Start replication on the recovered standby SOAM</p>	<p>Un-Inhibit (<i>Start</i>) Replication to the recovered Standby SOAM</p> <p>Navigate to Status & Manage -> Database</p>  <p>Click on the Allow Replication button as shown below on the recovered standby SOAM server.</p> <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> 
<p>36</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 standby SOAM server and click on Restart.</p> 

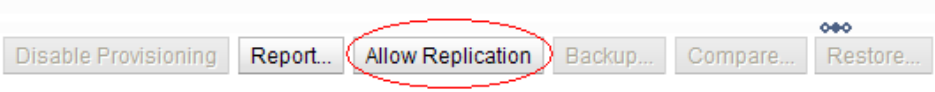
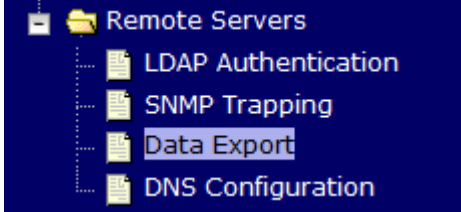
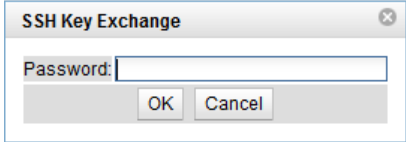
Procedure 1: Recovery Scenario 1

<p>37</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>38</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>

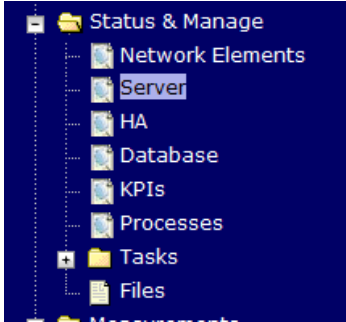
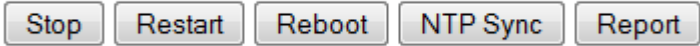
Procedure 1: Recovery Scenario 1

<p>39</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>40</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>

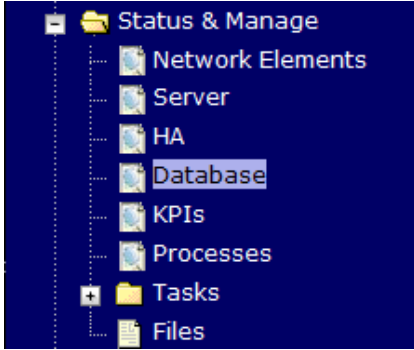
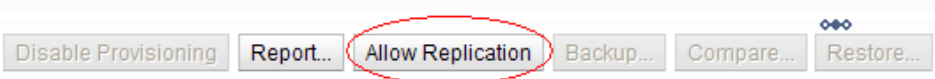
Procedure 1: Recovery Scenario 1

<p>41</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>42</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Perform Key Exchange with Export Server</p>	<p>Navigate to Main Menu -> Administration -> Remote Servers -> Data Export</p>  <p>Click on SSH Key Exchange at the bottom of the screen</p> <p>Enter the Password and press OK</p> 

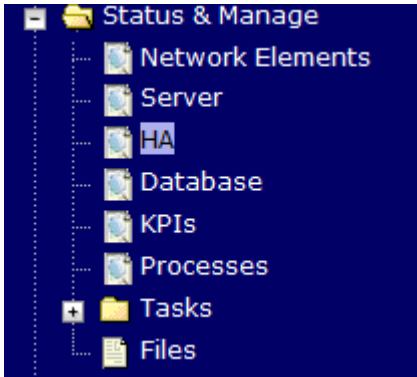
Procedure 1: Recovery Scenario 1

<p>43 <input type="checkbox"/></p>	<p>(PCA Only) Activate PCA Feature</p>	<p>If you are installing PCA, execute the applicable procedures (Added SOAM site activation or complete system activation) within Appendix A of [13] to activate PCA.</p> <p>Note: If not all SOAM sites are ready at this point, then you should repeat activation for each *new* SOAM site that comes online.</p>
<p>44 <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 Blade Servers</i>”, Steps 1, 7, 11-14, and 17 from reference [8].</p> <p>Note: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XML network.</p> <p>Repeat this step for any remaining failed MP servers.</p>
<p>45 <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 C-Level servers and click on Restart.</p> 

Procedure 1: Recovery Scenario 1

46 <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

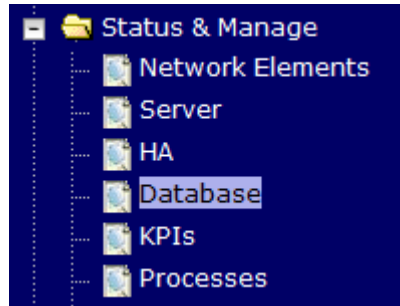
<p>47</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Set HA on all C-Level Servers</p>	<p>Navigate to Status & Manage -> HA</p>  <p>Click on Edit at the bottom of the screen</p> <p>For each server whose Max Allowed HA Role is set to Standby, set it to Active</p> <p>Press OK</p>
<p>48</p> <p><input 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>49</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 1: Recovery Scenario 1

50

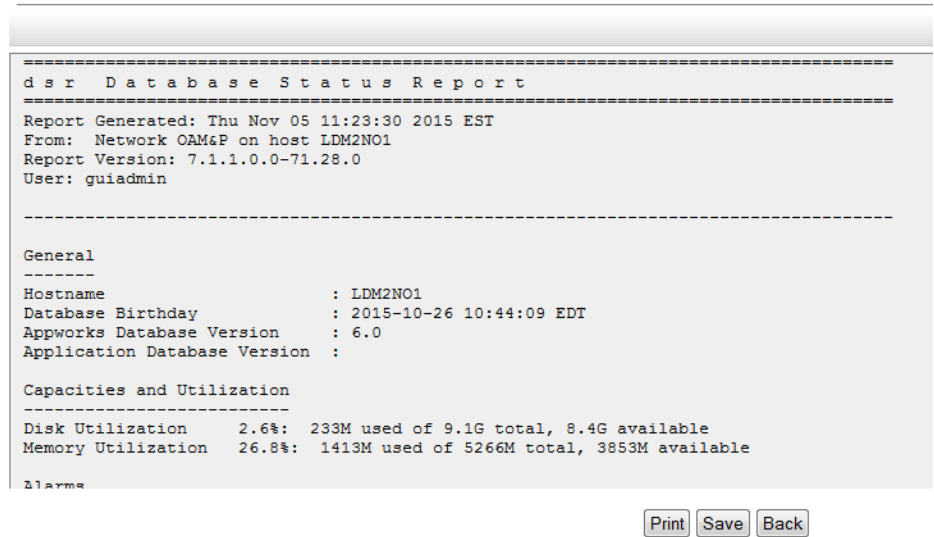
NOAM VIP GUI:
Fetch and Store
the database
Report for the
Newly Restored
Data and Save it

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]

A screenshot of the 'dsr Database Status Report' displayed in a web browser. The report is titled 'dsr Database Status Report' and is enclosed in a light gray box. The report content is as follows:

dsr Database Status Report

Report Generated: Thu Nov 05 11:23:30 2015 EST
From: Network OAM&P on host LDM2N01
Report Version: 7.1.1.0.0-71.28.0
User: guiadmin

General

Hostname : LDM2N01
Database Birthday : 2015-10-26 10:44:09 EDT
Appworks Database Version : 6.0
Application Database Version :

Capacities and Utilization

Disk Utilization 2.6%: 233M used of 9.1G total, 8.4G available
Memory Utilization 26.8%: 1413M used of 5266M total, 3853M available

Alarms

At the bottom right of the report box, there are three buttons: 'Print', 'Save', and 'Back'.

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

Procedure 1: Recovery Scenario 1

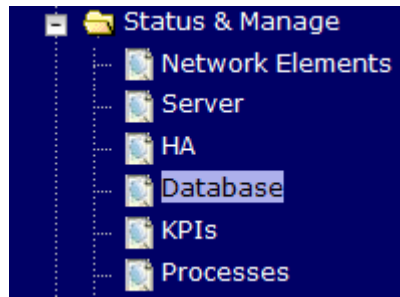
<p>51</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Verify Replication Between Servers.</p>	<p>Login to the Active NOAM via SSH terminal as <i>admusr</i>. Execute the following command:</p> <pre style="background-color: #f0f0f0; padding: 10px;">\$ sudo irepstat -m</pre> <p>Output like below shall be generated:</p> <pre style="background-color: #f0f0f0; padding: 10px;">-- Policy 0 ActStb [DbReplication] ----- ----- 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

52

NOAM VIP GUI:
Verify the
Database states

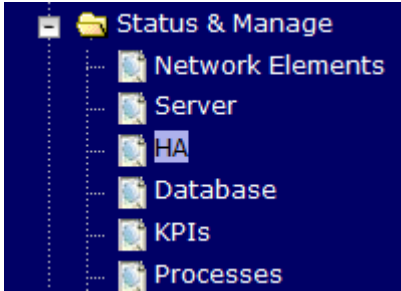
Click on **Main Menu->Status and Manager->Database**



Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below:

Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
NO_10303	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

Procedure 1: Recovery Scenario 1

<p>53</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Verify the HA Status</p>	<p>Click on Main Menu->Status and Manage->HA</p>  <p>Verify that the "OAM HA Role" for all rows is either "Active" or "Standby" as shown below.</p> <p>Main Menu: Status & Manage -> HA</p> <p>Filter <input type="text"/></p> <table border="1"> <thead> <tr> <th>Hostname</th> <th>OAM HA Role</th> <th>Application HA Role</th> <th>Max Allowed HA Role</th> </tr> </thead> <tbody> <tr><td>RamblerNOAM1</td><td>Standby</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerNOAM2</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerDRNOAM1</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerDRNOAM2</td><td>Standby</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerSOAM1</td><td>Standby</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerSOAM2</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerDAMP1</td><td>Active</td><td>Active</td><td>Active</td></tr> <tr><td>RamblerIPFE1</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerIPFE2</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerDAMP2</td><td>Standby</td><td>Active</td><td>Active</td></tr> </tbody> </table>	Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role	RamblerNOAM1	Standby	OOS	Active	RamblerNOAM2	Active	OOS	Active	RamblerDRNOAM1	Active	OOS	Active	RamblerDRNOAM2	Standby	OOS	Active	RamblerSOAM1	Standby	OOS	Active	RamblerSOAM2	Active	OOS	Active	RamblerDAMP1	Active	Active	Active	RamblerIPFE1	Active	OOS	Active	RamblerIPFE2	Active	OOS	Active	RamblerDAMP2	Standby	Active	Active
Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role																																											
RamblerNOAM1	Standby	OOS	Active																																											
RamblerNOAM2	Active	OOS	Active																																											
RamblerDRNOAM1	Active	OOS	Active																																											
RamblerDRNOAM2	Standby	OOS	Active																																											
RamblerSOAM1	Standby	OOS	Active																																											
RamblerSOAM2	Active	OOS	Active																																											
RamblerDAMP1	Active	Active	Active																																											
RamblerIPFE1	Active	OOS	Active																																											
RamblerIPFE2	Active	OOS	Active																																											
RamblerDAMP2	Standby	Active	Active																																											

Procedure 1: Recovery Scenario 1

54

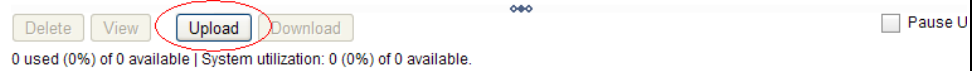


NOAM VIP GUI:
Upload the backed up RADIUS Key file (RADIUS Only)

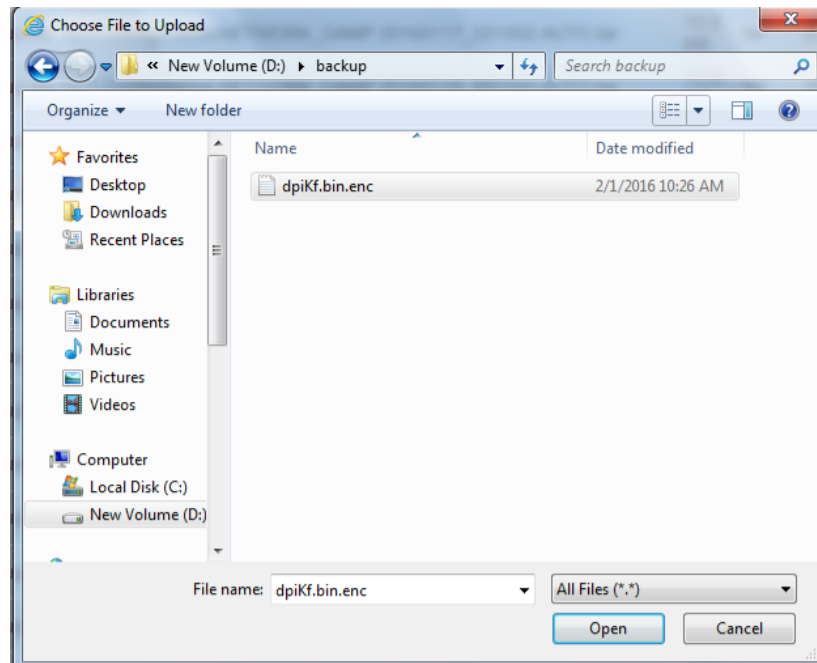
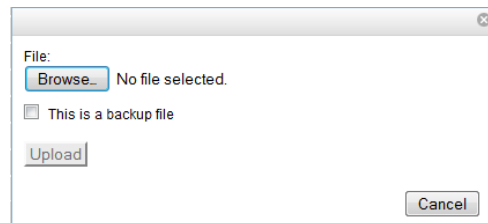
If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)

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

Select the Active NOAM server. The following screen will appear. Click on Upload as shown below and select the file "RADIUS shared secret encryption key:" file backed up after initial installation and provisioning or after key revocation execution.



Click on Browse and Locate the DpiKf.bin.encr 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 file. The file will be visible on the list of entries after the upload is complete.

Note: This file should be deleted from the operator's local servers as soon as key file is uploaded to Active NOAM server.

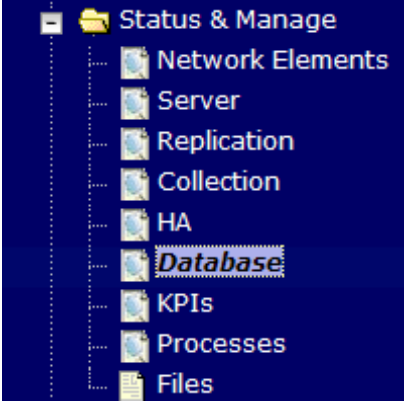

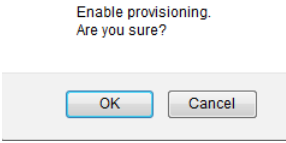
Procedure 1: Recovery Scenario 1

<p>55</p> <p><input type="checkbox"/></p>	<p>NOAM VIP: Copy and distribute RADIUS Key file on Active NOAM (RADIUS Only)-Part 1</p>	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Login to the Active NOAM VIP via SSH terminal as <i>admusr</i> user.</p> <p>Execute the following commands to copy the key file:</p> <pre>\$ cd /usr/TKLC/dpi/bin \$./sharedKrevo -decr \$ sudo rm /var/TKLC/db/filemgmt/<backed up key file name></pre> <p>Execute following command to check if all the servers in topology are accessible:</p> <pre>\$./sharedKrevo -checkAccess</pre> <pre>[admusr@NOAM-2 bin]\$./sharedKrevo -checkAccess FIPS integrity verification test failed. 1450723084: [INFO] 'NOAM-1' is accessible. FIPS integrity verification test failed. 1450723084: [INFO] 'SOAM-1' is accessible. FIPS integrity verification test failed. 1450723085: [INFO] 'SOAM-2' is accessible. FIPS integrity verification test failed. 1450723085: [INFO] 'IPFE' is accessible. FIPS integrity verification test failed. 1450723085: [INFO] 'MP-2' is accessible.</pre> <p>Note: If all the servers are not accessible then refer Appendix L: My Oracle Support (MOS).</p>
---	---	--

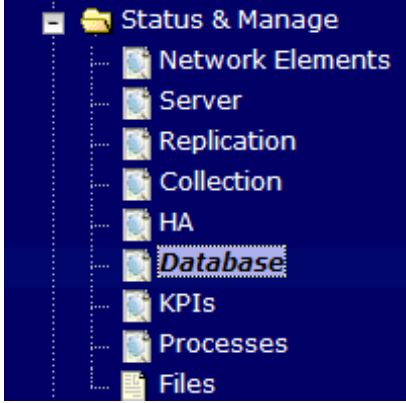
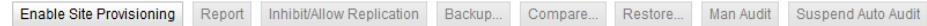

Procedure 1: Recovery Scenario 1

<p>56</p> <p>□</p>	<p>NOAM VIP: Copy and distribute RADIUS Key file on Active NOAM (RADIUS Only)-Part 2</p>	<p>Execute following command to distribute key file to all the servers in the topology :</p> <pre>\$./sharedKrevo -synchronize \$./sharedKrevo -updateData</pre> <p>Example output:</p> <pre>1450723210: [INFO] Key file on Active NOAM and IPFE are same. 1450723210: [INFO] NO NEED to sync key file to IPFE. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723210: [INFO] Key file on Active NOAM and MP-2 are same. 1450723210: [INFO] NO NEED to sync key file to MP-2. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723211: [INFO] Key file on Active NOAM and MP-1 are same. 1450723211: [INFO] NO NEED to sync key file to MP-1. [admusr@NOAM-2 bin]\$./sharedKrevo -updateData 1450723226: [INFO] Updating data on server 'NOAM-2' 1450723227: [INFO] Data updated to 'NOAM-2' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723228: [INFO] Updating data on server 'SOAM-2' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723230: [INFO] 1 rows updated on 'SOAM-2'... 1450723230: [INFO] Data updated to 'SOAM-2' [admusr@NOAM-2 bin]\$</pre> <p>Note: For any errors refer Appendix L: My Oracle Support (MOS).</p>
--------------------	---	---

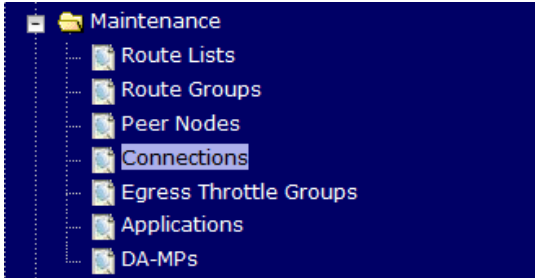
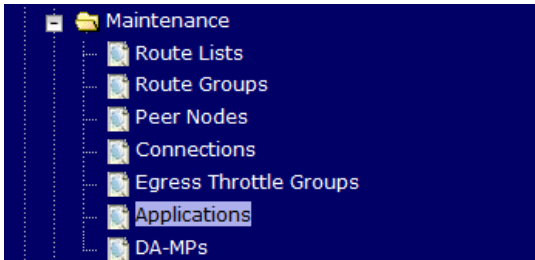
Procedure 1: Recovery Scenario 1

57 <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> 
--------------------------------	---	---

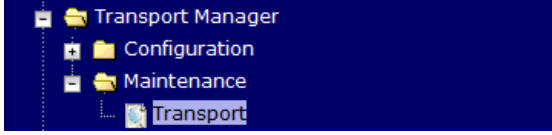

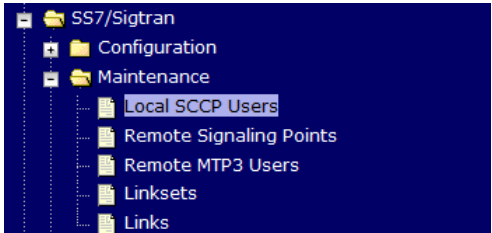

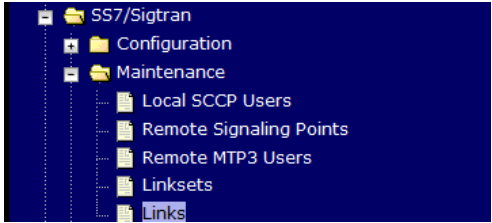

Procedure 1: Recovery Scenario 1

<p>58</p> <p><input type="checkbox"/></p>	<p>SOAM GUI: Enable Site Provisioning</p>	<p>Click on Main Menu->Status & Manage->Database</p>  <p>Enable Site Provisioning by clicking on Enable Site Provisioning button at the bottom of the screen as shown below.</p>  <p>A confirmation window will appear, press OK to enable Provisioning.</p> 
<p>59</p> <p><input type="checkbox"/></p>	<p>MP Servers: Disable SCTP Auth Flag</p>	<p>For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [14]</p> <p>Execute this procedure on all Failed MP Servers.</p>

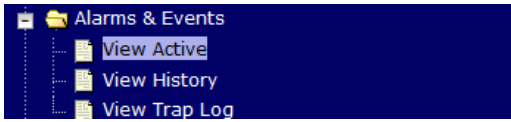
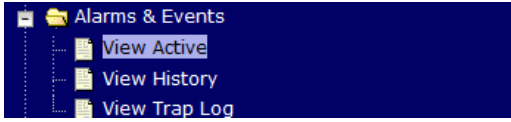
Procedure 1: Recovery Scenario 1

<p>60</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>61</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>62</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable Transports if Needed</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>63</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable MAPIWF application if needed</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>64</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable links if needed</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>65</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 L: My Oracle Support (MOS).</p>
<p>66</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 L: My Oracle Support (MOS).</p>
<p>67</p> <p><input type="checkbox"/></p>	<p>Restore GUI Usernames and Passwords</p>	<p>If applicable, Execute steps in Section 6.0 Resolving User Credential Issues after Database Restore to recover the user and group information restored.</p>
<p>68</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>
<p>69</p> <p><input type="checkbox"/></p>	<p>Recover IDIH</p>	<p>If IDIH were affected, refer to Section 0 to perform disaster recovery on IDIH.</p>

5.1.2 Recovery Scenario 2 (Partial Server Outage with one NOAM server intact and ALL 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.

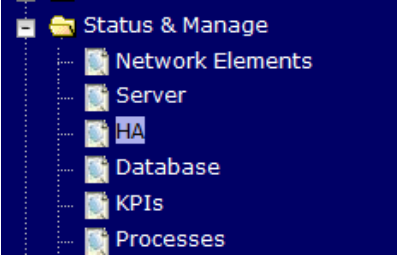
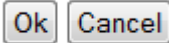
Recover any failed **SOAM and MP** servers by recovering base hardware and software.

- 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.

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 L: 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: 2px; 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;">  <p>Oracle System Login Fri Mar 20 12:29:52 2015 EDT</p> <hr style="width: 60%; margin: 0 auto;"/> <div style="border: 1px solid gray; padding: 10px; width: fit-content; 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: 60%; 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>

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>Replace Failed Equipment</p>	<p>HW vendor to replace the failed equipment</p>
<p>6</p> <p><input type="checkbox"/></p>	<p>RMS NOAM Failure: Configure BIOS Settings and Update Firmware</p>	<p>If the failed server is NOT a rack mount server, skip to step 10.</p> <ol style="list-style-type: none"> 1. Configure and verify the BIOS settings by executing procedure “<i>Configure the RMS and Blade Server BIOS Settings</i>” from reference [10] 2. Verify and/or upgrade server firmware by executing procedure “<i>Upgrade Management Server Firmware</i>” from reference[10] <p>Note: Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.</p>
<p>7</p> <p><input type="checkbox"/></p>	<p>RMS NOAM Failure: Backups Available</p>	<p>If the failed server is NOT a rack mount server, skip to step 10.</p> <p>This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> 1. Restore the TVOE backup by executing Appendix H: Restore TVOE Configuration from Backup Media <p>If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing</p> <ol style="list-style-type: none"> 2. Appendix I: Restore PMAC from Backup


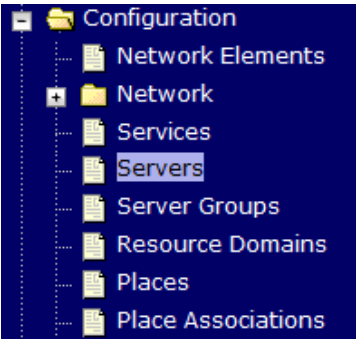
Procedure 2: Recovery Scenario 2

<p>8</p> <p><input type="checkbox"/></p>	<p>Recover Failed Aggregation/Enclosure Switches, and OAs</p>	<p>Recover failed OAs, aggregation and enclosure switches if needed.</p> <p>Backups Available:</p> <ol style="list-style-type: none"> 1. Refer to Appendix B: Recovering/Replacing Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches <p>Backups NOT Available:</p> <ol style="list-style-type: none"> 1. Execute section “<i>HP C-7000 Enclosure Configuration</i>” from reference [10] to recover and configure any failed OAs if needed. 2. Execute section “Configure Enclosure Switches” from reference [10] to recover enclosure switches if needed.
<p>9</p> <p><input type="checkbox"/></p>	<p>RMS NOAM Failure: Backups NOT Available</p>	<p>If the failed server is NOT a rack mount server, skip to step 10.</p> <p>This step assumes that TVOE and PMAC backups NOT are available, if the TVOE and PMAC have already been restored, skip this step.</p> <p>If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures:</p> <ol style="list-style-type: none"> 1. Section “<i>Configure and IPM Management Server</i>” from reference [10]. 2. Section “<i>Install PM&C</i>” from reference [10]. 3. Section “<i>Configure PM&C Application</i>” from reference [10]. <p>If the PMAC is NOT located on the same TVOE host as the failed NOAM, Execute the following sections/procedures</p> <ol style="list-style-type: none"> 1. Section “<i>Installing TVOE on Rack Mount Server(s)</i>” from reference [10].
<p>10</p> <p><input type="checkbox"/></p>	<p>HP-Class Blade Failure: Configure Blade Server iLO, Update Firmware/BIOS Settings</p>	<p>If the failed server is NOT an HP C-Class Blade, skip to step 14.</p> <ol style="list-style-type: none"> 1. Execute procedure “<i>Configure Blade Server iLO Password for Administrator Account</i>” from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing section “<i>Server Blades Installation Preparation</i>” from reference [10]

Procedure 2: Recovery Scenario 2

<p>11 <input type="checkbox"/></p>	<p>HP-Class Blade Failure: Backups Available</p>	<p>If the failed server is NOT an OAM type HP C-Class Blade, skip to step 14.</p> <p>This step assumes that TVOE backups are available, if backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> 1. Install and configure TVOE on failed TVOE blade servers by executing section “<i>Install TVOE on Blade Servers</i>” from reference [10]. 2. Restore the TVOE backup by executing Appendix H: Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers.
<p>12 <input type="checkbox"/></p>	<p>HP-Class Blade Failure: Backups NOT Available</p>	<p>If the failed server is NOT an OAM type HP C-Class Blade, skip to step 14.</p> <p>This step assumes that TVOE backups are NOT are available</p> <ol style="list-style-type: none"> 1. Install and configure TVOE on failed TVOE blade servers by executing section “<i>Install TVOE on Blade Servers</i>” from reference [10]. 2. Configure the NOAM and/or SOAM failed TVOE server blades by executing procedure “Configure SOAM TVOE Server Blades” from reference [8] <p>Note: Although the title of the procedure is related to SOAMs only, execute this procedure for any failed NOAMs located on TVOE server blades.</p>
<p>13 <input type="checkbox"/></p>	<p>Create VMs</p>	<p>Execute Appendix K: Create NOAM/SOAM Virtual Machines to create the NOAM and SOAM VMs on failed TVOE servers.</p>
<p>14 <input type="checkbox"/></p>	<p>IPM and Install DSR Application on Failed Guest/Servers</p>	<ol style="list-style-type: none"> 1. Execute procedure “<i>IPM Blades and VMs</i>” for the failed SOAM VMs and MP blades from reference [8]. 2. Execute procedure “<i>Install the Application</i>” for the failed SOAM VMs and MP blades from reference [8].
<p>15 <input type="checkbox"/></p>	<p>Install NetBackup Client (Optional)</p>	<p>If NetBackup is used execute procedure “<i>Install NetBackup Client</i>” from reference [8]</p>

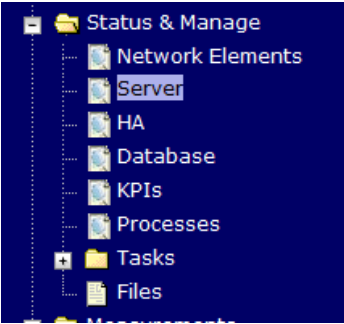
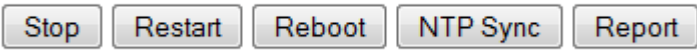
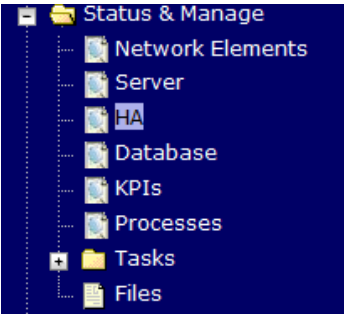
Procedure 2: Recovery Scenario 2

<p>16 □</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; 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>17 □</p>	<p>NOAM VIP GUI: Export the Initial Configuration</p>	<p>Navigate to Main Menu -> Configuration -> Servers.</p>  <p>From the GUI screen, select the failed NOAM server and then select Export to generate the initial configuration data for that server.</p> <div style="margin-top: 20px;"> <p>Insert Edit Delete Export Report</p> </div>

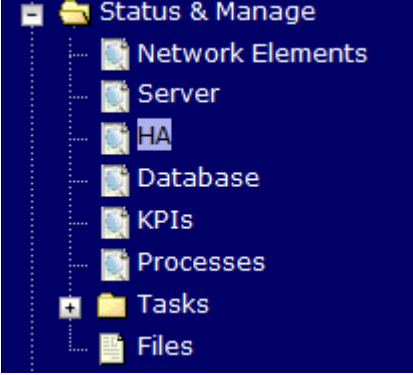
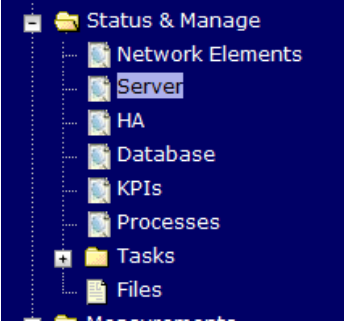
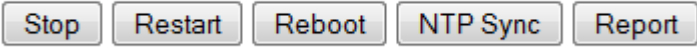
Procedure 2: Recovery Scenario 2

<p>18 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Copy Configuration File to Failed NOAM Server</p>	<p>Obtain a terminal session to the NOAM VIP, login as the admusr user. Execute the following command to configure the failed NOAM server:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<Failed_NOAM_Hostname>.sh admusr@<Failed_NOAM_control_IP_address>:/var/tmp/TKLCConfigData.sh</pre>
<p>19 <input type="checkbox"/></p>	<p>Failed NOAM Server: Verify the configuration was called and Reboot the Server</p>	<p>Establish an SSH session to the failed NOAM server, login as the admusr user.</p> <p>The automatic configuration daemon will look for the file named “TKLCConfigData.sh” in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server.</p> <p>Verify awpushcfg was called by checking the following file</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> <p>Verify the following message is displayed:</p> <pre style="border: 1px solid black; padding: 5px;">[SUCCESS] script completed successfully!</pre> <p>Now Reboot the Server:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo init 6</pre> <p>Wait for the server to reboot</p>
<p>20 <input type="checkbox"/></p>	<p>Failed NOAM Server: Configure Networking for Dedicated NetBackup Interface (Optional)</p>	<p>Note: You will only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.</p> <p>Obtain a terminal window to the failed NOAM server, logging in as the admusr.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP_Address> --netmask=<NO2_NetBackup_NetMask></pre> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NO1_NetBackup_Network_ID> --netmask=<NO2_NetBackup_NetMask> --gateway=<NO2_NetBackup_Gateway_IP_Address></pre>

Procedure 2: Recovery Scenario 2

<p>21 ☐</p>	<p>Failed NOAM Server: Verify Server Health</p>	<p>Execute the following command on the 2nd NOAM server and make sure that no errors are returned:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>
<p>22 ☐</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>23 ☐</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

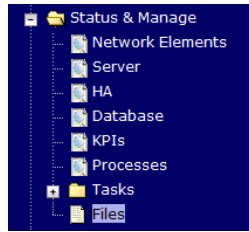
<p>26</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Set HA on SOAM Server</p>	<p>Navigate to Status & Manage -> HA</p>  <p>Click on Edit at the bottom of the screen</p> <p>Select the SOAM server, set it to Active</p> <p>Press OK</p>
<p>27</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Restart DSR application</p>	<p>Navigate to Main Menu->Status & Manage->Server,</p>  <p>Select the recovered SOAM server and click on Restart.</p> 

Procedure 2: Recovery Scenario 2

28
□

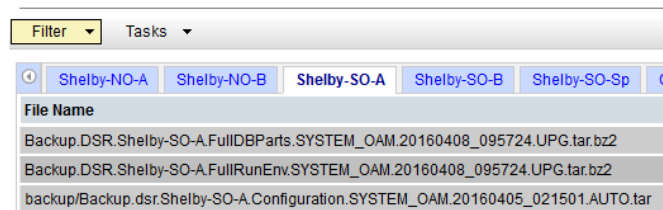
NOAM VIP GUI: Upload the backed up SOAM Database file

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

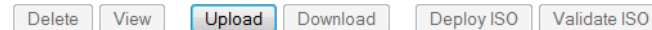


Select the Active SOAM server. The following screen will appear:

Main Menu: Status & Manage -> Files

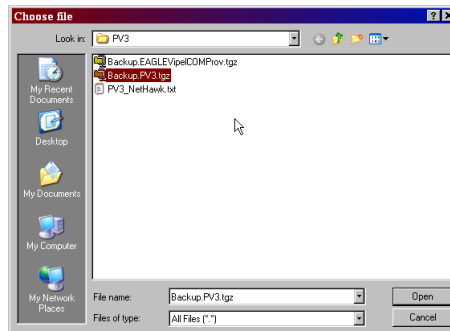
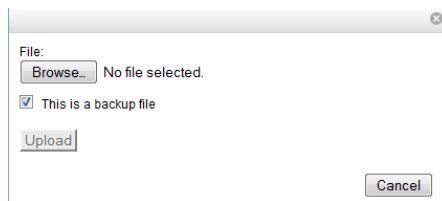


Click on **Upload** as shown below and select the file *“NO Provisioning and Configuration:”* file backed up after initial installation and provisioning.



1 GB used (3.00%) of 34 GB available | System utilization: 1.8 GB (5.24%) of 34 GB available.

1. Click on **Browse** and locate the backup file
2. Check **This is a backup file** Box
3. 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 2: Recovery Scenario 2

29



Recovered SOAM GUI:
Login

Establish a GUI session on the recovered SOAM server.
Open the web browser and enter a URL of:

`http://<Recovered_SOAM_IP_Address>`

Login as the *guiadmin* user:



Oracle System Login

Fri Mar 20 12:29:52 2015 EDT

Log In
Enter your username and password to log in

Username:

Password:

Change password

Welcome to the Oracle System Login.

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies.

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

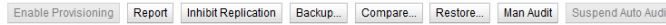
Procedure 2: Recovery Scenario 2

30

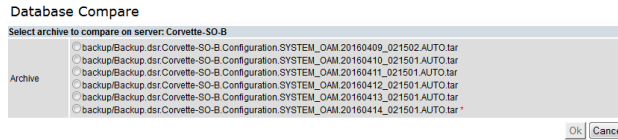
Recovered SOAM GUI:
Verify the Archive Contents and Database Compatibility

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 L: 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.

Topology Compatibility
THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID

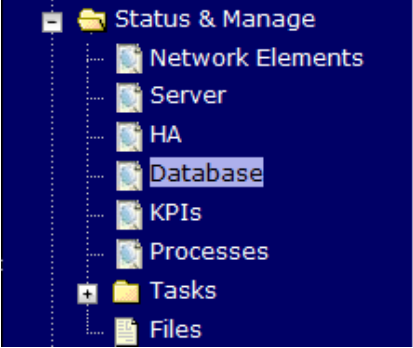
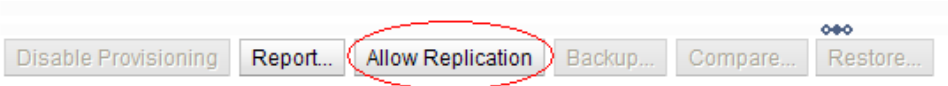
Note: USER AND AUTHENTICATION DATA may not be compatible

Note: These compatibility errors do not have an impact on the database restore.

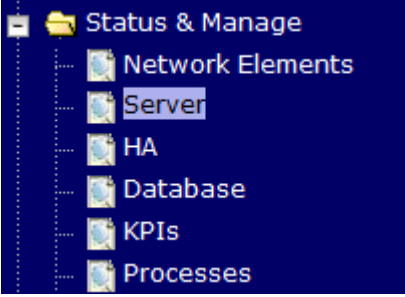
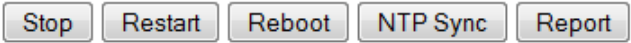
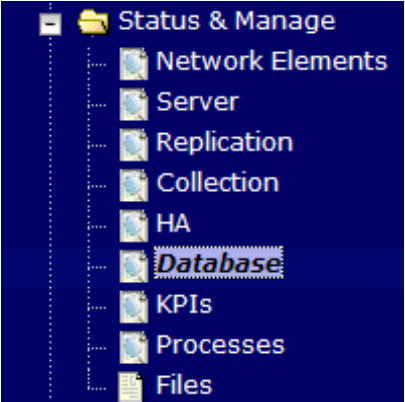
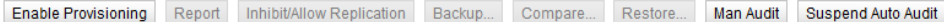
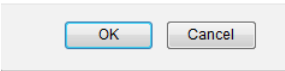
Procedure 2: Recovery Scenario 2

<p>31</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>Main Menu: Status & Manage -> Database [Restore]</p> <hr/> <p>Database Restore</p> <p>Select archive to Restore on server: Corvette-SO-B</p> <p>Archive</p> <ul style="list-style-type: none"> <input type="radio"/> backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160409_021502.AUTO.tar <input type="radio"/> backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160410_021501.AUTO.tar <input type="radio"/> backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160411_021501.AUTO.tar <input type="radio"/> backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160412_021501.AUTO.tar <input type="radio"/> backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160413_021501.AUTO.tar <input type="radio"/> backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160414_021501.AUTO.tar* <p style="text-align: right;"><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> <div style="border: 1px solid red; padding: 5px;"> <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> <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 Force restore on blade07, despite compare errors.</p> <p style="text-align: right;"><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>32</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 restore 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>

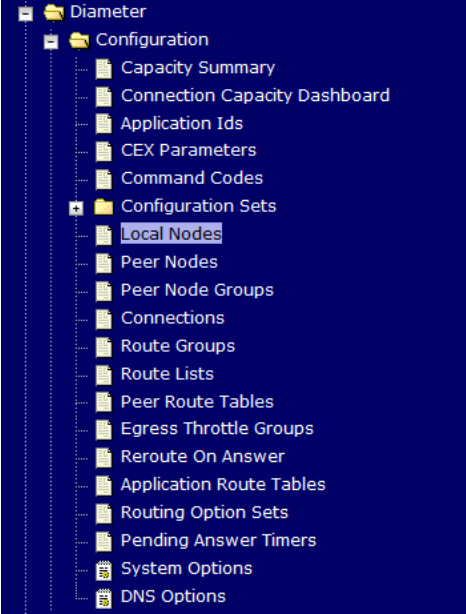
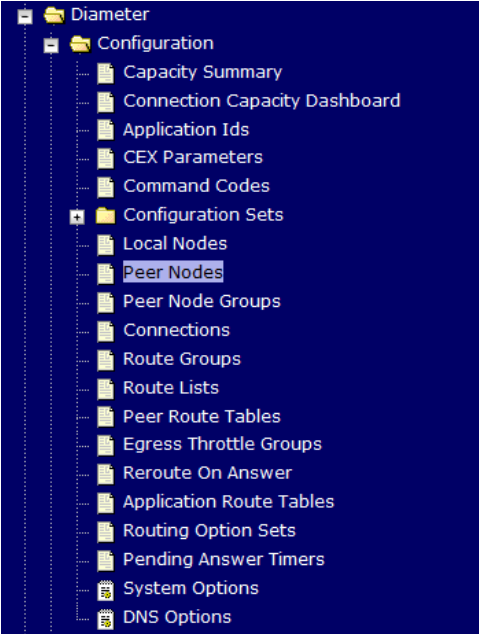
Procedure 2: Recovery Scenario 2

<p>33</p> <p><input type="checkbox"/></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. Execute procedure “Configure the SOAM Servers”, steps 1-3, and 5-8 from reference [8]. <p>Note: If you are using NetBackup, also execute step 10</p> <ol style="list-style-type: none"> 2. If you are using NetBackup, execute procedure “<i>Install NetBackup Client</i>” from reference [8].
<p>34</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Start replication on the recovered SOAMs</p>	<p>Un-Inhibit (<i>Start</i>) Replication to the remaining recovered SOAM servers</p> <p>Navigate to Status & Manage -> Database</p>  <p>Click on the Allow Replication button as shown below on the remaining recovered SOAM servers.</p> <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> 

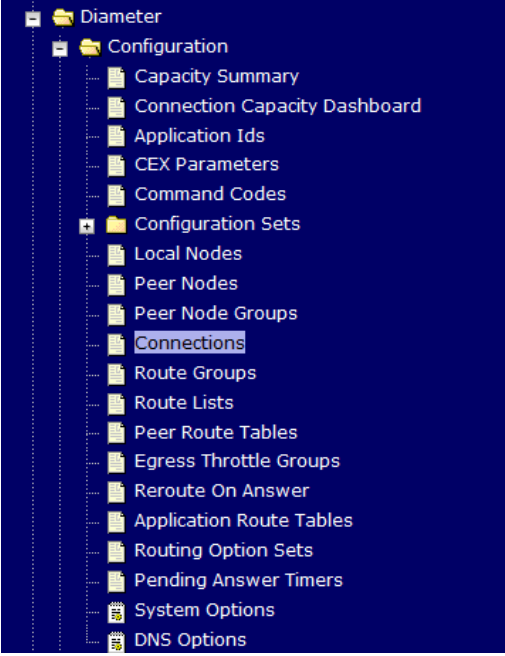
Procedure 2: Recovery Scenario 2

<p>35</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 remaining recovered SOAM servers and click on Restart.</p> 
<p>36</p> <p><input type="checkbox"/></p>	<p>SOAM GUI: Enable Provisioning</p>	<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> 

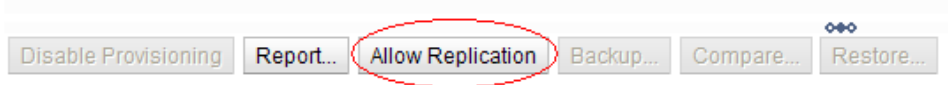
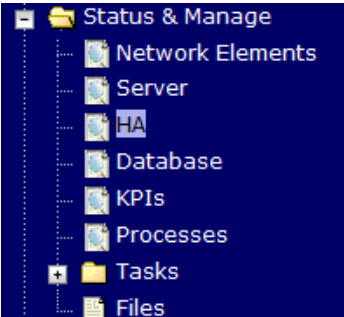
Procedure 2: Recovery Scenario 2

<p>37</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>38</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>

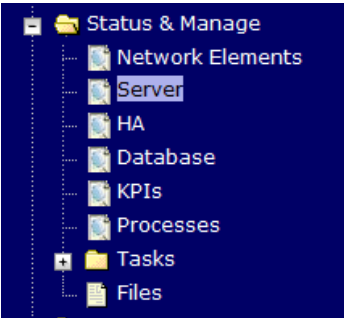
Procedure 2: Recovery Scenario 2

<p>39</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>
---	---	--

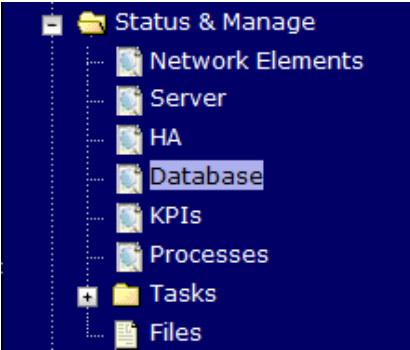
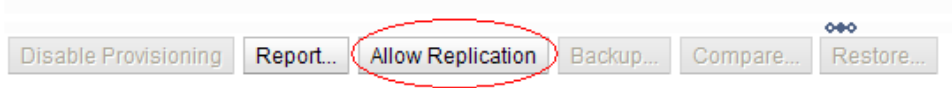
Procedure 2: Recovery Scenario 2

<p>40</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>41</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>

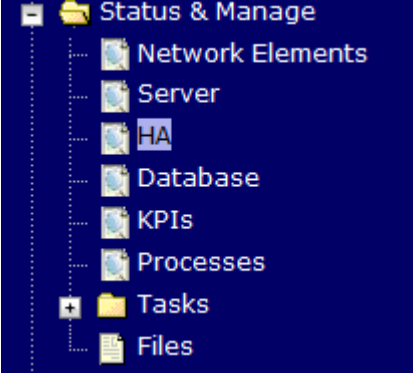
Procedure 2: Recovery Scenario 2

<p>42</p> <p><input type="checkbox"/></p>	<p>(PCA Only) Activate PCA Feature</p>	<p>If you are installing PCA, execute the applicable procedures (Added SOAM site activation or complete system activation) within Appendix A of [13] to activate PCA.</p> <p>Note: If not all SOAM sites are ready at this point, then you should repeat activation for each *new* SOAM site that comes online.</p>
<p>43</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 Blade Servers</i>”, Steps 1, 7, 11-14, and 17 from reference [8].</p> <p>Note: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.</p> <p>Repeat this step for any remaining failed MP servers.</p>
<p>44</p> <p><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 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 2: Recovery Scenario 2

45 <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 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

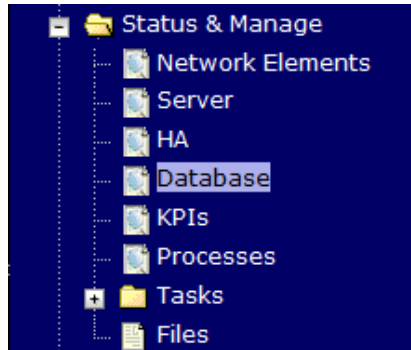
<p>46</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Set HA on all C-Level Servers</p>	<p>Navigate to Status & Manage -> HA</p>  <p>Click on Edit at the bottom of the screen</p> <p>For each server whose Max Allowed HA Role is set to Standby, set it to Active</p> <p>Press OK</p>
<p>47</p> <p><input 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>48</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>Note: While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:</p> <pre>iload#31000{S/W Fault}</pre>

Procedure 2: Recovery Scenario 2

49

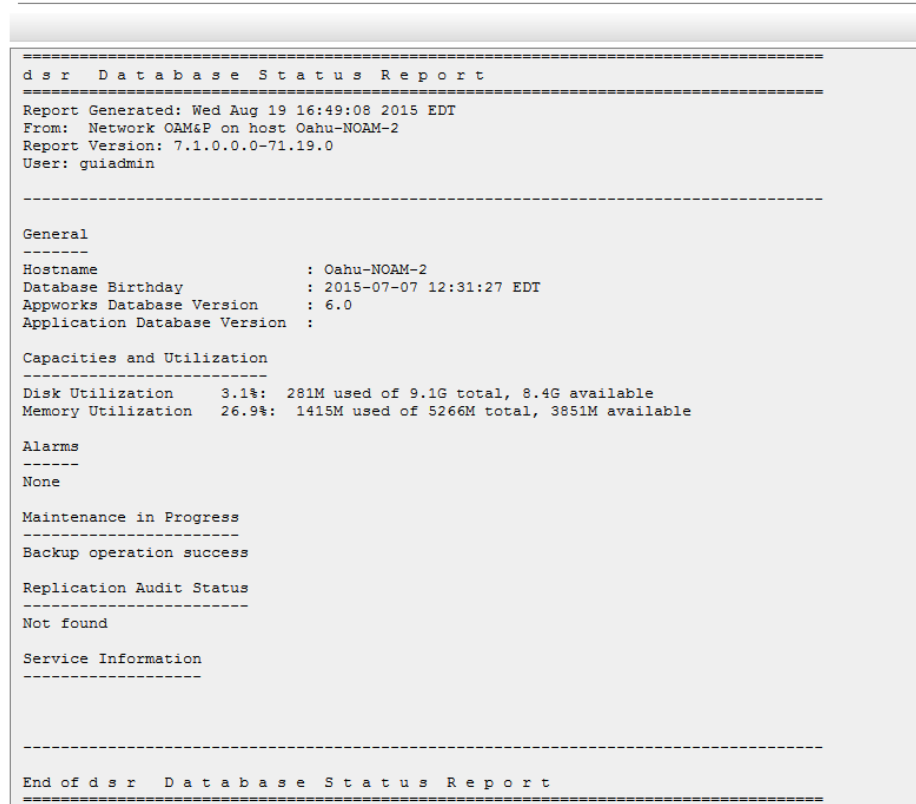
NOAM VIP
GUI: Fetch and Store the database Report for the Newly Restored Data and Save it

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]



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

Procedure 2: Recovery Scenario 2

50



ACTIVE NOAM:
Verify Replication Between Servers.

Login to the Active NOAM via SSH terminal as *admusr*.
Execute the following command:

```
$ sudo irepstat -m
```

Output like below shall be generated:

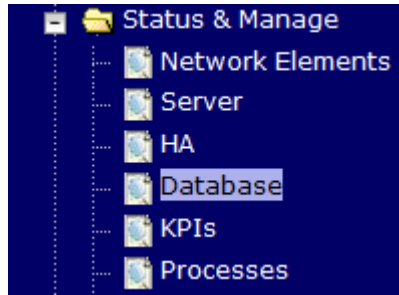
```
-- Policy 0 ActStb [DbReplication] -----  
-----  
Oahu-DAMP-1 -- Active  
  BC From Oahu-SOAM-2 Active      0  0.50 ^0.15%cpu 25B/s  A=me  
  CC To  Oahu-DAMP-2 Active      0  0.10  0.14%cpu 25B/s  A=me  
Oahu-DAMP-2 -- Stby  
  BC From Oahu-SOAM-2 Active      0  0.50 ^0.11%cpu 31B/s  
A=C3642.212  
  CC From Oahu-DAMP-1 Active      0  0.10 ^0.14 1.16%cpu 31B/s  
A=C3642.212  
Oahu-IPFE-1 -- Active  
  BC From Oahu-SOAM-2 Active      0  0.50 ^0.03%cpu 24B/s  
A=C3642.212  
Oahu-IPFE-2 -- Active  
  BC From Oahu-SOAM-2 Active      0  0.50 ^0.03%cpu 28B/s  
A=C3642.212  
Oahu-NOAM-1 -- Stby  
  AA From Oahu-NOAM-2 Active      0  0.25 ^0.03%cpu 23B/s  
Oahu-NOAM-2 -- Active  
  AA To  Oahu-NOAM-1 Active      0  0.25 1%R 0.04%cpu 61B/s  
  AB To  Oahu-SOAM-2 Active      0  0.50 1%R 0.05%cpu 75B/s  
Oahu-SOAM-1 -- Stby  
  BB From 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
```

Procedure 2: Recovery Scenario 2

51

NOAM VIP GUI: Verify the Database states

Click on **Main Menu->Status and Manager->Database**



Verify that the "OAM Max HA Role" is either "Active" or "Standby" for NOAM and SOAM and "Application Max HA Role" for MPs is "Active", and that the status is "Normal" as shown below:

Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
NO_10303	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	SO1	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	IPFE	MP	Active	OOS	Normal	0	Normal	Normal	Allowed	AutoInProg
SO_10303	SO2	System OAM	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg

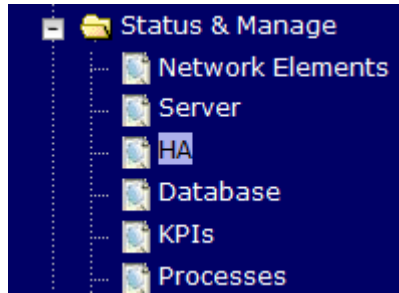
Procedure 2: Recovery Scenario 2

52

NOAM VIP
GUI: Verify the
 HA Status



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

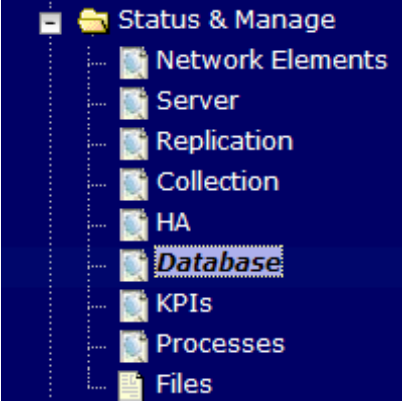
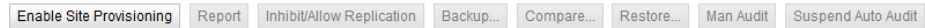
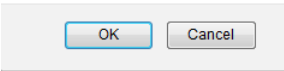
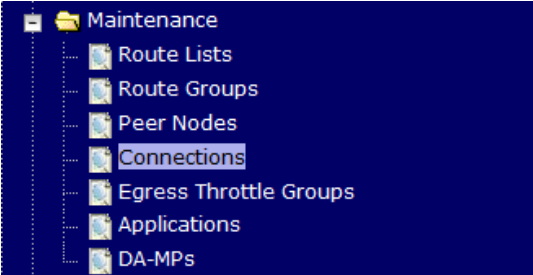
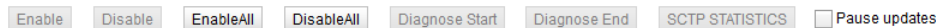


Verify that the “OAM HA Role” for all rows is either “Active” or “Standby” as shown below.

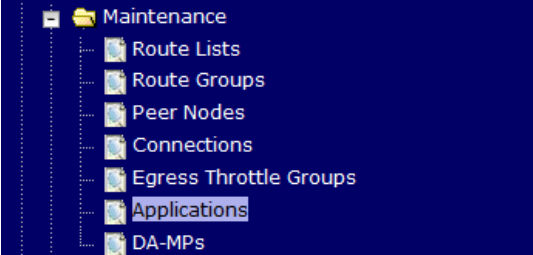
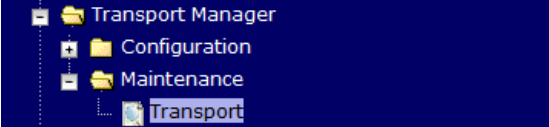
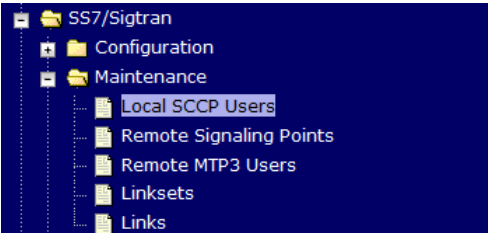
Main Menu: Status & Manage -> HA

Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role
RamblerNOAM1	Standby	OOS	Active
RamblerNOAM2	Active	OOS	Active
RamblerDRNOAM1	Active	OOS	Active
RamblerDRNOAM2	Standby	OOS	Active
RamblerSOAM1	Standby	OOS	Active
RamblerSOAM2	Active	OOS	Active
RamblerDAMP1	Active	Active	Active
RamblerPFE1	Active	OOS	Active
RamblerPFE2	Active	OOS	Active
RamblerDAMP2	Standby	Active	Active

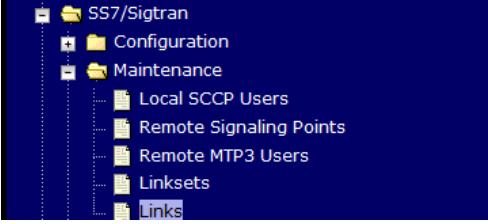

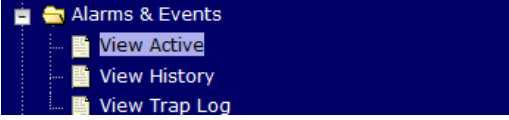
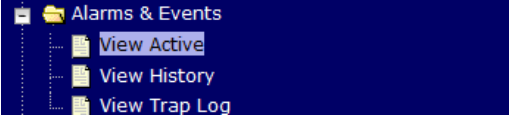
Procedure 2: Recovery Scenario 2

<p>53</p> <p><input type="checkbox"/></p>	<p>SOAM GUI: Enable Site Provisioning</p>	<p>Click on Main Menu->Status & Manage->Database</p>  <p>Enable Site Provisioning by clicking on Enable Site Provisioning button at the bottom of the screen as shown below.</p>  <p>A confirmation window will appear, press OK to enable Provisioning.</p> 
<p>54</p> <p><input type="checkbox"/></p>	<p>MP Servers: Disable SCTP Auth Flag</p>	<p>For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [14]</p> <p>Execute this procedure on all Failed MP Servers.</p>
<p>55</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 2: Recovery Scenario 2

<p>56</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><input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="checkbox"/> Pause updates</p>
<p>57</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable Transports if Needed</p>	<p>Navigate to Main Menu->Transport Manager -> Maintenance -> Transport</p>  <p>Select each transport and click on the Enable button</p> <p><input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Block"/></p> <p>Verify that the Operational Status for each transport is Up.</p>
<p>58</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable MAPIWF application if needed</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><input type="button" value="Enable"/> <input type="button" value="Disable"/></p> <p>Verify that the SSN Status is Enabled.</p>

Procedure 2: Recovery Scenario 2

<p>59</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable links if needed</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>60</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 L: My Oracle Support (MOS).</p>
<p>61</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>

Procedure 2: Recovery Scenario 2

<p>62</p> <p><input type="checkbox"/></p>	<p>NOAM VIP: Verify all servers in Topology are accessible (RADIUS Only)</p>	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Establish an SSH session to the NOAM VIP. Login as <i>admusr</i>.</p> <p>Execute following commands to check if all the servers in the Topology are accessible :</p> <pre>\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -checkAccess</pre> <p>Example Output:</p> <pre>[admusr@NOAM-2 bin]\$./sharedKrevo -checkAccess FIPS integrity verification test failed. 1450723403: [INFO] 'NOAM-1' is accessible. FIPS integrity verification test failed. 1450723403: [INFO] 'SOAM-1' is accessible. FIPS integrity verification test failed. 1450723403: [INFO] 'SOAM-2' is accessible. FIPS integrity verification test failed. 1450723404: [INFO] 'IPFE' is accessible. FIPS integrity verification test failed. 1450723404: [INFO] 'MP-2' is accessible. FIPS integrity verification test failed. 1450723404: [INFO] 'MP-1' is accessible. [admusr@NOAM-2 bin]\$</pre>
---	---	---

Procedure 2: Recovery Scenario 2

<p>63</p> <p><input type="checkbox"/></p>	<p>NOAM VIP: Copy key file to all the servers in Topology (RADIUS Only)</p>	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Execute following commands to check if existing Key file on Active NOAM (The NOAM which is intact and was not recovered) server is valid :</p> <pre>\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -validate</pre>  <pre>[admsr@NOAM-2 bin]\$./sharedKrevo -validate FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723458: [INFO] Key file for 'NOAM-1' is valid 1450723458: [INFO] Key file for 'NOAM-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723459: [INFO] Key file for 'SOAM-1' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723460: [INFO] Key file for 'SOAM-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723461: [INFO] Key file for 'IPFE' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723461: [INFO] Key file for 'MP-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723462: [INFO] Key file for 'MP-1' is valid [admsr@NOAM-2 bin]\$</pre> <p>If output of above command shows that the existing key file is not valid, contact Appendix L: My Oracle Support (MOS)</p> <p>Execute following command to copy the key file to all the servers in the Topology:</p> <pre>\$./sharedKrevo -synchronize</pre>  <pre>\$./sharedKrevo -synchronize FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722733: [INFO] Synched key to IPFE FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722734: NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722735: [INFO] Synched key to MP-2 FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722736: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722738: [INFO] Synched key to MP-1 [admsr@NOAM-2 bin]\$</pre> <pre>\$./sharedKrevo -updateData</pre>  <pre>[admsr@NOAM-1 bin]\$./sharedKrevo -updateData 1450203518: [INFO] Updating data on server 'NOAM-1' 1450203519: [INFO] Data updated to 'NOAM-1' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203520: [INFO] Updating data on server 'SOAM-2' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203522: [INFO] 1 rows updated on 'SOAM-2'... 1450203522: [INFO] Data updated to 'SOAM-2'</pre> <p>Note: If any errors are present, stop and contact Appendix L: My Oracle Support (MOS)</p>
---	--	---

Procedure 2: Recovery Scenario 2

64 <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:
65 <input type="checkbox"/>	Recover IDIH	If IDIH were affected, refer to Section 0 to perform disaster recovery on IDIH.

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 L: 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"/>	Replace Failed Equipment	HW vendor to replace the failed equipment
4 <input type="checkbox"/>	RMS NOAM Failure: Configure BIOS Settings and Update Firmware	<p style="text-align: center;">If the failed server is NOT a rack mount server, skip to step 7.</p> <ol style="list-style-type: none"> 1. Configure and verify the BIOS settings by executing procedure “<i>Configure the RMS and Blade Server BIOS Settings</i>” from reference [10] 2. Verify and/or upgrade server firmware by executing procedure “<i>Upgrade Management Server Firmware</i>” from reference[10] <p style="text-align: center;">Note: Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.</p>
5 <input type="checkbox"/>	RMS NOAM Failure: Backups Available	<p style="text-align: center;">If the failed server is NOT a rack mount server, skip to step 7.</p> <p>This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> 1. Restore the TVOE backup by executing Appendix H: Restore TVOE Configuration from Backup Media <p>If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing</p> <ol style="list-style-type: none"> 2. Appendix I: Restore PMAC from Backup


Procedure 3: Recovery Scenario 3

<p>6</p> <p><input type="checkbox"/></p>	<p>Recover Failed Aggregation/ Enclosure Switches, and OAs</p>	<p>Recover failed OAs, aggregation and enclosure switches if needed.</p> <p>Backups Available:</p> <ol style="list-style-type: none"> 1. Refer to Appendix B: Recovering/Replacing Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches <p>Backups NOT Available:</p> <ol style="list-style-type: none"> 1. Execute section “<i>HP C-7000 Enclosure Configuration</i>” from reference [10] to recover and configure any failed OAs if needed. 2. Execute section “Configure Enclosure Switches” from reference [10] to recover enclosure switches if needed.
<p>7</p> <p><input type="checkbox"/></p>	<p>RMS NOAM Failure: Backups NOT Available</p>	<p>If the failed server is NOT a rack mount server, skip to step 7.</p> <p>This step assumes that TVOE and PMAC backups NOT are available, if the TVOE and PMAC have already been restored, skip this step.</p> <p>If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures:</p> <ol style="list-style-type: none"> 1. Section “<i>Configure and IPM Management Server</i>” from reference [10]. 2. Section “<i>Install PM&C</i>” from reference [10]. 3. Section “<i>Configure PM&C</i>” from reference [10]. <p>If the PMAC is NOT located on the same TVOE host as the failed NOAM, Execute the following sections/procedures</p> <ol style="list-style-type: none"> 1. Section “<i>Installing TVOE on Rack Mount Server(s)</i>” from reference [10].
<p>8</p> <p><input type="checkbox"/></p>	<p>HP-Class Blade Failure: Configure Blade Server iLO, Update Firmware/BIOS Settings</p>	<p>If the failed server is NOT an HP C-Class Blade, skip to step 11.</p> <ol style="list-style-type: none"> 1. Execute procedure “<i>Configure Blade Server iLO Password for Administrator Account</i>” from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing section “<i>Server Blades Installation Preparation</i>” from reference [10]

Procedure 3: Recovery Scenario 3

<p>9 <input type="checkbox"/></p>	<p>HP-Class Blade Failure: Backups Available</p>	<p>If the failed server is NOT an OAM type HP C-Class Blade, skip to step 11.</p> <p>This step assumes that TVOE backups are available, if backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> 1. Install and configure TVOE on failed TVOE blade servers by executing section <i>“Install TVOE on Blade Servers”</i> from reference [10]. 2. Restore the TVOE backup by executing Appendix H: Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers.
<p>10 <input type="checkbox"/></p>	<p>HP-Class Blade Failure: Backups NOT Available</p>	<p>If the failed server is NOT an OAM type HP C-Class Blade, skip to step 11.</p> <p>This step assumes that TVOE backups are NOT are available</p> <ol style="list-style-type: none"> 1. Install and configure TVOE on failed TVOE blade servers by executing section <i>“Install TVOE on Blade Servers”</i> from reference [10].
<p>11 <input type="checkbox"/></p>	<p>Execute Fast Deployment File for NOAMs</p>	<p>The backup fdconfig file used during the initial DSR 7.2/7.3 installation, this file will be available on the PMAC if a database backup was restored on the PMAC.</p> <p>If a backup fast deployment xml is NOT available, execute procedure <i>“Configure NOAM Servers”</i> from reference [8].</p> <p>If a backup fast deployment xml is already present on the PMAC, execute the following procedure:</p> <ol style="list-style-type: none"> 3) Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade has been performed since initial installation). 4) Execute the following commands: <pre style="border: 1px solid black; padding: 5px;">\$ cd /usr/TKLC/smac/etc \$ screen \$ sudo fdconfig config --file=<Created_FD_File>.xml</pre>
<p>12 <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 <i>Required Materials</i>; use site survey documents and Network Element report (if available), to determine network configuration data.</p>

Procedure 3: Recovery Scenario 3

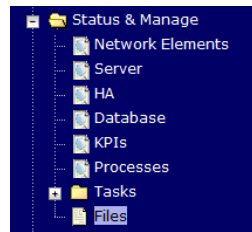
13 <input type="checkbox"/>	Execute DSR Installation Procedure for the First NOAM	<ol style="list-style-type: none">1. Configure the first NOAM server by executing procedure “<i>Configure the First NOAM NE and Server</i>” from reference [8].2. Configure the NOAM server group by executing procedure “<i>Configure the NOAM Server Group</i>” from reference [8]. <p>Note: Use the backup copy of network configuration data and site surveys (Step 2)</p>
14 <input type="checkbox"/>	NOAM GUI: Login	<p>Login to the NOAM GUI as the <i>guiadmin</i> user:</p> 

Procedure 3: Recovery Scenario 3

15
□

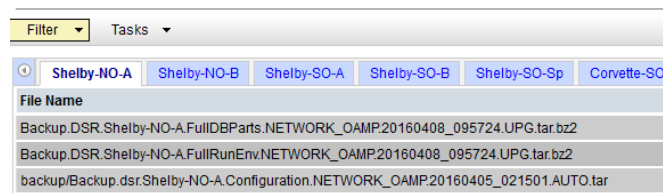
NOAM GUI:
Upload the
Backed up
Database File

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

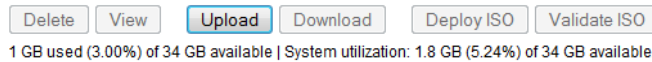


Select the Active NOAM server. The following screen will appear:

Main Menu: Status & Manage -> Files

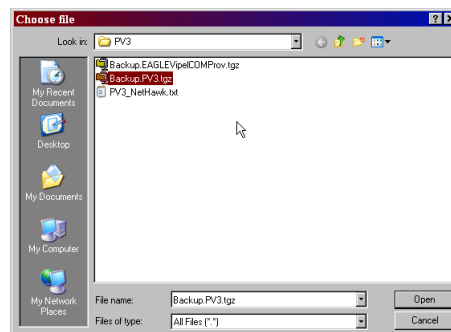
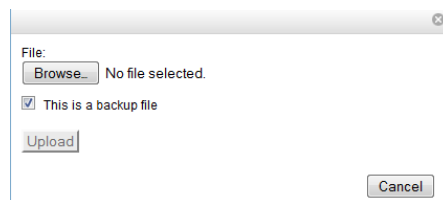


Click on **Upload** as shown below and select the file *“NO Provisioning and Configuration:”* file backed up after initial installation and provisioning.



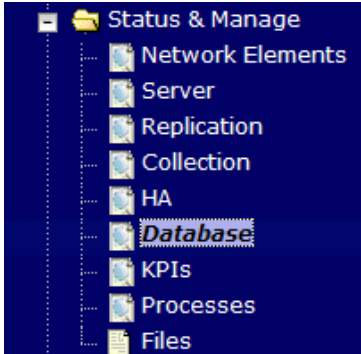

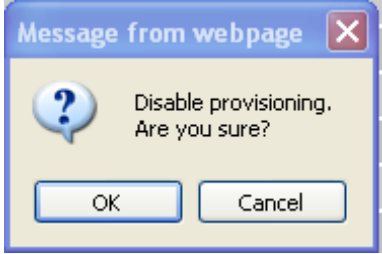
1 GB used (3.00%) of 34 GB available | System utilization: 1.8 GB (5.24%) of 34 GB available.

1. Click on **Browse** and locate the backup file
2. Check **This is a backup file** Box
3. 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

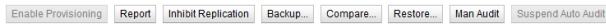
<p>16</p> <p>□</p>	<p>NOAM GUI: Disable Provisioning</p>	<p>Click on Main Menu->Status & Manage->Database</p>  <p>Disable Provisioning by clicking on Disable Provisioning button at the bottom of the screen as shown below.</p>  <p>A confirmation window will appear, press OK to disable Provisioning.</p>  <p>The message <i>"Warning Code 002"</i> will appear.</p>
--------------------	--	--

Procedure 3: Recovery Scenario 3

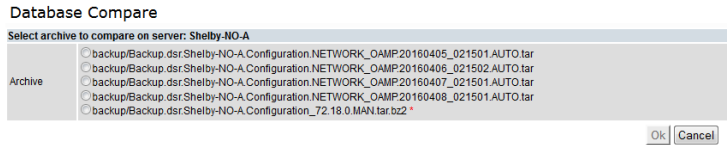
17

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 Topology Compatibility warnings. That is expected. If that is the only mismatch, proceed, otherwise stop and contact **Appendix L: 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: USER AND AUTHENTICATION DATA may not be compatible

Note: These compatibility errors do not have an impact on the database restore.

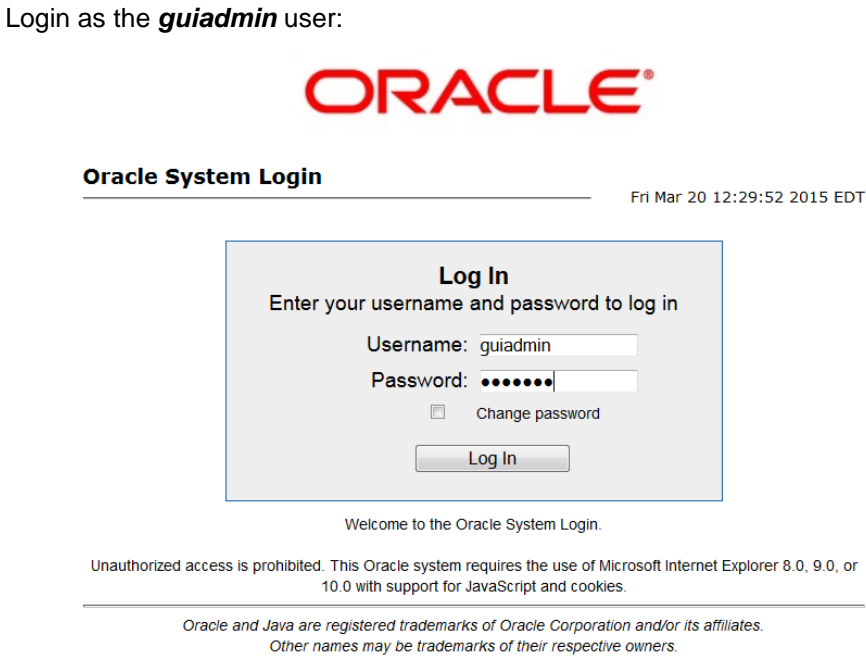
Note: We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility.

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

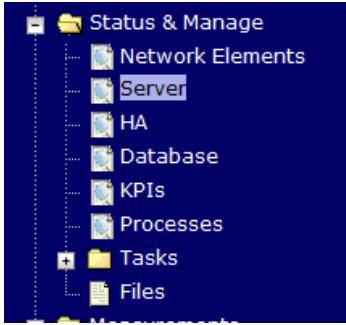
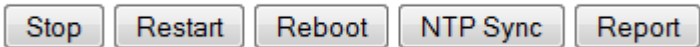
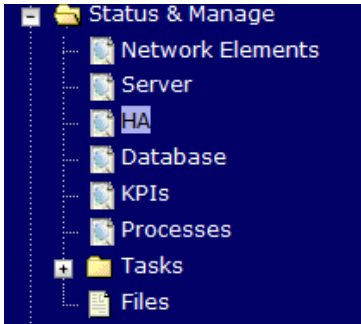
Procedure 3: Recovery Scenario 3

<p>18</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>Main Menu: Status & Manage -> Database [Restore]</p> <hr/> <p>Database Restore</p> <p>Select archive to Restore on server: Shelby-NO-A</p> <p>Archive</p> <ul style="list-style-type: none"><input type="radio"/> backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP20160405_021501.AUTO.tar<input type="radio"/> backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP20160406_021502.AUTO.tar<input type="radio"/> backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP20160407_021501.AUTO.tar<input type="radio"/> backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP20160408_021501.AUTO.tar<input type="radio"/> backup/Backup.dsr.Shelby-NO-A.Configuration_72.18.0.MAN.tar.bz2 * <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> <div style="border: 1px solid red; padding: 5px;"><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> <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="button" value="Ok"/> <input type="button" value="Cancel"/> Force restore on blade07, despite compare errors.</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>
---	---	---

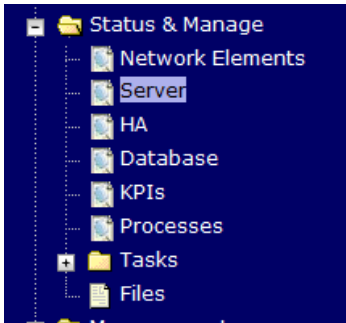
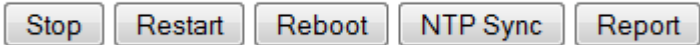
Procedure 3: Recovery Scenario 3

<p>19</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>20</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 restore 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>21</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Login</p>	<p>Login to the recovered Active NOAM via SSH terminal as <i>admusr</i> user.</p>

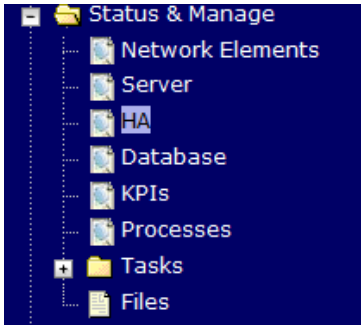
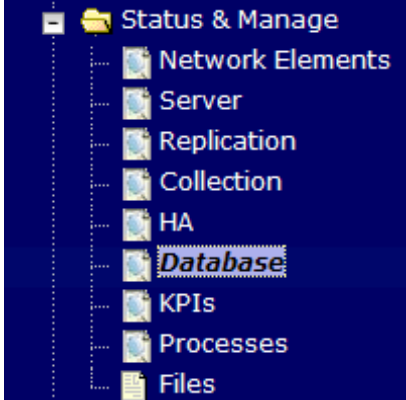

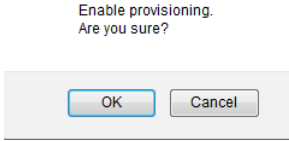
Procedure 3: Recovery Scenario 3

<p>22</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 3-5, 7 from reference [8].</p> <p>Note: Execute step 6 if NetBackup is used.</p>
<p>23</p> <p><input type="checkbox"/></p>	<p>Active NOAM: Correct the RecognizedAuth ority table</p>	<p>Establish an SSH session to the active NOAM, login as admusr.</p> <p>Execute the following command:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo top.setPrimary - Using my cluster: A1789 - New Primary Timestamp: 11/09/15 20:21:43.418 - Updating A1789.022: <DSR_NOAM_B_hostname> - Updating A1789.144: <DSR_NOAM_A_hostname></pre>
<p>24</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 NOAM server and click on Restart.</p> 
<p>25</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Set recovered NOAM Server to Active</p>	<p>Navigate to Status & Manage -> HA</p>  <p>Click on Edit at the bottom of the screen</p> <p>For the recovered standby NOAM that is set to forced standby, set it to Active</p> <p>Press OK</p>

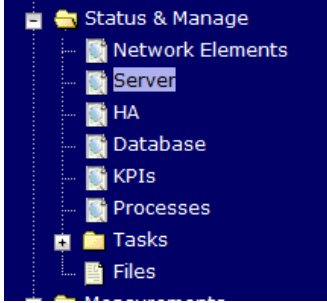
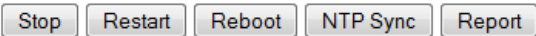
Procedure 3: Recovery Scenario 3

<p>26</p> <p><input type="checkbox"/></p>	<p>Install NetBackup Client (Optional)</p>	<p>If NetBackup is used execute procedure <i>“Install NetBackup Client”</i> from reference [8]</p>
<p>27</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover Failed SOAM Servers</p>	<p>Recover failed SOAM servers (standby, spare) by repeating the following steps for each SOAM server:</p> <ol style="list-style-type: none"> 1. Execute procedure <i>“Configure the SOAM Servers”</i>, steps 1-3, and 5-8 from reference [8]. <p>Note: If you are using NetBackup, also execute step 10</p> <ol style="list-style-type: none"> 2. If you are using NetBackup, execute procedure <i>“Install NetBackup Client”</i> from reference [8].
<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 SOAM server and click on Restart.</p> 
<p>29</p> <p><input type="checkbox"/></p>	<p>(PCA Only) Activate PCA Feature</p>	<p>If you are installing PCA, execute the applicable procedures (Added SOAM site activation or complete system activation) within Appendix A of [13] to activate PCA.</p> <p>Note: If not all SOAM sites are ready at this point, then you should repeat activation for each <i>*new*</i> SOAM site that comes online.</p>
<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 Blade Servers”</i>, Steps 1, 7, 11-14, and 17 from reference [8].</p> <p>Note: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.</p> <p>Repeat this step for any remaining failed MP servers.</p>

Procedure 3: Recovery Scenario 3

<p>31</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>32</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Enable Provisioning</p>	<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 3: Recovery Scenario 3

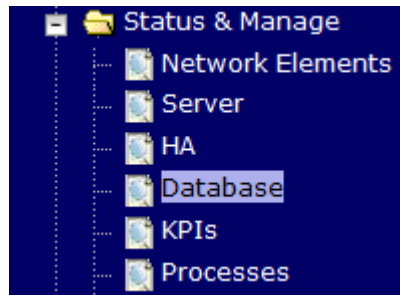
<p>33 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Restart DSR application</p>	<p>Navigate to Main Menu->Status & Manage->Server,</p>  <p>Select each recovered server and click on Restart.</p> 
<p>34 <input type="checkbox"/></p>	<p>ACTIVE NOAM: Perform key exchange between the active-NOAM and recovered 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>35 <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>Note: While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:</p> <pre>iload#31000{S/W Fault}</pre>

Procedure 3: Recovery Scenario 3

36

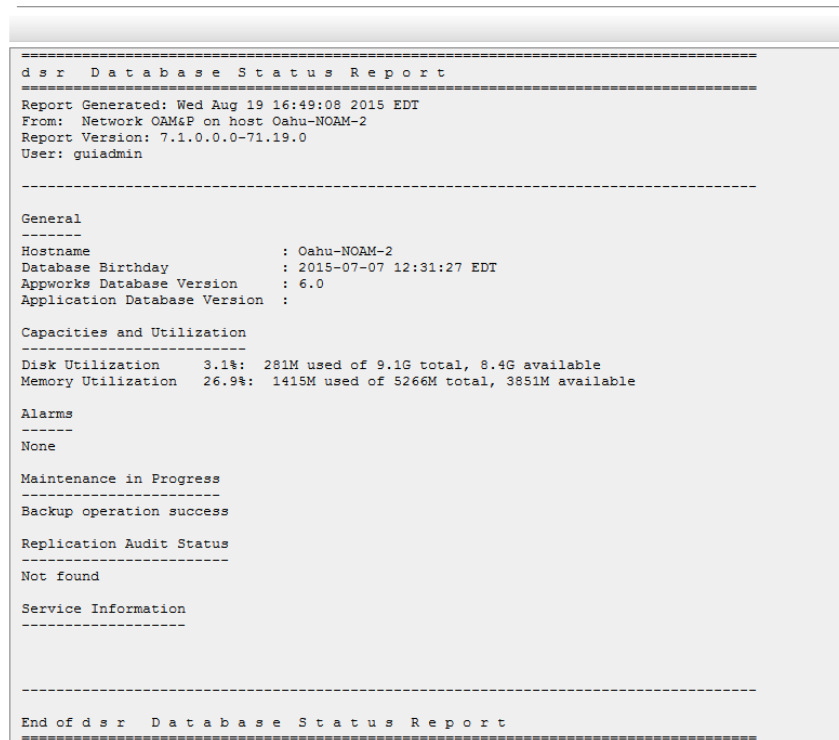
NOAM VIP GUI:
Fetch and Store
the database
Report for the
Newly Restored
Data and Save it

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



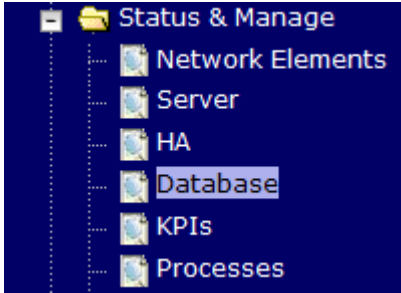
Select the **active** NOAM server and click on the **Report** button at the bottom of the page. The following screen is displayed:

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

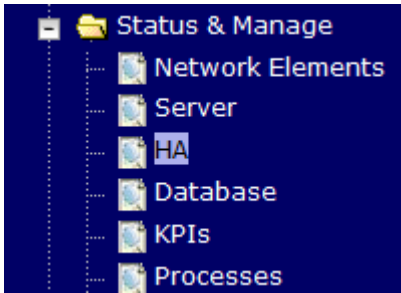


Click on **Save** and save the report to your local machine.

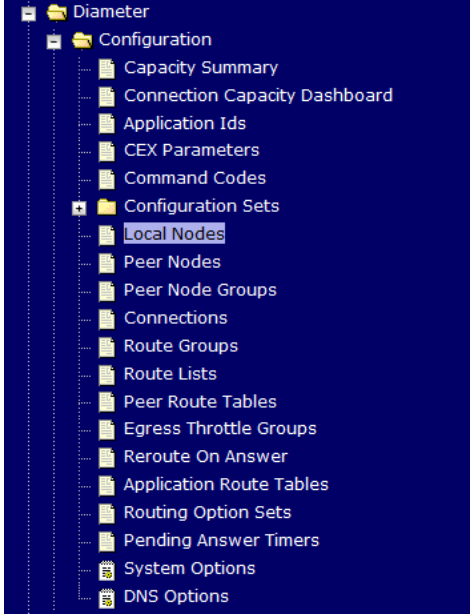
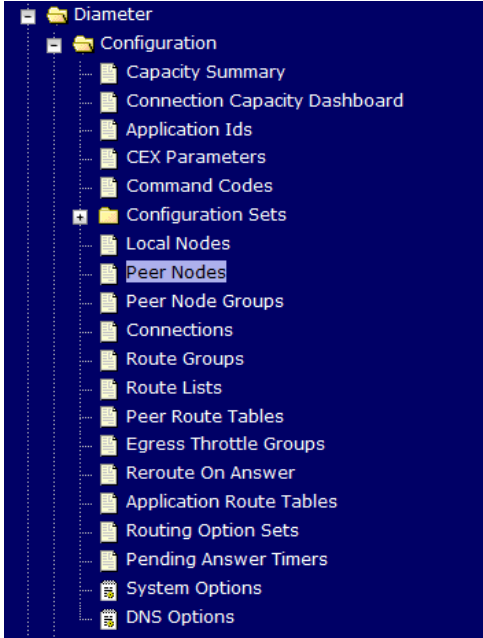
Procedure 3: Recovery Scenario 3

<p>37</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Verify Replication Between Servers.</p>	<p>Login to the Active NOAM via SSH terminal as <i>admusr</i> 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>38</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 1438 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>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>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>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>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	SO1	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	SO2	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	SO1	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	SO2	System OAM	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg																																																																																

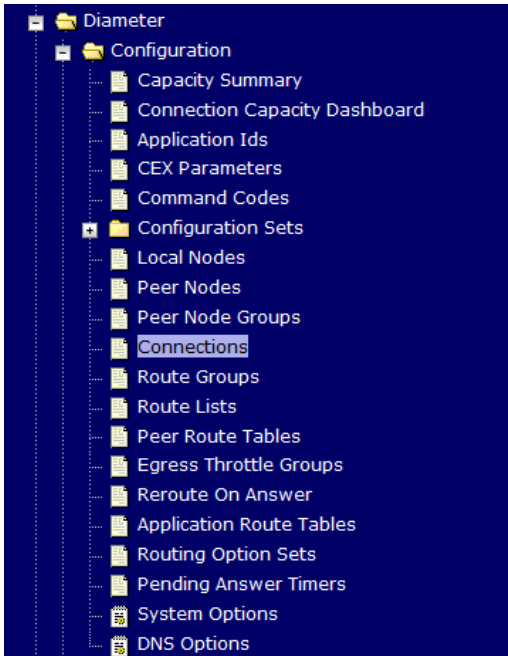
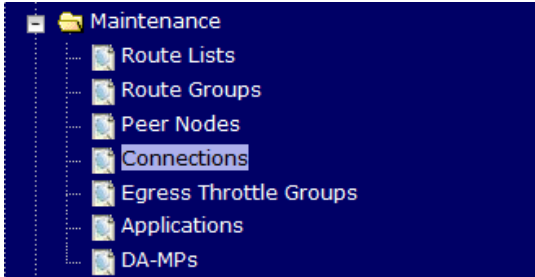
Procedure 3: Recovery Scenario 3

<p>39</p> <p>□</p>	<p>NOAM VIP GUI: Verify the HA Status</p>	<p>Click on Main Menu->Status and Manage->HA</p>  <p>Verify that the “OAM HA Role” for all rows is either “Active” or “Standby” as shown below.</p> <p>Main Menu: Status & Manage -> HA</p> <p>Filter ▾</p> <table border="1"> <thead> <tr> <th>Hostname</th> <th>OAM HA Role</th> <th>Application HA Role</th> <th>Max Allowed HA Role</th> </tr> </thead> <tbody> <tr><td>RamblerNOAM1</td><td>Standby</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerNOAM2</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerDRNOAM1</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerDRNOAM2</td><td>Standby</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerSOAM1</td><td>Standby</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerSOAM2</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerDAMP1</td><td>Active</td><td>Active</td><td>Active</td></tr> <tr><td>RamblerIPFE1</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerIPFE2</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerDAMP2</td><td>Standby</td><td>Active</td><td>Active</td></tr> </tbody> </table>	Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role	RamblerNOAM1	Standby	OOS	Active	RamblerNOAM2	Active	OOS	Active	RamblerDRNOAM1	Active	OOS	Active	RamblerDRNOAM2	Standby	OOS	Active	RamblerSOAM1	Standby	OOS	Active	RamblerSOAM2	Active	OOS	Active	RamblerDAMP1	Active	Active	Active	RamblerIPFE1	Active	OOS	Active	RamblerIPFE2	Active	OOS	Active	RamblerDAMP2	Standby	Active	Active
Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role																																											
RamblerNOAM1	Standby	OOS	Active																																											
RamblerNOAM2	Active	OOS	Active																																											
RamblerDRNOAM1	Active	OOS	Active																																											
RamblerDRNOAM2	Standby	OOS	Active																																											
RamblerSOAM1	Standby	OOS	Active																																											
RamblerSOAM2	Active	OOS	Active																																											
RamblerDAMP1	Active	Active	Active																																											
RamblerIPFE1	Active	OOS	Active																																											
RamblerIPFE2	Active	OOS	Active																																											
RamblerDAMP2	Standby	Active	Active																																											

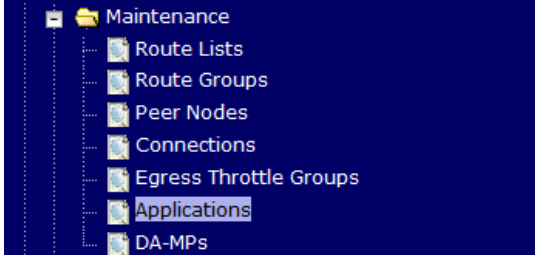

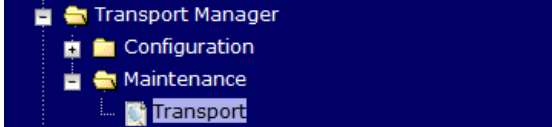

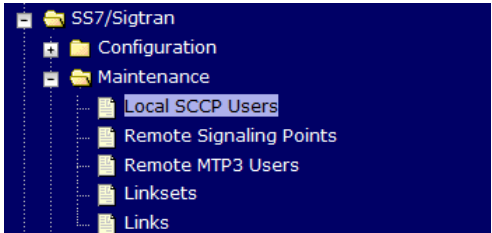

Procedure 3: Recovery Scenario 3

<p>40</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>41</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>42</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>43</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 3: Recovery Scenario 3

<p>44</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>45</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable Transports if Needed</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>46</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable MAPIWF application if needed</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>

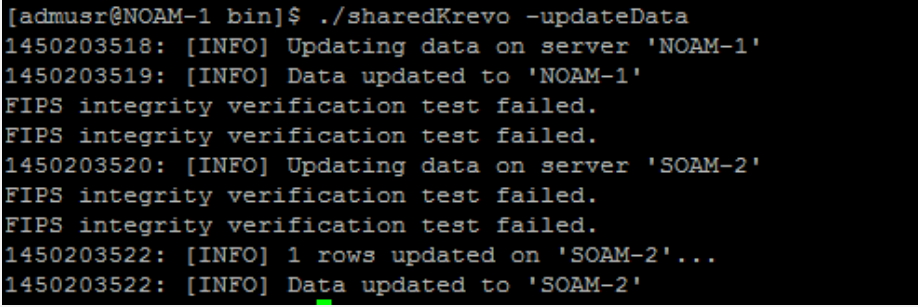
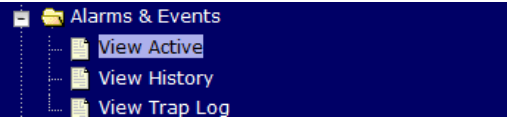
Procedure 3: Recovery Scenario 3

<p>47</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable links if needed</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>48</p> <p><input type="checkbox"/></p>	<p>NOAM VIP: Verify all servers in Topology are accessible (RADIUS Only)</p>	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Establish an SSH session to the NOAM VIP. Login as admusr.</p> <p>Execute following commands to check if all the servers in the Topology are accessible :</p> <pre>\$ /usr/TKLC/dpi/bin/sharedKrevo -checkAccess</pre> <p>Output Example:</p>  <p>Note: If any of the servers are not accessible, stop and contact Appendix L: My Oracle Support (MOS)</p>

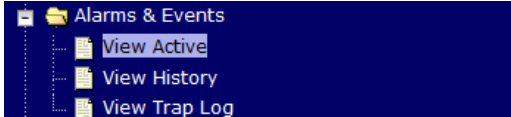
Procedure 3: Recovery Scenario 3

49 <input type="checkbox"/>	SOAM VIP: Copy key file to all the servers in Topology (RADIUS Only)	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Establish an SSH session to any of the Active SOAM which remained intact and operational (Need to Login to Active SOAM server which was not recovered or did not need recovery). Login as admusr.</p> <p>Execute following commands to check if existing Key file on Active SOAM server is valid :</p> <pre>\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -validate</pre> <p>Expected Output:</p> <pre>/usr/TKLC/dpi/</pre> <p>Note: If output of above command shows that existing key file is not valid, contact Appendix L: My Oracle Support (MOS)</p> <p>Establish an SSH session to the active SOAM, login as admusr.</p> <p>Execute following command to copy the key file to Active NOAM :</p> <pre>\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -copyKey -destServer <Active NOAM server name></pre>
--------------------------------	--	---

Procedure 3: Recovery Scenario 3

<p>50</p> <p><input type="checkbox"/></p>	<p>NOAM VIP: Copy key file to all the servers in Topology (RADIUS Only)</p>	<p>Establish an SSH session to any of the Active NOAM. Login as admusr.</p> <p>Execute following command to copy the key file to all the servers in the Topology :</p> <pre>\$./sharedKrevo -synchronize</pre>  <pre>\$./sharedKrevo -updateData</pre> 
<p>51</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 L: My Oracle Support (MOS).</p>

Procedure 3: Recovery Scenario 3

<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 L: My Oracle Support (MOS).</p>
<p>53 <input type="checkbox"/></p>	<p>Restore GUI Usernames and Passwords</p>	<p>If applicable, Execute steps in Section 0 to recover the user and group information restored.</p>
<p>54 <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>
<p>55 <input type="checkbox"/></p>	<p>Recover IDIH</p>	<p>If IDIH were affected, refer to Section 0 to perform disaster recovery on IDIH.</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.

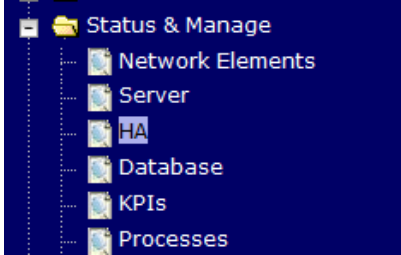
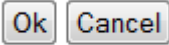
The database is intact at the active NOAM server and does not require restoration at the SO and MP servers.

- 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 L: 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: 60%; 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: 60%; 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: Configure BIOS Settings and Update Firmware</p>	<p>If the failed server is NOT a rack mount server, skip to step 9. If the failed server is NOT an OAM type blade server, skip to step 26</p> <ol style="list-style-type: none"> 1. Configure and verify the BIOS settings by executing procedure “<i>Configure the RMS and Blade Server BIOS Settings</i>” from reference [10] 2. Verify and/or upgrade server firmware by executing procedure “<i>Upgrade Management Server Firmware</i>” from reference[10] <p>Note: Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.</p>
<p>6</p> <p><input type="checkbox"/></p>	<p>RMS NOAM Failure: Backups Available</p>	<p>If the failed server is NOT a rack mount server, skip to step 9.</p> <p>This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> 1. Restore the TVOE backup by executing Appendix H: Restore TVOE Configuration from Backup Media <p>If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing</p> <ol style="list-style-type: none"> 2. Appendix I: Restore PMAC from Backup


Procedure 4: Recovery Scenario 4

<p>7 <input type="checkbox"/></p>	<p>Recover Failed Aggregation/ Enclosure Switches, and OAs</p>	<p>Recover failed OAs, aggregation and enclosure switches if needed.</p> <p>Backups Available:</p> <ol style="list-style-type: none"> 1. Refer to Appendix B: Recovering/Replacing Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches <p>Backups NOT Available:</p> <ol style="list-style-type: none"> 1. Execute section “<i>HP C-7000 Enclosure Configuration</i>” from reference [10] to recover and configure any failed OAs if needed. 2. Execute section “Configure Enclosure Switches” from reference [10] to recover enclosure switches if needed.
<p>8 <input type="checkbox"/></p>	<p>RMS NOAM Failure: Backups NOT Available</p>	<p>If the failed server is NOT a rack mount server, skip to step 9.</p> <p>This step assumes that TVOE and PMAC backups NOT are available, if the TVOE and PMAC have already been restored, skip this step.</p> <p>If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures:</p> <ol style="list-style-type: none"> 1. Section “<i>Configure and IPM Management Server</i>” from reference [10]. 2. Section “<i>Install PM&C</i>” from reference [10]. 3. Section “<i>Configure PM&C</i>” from reference [10]. <p>If the PMAC is NOT located on the same TVOE host as the failed NOAM, Execute the following sections/procedures</p> <p>Section “<i>Installing TVOE on Rack Mount Server(s)</i>” from reference [10].</p>
<p>9 <input type="checkbox"/></p>	<p>HP-Class Blade Failure: Configure Blade Server iLO, Update Firmware/BIOS Settings</p>	<p>If the failed server is NOT an HP C-Class Blade, skip to step 13.</p> <ol style="list-style-type: none"> 1. Execute procedure “<i>Configure Blade Server iLO Password for Administrator Account</i>” from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing section “<i>Server Blades Installation Preparation</i>” from reference [10]

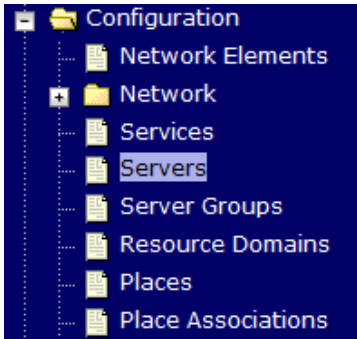
Procedure 4: Recovery Scenario 4

<p>10 <input type="checkbox"/></p>	<p>HP-Class Blade Failure: Backups Available</p>	<p>If the failed server is NOT an OAM type HP C-Class Blade, skip to step 13.</p> <p>This step assumes that TVOE backups are available, if backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> 1. Install and configure TVOE on failed TVOE blade servers by executing section <i>“Install TVOE on Blade Servers”</i> from reference [10]. 2. Restore the TVOE backup by executing Appendix H: Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers.
<p>11 <input type="checkbox"/></p>	<p>HP-Class Blade Failure: Backups NOT Available</p>	<p>If the failed server is NOT an OAM HP C-Class Blade, skip to step 13.</p> <p>This step assumes that TVOE backups are NOT are available</p> <ol style="list-style-type: none"> 1. Install and configure TVOE on failed TVOE blade servers by executing section <i>“Install TVOE on Blade Servers”</i> from reference [10]. 2. Configure the NOAM and/or SOAM failed TVOE server blades by executing procedure <i>“Configure SOAM TVOE Server Blades”</i> from reference [8] <p>Note: Although the title of the procedure is related to SOAMs only, execute this procedure for any failed NOAMs located on TVOE server blades.</p>
<p>12 <input type="checkbox"/></p>	<p>Create VMs</p>	<p>Execute Appendix K: Create NOAM/SOAM Virtual Machines to create the NOAM and SOAM VMs on failed TVOE server blades.</p>
<p>13 <input type="checkbox"/></p>	<p>IPM and Install DSR Application on Failed Guest/Servers</p>	<ol style="list-style-type: none"> 1. Execute procedure <i>“IPM Blades and VMs”</i> for the failed SOAM VMs and MP blades from reference [8]. 2. Execute procedure <i>“Install the Application”</i> for the failed SOAM VMs and MP blades from reference [8].
<p>14 <input type="checkbox"/></p>	<p>Install NetBackup Client (Optional)</p>	<p>If NetBackup is used execute procedure <i>“Install NetBackup Client”</i> from reference [8]</p>

Procedure 4: Recovery Scenario 4

<p>15 ☐</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> <pre>http://<Primary_NOAM_VIP_IP_Address></pre> <p>Login as the <i>guiadmin</i> user:</p> 
<p>16 ☐</p>	<p>Exchange SSH keys between PMAC and Failed NOAM Server</p>	<p>Use the PMAC GUI to determine the Control Network IP address of the failed NOAM server VM. From the PMAC GUI, navigate to Main Menu -> Software -> Software Inventory.</p> <p>Note the IP address for the failed NOAM server VM.</p> <p>Login to the PMAC terminal as the <i>admusr</i>.</p> <p>From a terminal window connection on the PMAC as the <i>admusr</i> user, exchange SSH keys for <i>admusr</i> between the PMAC and the failed NOAM server VM control network IP address. When prompted for the password, enter the password for the <i>admusr</i> user of the NOAM server.</p> <pre>\$ keyexchange admusr@<NO2_Control_IP Address></pre> <p>Note: if Key exchange fails, edit /home/admusr/.ssh/known_hosts and remove blank lines, and retry the keyexchange commands.</p>

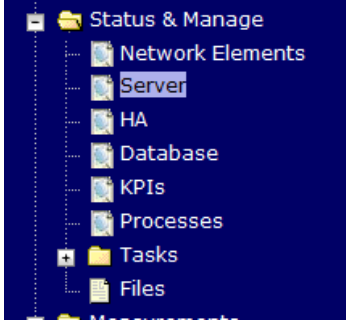
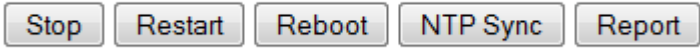
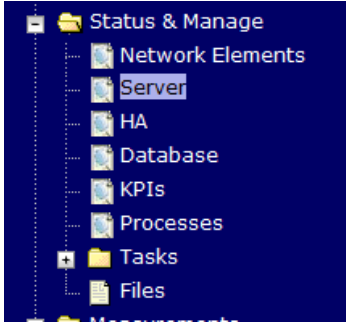
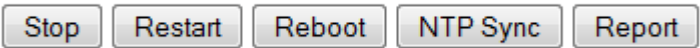
Procedure 4: Recovery Scenario 4

<p>17</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Export the Initial Configuration</p>	<p>Navigate to Main Menu -> Configuration -> Servers.</p>  <p>From the GUI screen, select the failed NOAM server and then select Export to generate the initial configuration data for that server.</p> <p><input type="button" value="Insert"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Export"/> <input type="button" value="Report"/></p>
<p>18</p> <p><input type="checkbox"/></p>	<p>NOAM VIP: Copy Configuration File to Failed NOAM Server</p>	<p>Obtain a terminal session to the NOAM VIP, login as the admusr.</p> <p>Use the awpushcfg utility to copy the configuration file created in the previous step from the <code>/var/TKLC/db/filemgmt</code> directory on the active NOAM to the failed NOAM server, using the Control network IP address for the failed NOAM VM.</p> <p>The configuration file will have a filename like <code>"TKLCConfigData.<hostname>.sh"</code>.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo awpushcfg</pre> <p>The awpushcfg utility is interactive, so the user will be prompted for the following:</p> <ul style="list-style-type: none"> • IP address of the local PMAC server: Use the local control network address from the PMAC. • Username: Use admusr • Control network IP address for the target server: In this case, enter the control IP for the failed NOAM VM). • Hostname of the target server: Enter the server name from Step 17

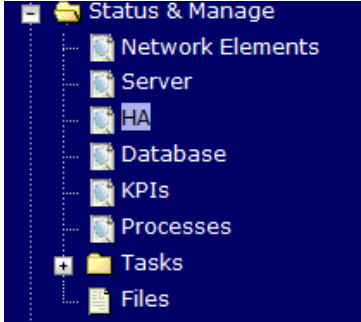
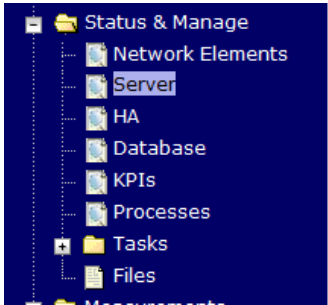
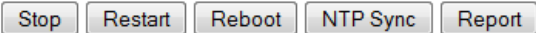
Procedure 4: Recovery Scenario 4

<p>19</p> <p><input type="checkbox"/></p>	<p>Failed NOAM Server: Verify awpushcfg was called and Reboot the Server</p>	<p>Establish an SSH session to the failed NOAM server, login as the <i>admusr</i> user.</p> <p>The automatic configuration daemon will look for the file named “<i>TKLCConfigData.sh</i>” in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server.</p> <p>Verify awpushcfg was called by checking the following file</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> <p>Verify the following message is displayed:</p> <pre style="border: 1px solid black; padding: 5px;">[SUCCESS] script completed successfully!</pre> <p>Now Reboot the Server:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo init 6</pre> <p>Wait for the server to reboot</p>
<p>20</p> <p><input type="checkbox"/></p>	<p>Failed NOAM Server: Configure Networking for Dedicated NetBackup Interface (Optional)</p>	<p>Note: You will only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.</p> <p>Obtain a terminal window to the failed NOAM server, logging in as the <i>admusr</i>.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP_Address> --netmask=<NO2_NetBackup_NetMask></pre> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NO1_NetBackup_Network_ID> --netmask=<NO2_NetBackup_NetMask> --gateway=<NO2_NetBackup_Gateway_IP_Address></pre>
<p>21</p> <p><input type="checkbox"/></p>	<p>Failed NOAM Server: Verify Server Health</p>	<p>Execute the following command on the 2nd NOAM server and make sure that no errors are returned:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

Procedure 4: Recovery Scenario 4

<p>22</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 NOAM server and click on Restart.</p> 
<p>23</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover Failed SOAM Servers</p>	<p>Recover failed SOAM servers (standby, spare) by repeating the following steps for each SOAM server:</p> <ol style="list-style-type: none"> 1. Execute procedure “Configure the SOAM Servers”, steps 1-3, and 5-8 from reference [8]. <p>Note: If you are using NetBackup, also execute step 10</p> <ol style="list-style-type: none"> 2. If you are using NetBackup, execute procedure “Install NetBackup Client” from reference [8].
<p>24</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 SOAM server and click on Restart.</p> 

Procedure 4: Recovery Scenario 4

<p>25 <input type="checkbox"/></p>	<p>(PCA Only) Activate PCA Feature</p>	<p>If you are installing PCA, execute the applicable procedures (Added SOAM site activation or complete system activation) within Appendix A of [13] to activate PCA.</p> <p>Note: If not all SOAM sites are ready at this point, then you should repeat activation for each *new* SOAM site that comes online.</p>
<p>26 <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 Blade Servers</i>”, Steps 1, 7, 11-14, and 17 from reference [8].</p> <p>Note: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.</p> <p>Repeat this step for any remaining failed MP servers.</p>
<p>27 <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>28 <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> 

Procedure 4: Recovery Scenario 4

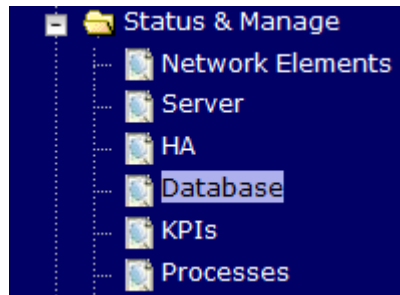
<p>29 <input type="checkbox"/></p>	<p>ACTIVE NOAM: Login</p>	<p>Login to the recovered Active NOAM via SSH terminal as <i>admusr</i> user.</p>
<p>30 <input type="checkbox"/></p>	<p>ACTIVE NOAM: Perform key exchange between the active-NOAM and recovered servers.</p>	<p>Establish an SSH session to the Active NOAM, login as <i>admusr</i>.</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: 2px;">\$ keyexchange admusr@<Recovered Server Hostname></pre>
<p>31 <input type="checkbox"/></p>	<p>ACTIVE NOAM: Activate Optional Features</p>	<p>Establish an SSH session to the active NOAM, login as <i>admusr</i>.</p> <p>Refer to section 1.5 Optional Features to activate any features that were previously activated.</p> <p>Note: While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:</p> <pre><i>iload#31000{S/W Fault}</i></pre>

Procedure 4: Recovery Scenario 4

32

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

Navigate to **Configuration-> Server -> 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: Thu Nov 05 11:23:30 2015 EST
From: Network OAM&P on host LDM2N01
Report Version: 7.1.1.0.0-71.28.0
User: guidadmin

-----

General
-----
Hostname           : LDM2N01
Database Birthday  : 2015-10-26 10:44:09 EDT
Appworks Database Version : 6.0
Application Database Version :

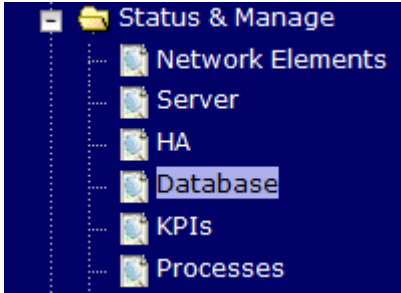
Capacities and Utilization
-----
Disk Utilization   2.6%: 233M used of 9.1G total, 8.4G available
Memory Utilization 26.8%: 1413M used of 5266M total, 3853M available

Alarms

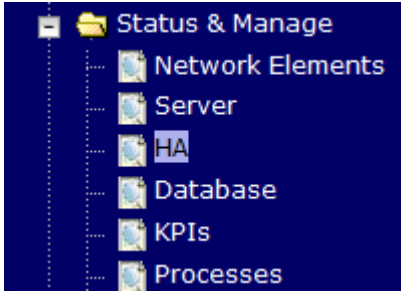
-----
Print Save Back
```

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

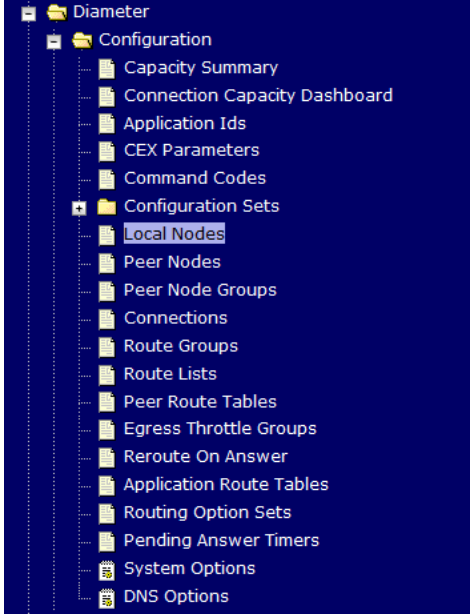
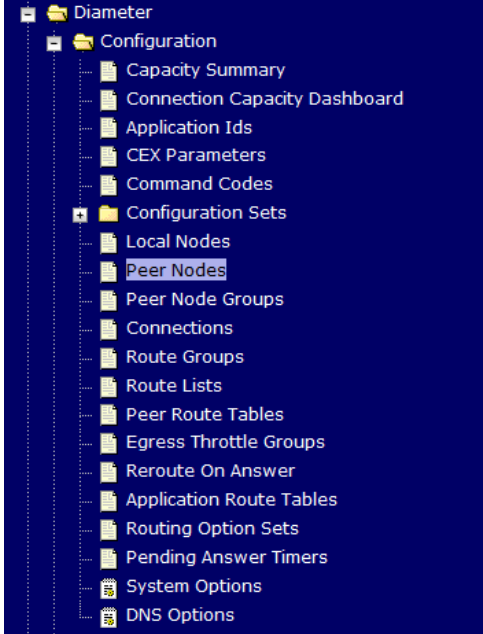
Procedure 4: Recovery Scenario 4

<p>33</p> <p><input type="checkbox"/></p>	<p>ACTIVE NOAM: Verify Replication Between Servers.</p>	<p>Login to the Active NOAM via SSH terminal as <i>admusr</i> 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>34</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>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>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>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>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	SO1	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	SO2	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	SO1	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	SO2	System OAM	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg																																																																																

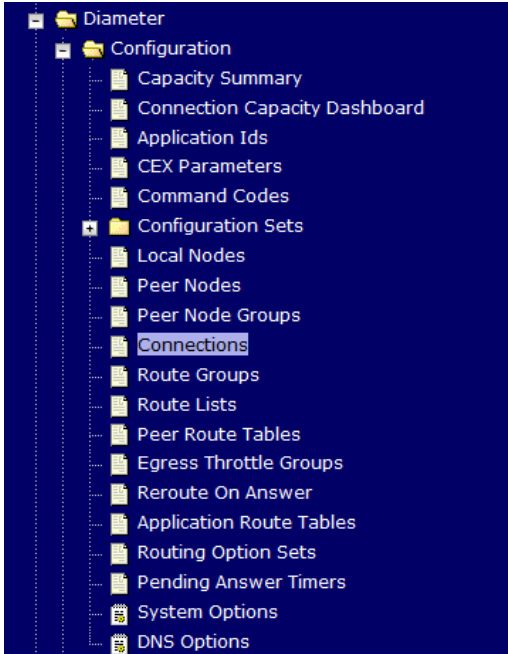
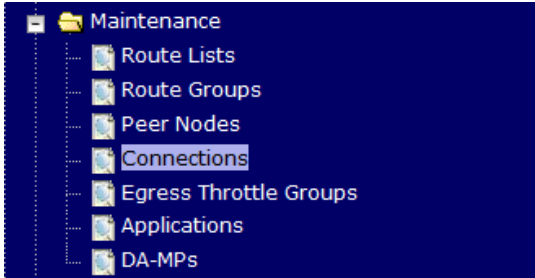
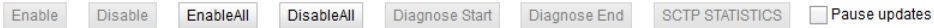
Procedure 4: Recovery Scenario 4

<p>35</p> <p>□</p>	<p>NOAM VIP GUI: Verify the HA Status</p>	<p>Click on Main Menu->Status and Manage->HA</p>  <p>Verify that the “OAM HA Role” for all rows is either “Active” or “Standby” as shown below.</p> <p>Main Menu: Status & Manage -> HA</p> <p>Filter ▾</p> <table border="1"> <thead> <tr> <th>Hostname</th> <th>OAM HA Role</th> <th>Application HA Role</th> <th>Max Allowed HA Role</th> </tr> </thead> <tbody> <tr><td>RamblerNOAM1</td><td>Standby</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerNOAM2</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerDRNOAM1</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerDRNOAM2</td><td>Standby</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerSOAM1</td><td>Standby</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerSOAM2</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerDAMP1</td><td>Active</td><td>Active</td><td>Active</td></tr> <tr><td>RamblerIPFE1</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerIPFE2</td><td>Active</td><td>OOS</td><td>Active</td></tr> <tr><td>RamblerDAMP2</td><td>Standby</td><td>Active</td><td>Active</td></tr> </tbody> </table>	Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role	RamblerNOAM1	Standby	OOS	Active	RamblerNOAM2	Active	OOS	Active	RamblerDRNOAM1	Active	OOS	Active	RamblerDRNOAM2	Standby	OOS	Active	RamblerSOAM1	Standby	OOS	Active	RamblerSOAM2	Active	OOS	Active	RamblerDAMP1	Active	Active	Active	RamblerIPFE1	Active	OOS	Active	RamblerIPFE2	Active	OOS	Active	RamblerDAMP2	Standby	Active	Active
Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role																																											
RamblerNOAM1	Standby	OOS	Active																																											
RamblerNOAM2	Active	OOS	Active																																											
RamblerDRNOAM1	Active	OOS	Active																																											
RamblerDRNOAM2	Standby	OOS	Active																																											
RamblerSOAM1	Standby	OOS	Active																																											
RamblerSOAM2	Active	OOS	Active																																											
RamblerDAMP1	Active	Active	Active																																											
RamblerIPFE1	Active	OOS	Active																																											
RamblerIPFE2	Active	OOS	Active																																											
RamblerDAMP2	Standby	Active	Active																																											

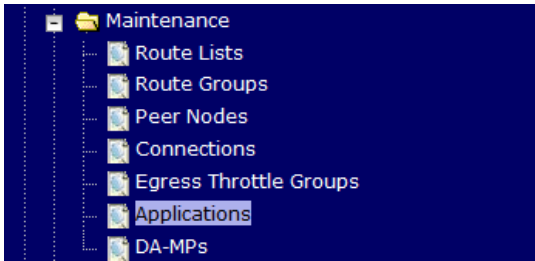
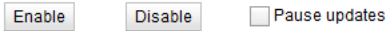
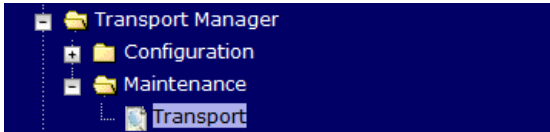
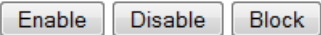
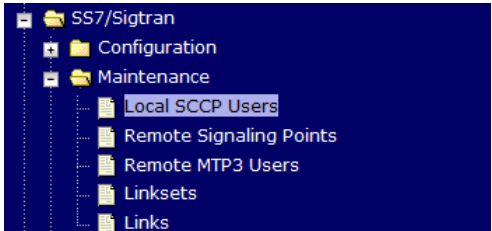

Procedure 4: Recovery Scenario 4

<p>36</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>37</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>38</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>39</p> <p><input type="checkbox"/></p>	<p>MP Servers: Disable SCTP Auth Flag</p>	<p>For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [14]</p> <p>Execute this procedure on all Failed MP Servers.</p>
<p>40</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>41</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>42</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>43</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable MAPIWF application if needed</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>

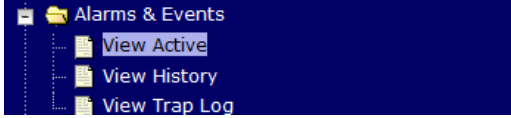
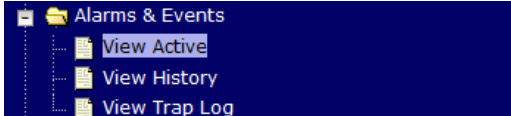
Procedure 4: Recovery Scenario 4

<p>44</p> <p><input type="checkbox"/></p>	<p>SOAM VIP GUI: Re-enable links if needed</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>45</p> <p><input type="checkbox"/></p>	<p>NOAM VIP: Verify all servers in Topology are accessible (RADIUS Only)</p>	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Establish an SSH session to the NOAM VIP. Login as <i>admusr</i>.</p> <p>Execute following commands to check if all the servers in the Topology are accessible :</p> <pre>\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -checkAccess</pre> <p>Example Output:</p>  <p>Note: If any of the servers are not accessible, stop and contact Appendix L: My Oracle Support (MOS)</p>

Procedure 4: Recovery Scenario 4

<p>46</p> <p><input type="checkbox"/></p>	<p>NOAM VIP: Copy key file to all the servers in Topology (RADIUS Only)</p>	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Execute following commands to check if existing Key file on Active NOAM server is valid :</p> <pre>\$./sharedKrevo -validate</pre>  <pre>[admusr@NOAM-2 bin]\$./sharedKrevo -validate FIPS integrity verification test failed. FIPS integrity verification test failed. 1450887507: [INFO] Key file for 'NOAM-1' is valid 1450887507: [INFO] Key file for 'NOAM-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450887507: [INFO] Key file for 'SOAM-1' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450887508: [INFO] Key file for 'SOAM-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450887509: [INFO] Key file for 'IPFE' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450887510: [INFO] Key file for 'MP-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450887510: [INFO] Key file for 'MP-1' is valid [admusr@NOAM-2 bin]\$</pre> <p>If output of above command shows that existing key file is not valid then contact Appendix L: My Oracle Support (MOS)</p> <p>Execute following command to copy the key file to all the servers in the Topology :</p> <pre>\$./sharedKrevo -synchronize</pre>  <pre>[admusr@NOAM-2 bin]\$./sharedKrevo -synchronize FIPS integrity verification test failed. FIPS integrity verification test failed. 1450887549: NOAM-2 and NOAM-1 key files differ. Sync NOAM-2 key file to NOAM-1. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450887551: [INFO] Synched key to NOAM-1 FIPS integrity verification test failed. FIPS integrity verification test failed. 1450887552: NOAM-2 and SOAM-1 key files differ. Sync NOAM-2 key file to SOAM-1. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450887554: [INFO] Synched key to SOAM-1 FIPS integrity verification test failed. FIPS integrity verification test failed. 1450887554: [INFO] Key file on Active NOAM and SOAM-2 are same. 1450887554: [INFO] NO NEED to sync key file to SOAM-2. FIPS integrity verification test failed.</pre> <pre>\$./sharedKrevo -updateData</pre>  <pre>[admusr@NOAM-2 bin]\$./sharedKrevo -updateData 1450887607: [INFO] Updating data on server 'NOAM-2' 1450887608: [INFO] Data updated to 'NOAM-2' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450887609: [INFO] Updating data on server 'SOAM-2' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450887611: [INFO] 1 rows updated on 'SOAM-2'... 1450887611: [INFO] Data updated to 'SOAM-2'</pre>
---	--	---

Procedure 4: Recovery Scenario 4

<p>47 <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 L: My Oracle Support (MOS).</p>
<p>48 <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 L: My Oracle Support (MOS).</p>
<p>49 <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 admusr</p> <p>Execute the following commands:</p> <pre data-bbox="488 1182 990 1276">\$ sudo pm.set off oampAgent \$ sudo pm.set on oampAgent</pre>
<p>50 <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>
<p>51 <input type="checkbox"/></p>	<p>Recover IDIH</p>	<p>If IDIH were affected, refer to Section 0 to perform disaster recovery on IDIH.</p>

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.

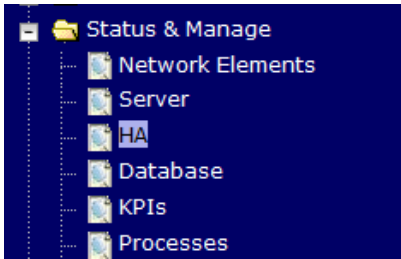
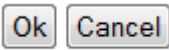
If applicable, recover any failed SOAM and MP servers by recovering base hardware and software.

- 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 L: 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.
4 <input type="checkbox"/>	Recover Failed SOAMs	If ALL SOAM servers have failed, execute Procedure 2
5 <input type="checkbox"/>	DR-NOAM VIP GUI: Login	<p>Establish a GUI session on the DR-NOAM server by using the VIP IP address of the DR-NOAM server. Open the web browser and enter a URL of:</p> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 10px auto;"> <p><code>http://<Primary_DR-NOAM_VIP_IP_Address></code></p> </div> <p>Login as the guiadmin user:</p> <div style="text-align: center; margin: 20px 0;">  </div>

Procedure 5: Recovery Scenario 5

<p>6</p> <p><input type="checkbox"/></p>	<p>DR-NOAM VIP GUI: Set Failed NOAM 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 NOAM servers.</p> <p>Select Ok</p> 
<p>7</p> <p><input type="checkbox"/></p>	<p>RMS NOAM Failure: Configure BIOS Settings and Update Firmware</p>	<p>If the failed server is NOT a rack mount server, skip to step 11.</p> <ol style="list-style-type: none"> 1. Configure and verify the BIOS settings by executing procedure <i>“Configure the RMS and Blade Server BIOS Settings”</i> from reference [10] 2. Verify and/or upgrade server firmware by executing procedure <i>“Upgrade Management Server Firmware”</i> from reference[10] <p>Note: Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.</p>
<p>8</p> <p><input type="checkbox"/></p>	<p>RMS NOAM Failure: Backups Available</p>	<p>If the failed server is NOT a rack mount server, skip to step 11.</p> <p>This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> 1. Restore the TVOE backup by executing Appendix H: Restore TVOE Configuration from Backup Media <p>If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing</p> <ol style="list-style-type: none"> 2. Appendix I: Restore PMAC from Backup

Procedure 5: Recovery Scenario 5

<p>9</p> <p><input type="checkbox"/></p>	<p>Recover Failed Aggregation/ Enclosure Switches, and OAs</p>	<p>Recover failed OAs, aggregation and enclosure switches if needed.</p> <p>Backups Available:</p> <ol style="list-style-type: none"> 1. Refer to Appendix B: Recovering/Replacing Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches <p>Backups NOT Available:</p> <ol style="list-style-type: none"> 1. Execute section “<i>HP C-7000 Enclosure Configuration</i>” from reference [10] to recover and configure any failed OAs if needed. 2. Execute section “Configure Enclosure Switches” from reference [10] to recover enclosure switches if needed.
<p>10</p> <p><input type="checkbox"/></p>	<p>RMS NOAM Failure: Backups NOT Available</p>	<p>If the failed server is NOT a rack mount server, skip to step 11.</p> <p>This step assumes that TVOE and PMAC backups NOT are available, if the TVOE and PMAC have already been restored, skip this step.</p> <p>If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures:</p> <ol style="list-style-type: none"> 1. Section “<i>Configure and IPM Management Server</i>” from reference [10]. 2. Section “<i>Install PM&C</i>” from reference [10]. 3. Section “<i>Configure PM&C</i>” from reference [10]. <p>If the PMAC is NOT located on the same TVOE host as the failed NOAM, Execute the following sections/procedures</p> <ol style="list-style-type: none"> 1. Section “<i>Installing TVOE on Rack Mount Server(s)</i>” from reference [10].
<p>11</p> <p><input type="checkbox"/></p>	<p>HP-Class Blade Failure: Configure Blade Server iLO, Update Firmware/BIOS Settings</p>	<p>If the failed server is NOT an HP C-Class Blade, skip to step 14.</p> <ol style="list-style-type: none"> 1. Execute procedure “<i>Configure Blade Server iLO Password for Administrator Account</i>” from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing section “<i>Server Blades Installation Preparation</i>” from reference [10]

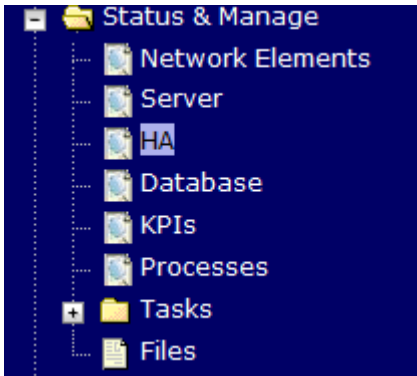
Procedure 5: Recovery Scenario 5

<p>12</p> <p><input type="checkbox"/></p>	<p>HP-Class Blade Failure: Backups Available</p>	<p>If the failed server is NOT an OAM type HP C-Class Blade, skip to step 14.</p> <p>This step assumes that TVOE backups are available, if backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> 1. Install and configure TVOE on failed TVOE blade servers by executing section <i>“Install TVOE on Blade Servers”</i> from reference [10]. 2. Restore the TVOE backup by executing Appendix H: Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers.
<p>13</p> <p><input type="checkbox"/></p>	<p>HP-Class Blade Failure: Backups NOT Available</p>	<p>If the failed server is NOT an OAM type HP C-Class Blade, skip to step 14.</p> <p>This step assumes that TVOE backups are NOT are available</p> <ol style="list-style-type: none"> 1. Install and configure TVOE on failed TVOE blade servers by executing section <i>“Install TVOE on Blade Servers”</i> from reference [10].
<p>14</p> <p><input type="checkbox"/></p>	<p>Execute Fast Deployment File for NOAMs</p>	<p>The backup fdconfig file used during the initial DSR 7.2/7.3 installation, this file will be available on the PMAC if a database backup was restored on the PMAC.</p> <p>If a backup fast deployment xml is NOT available, execute procedure <i>“Configure NOAM Servers”</i> from reference [8].</p> <p>If a backup fast deployment xml is already present on the PMAC, execute the following procedure:</p> <ol style="list-style-type: none"> 5) Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade has been performed since initial installation). 6) Execute the following commands: <pre style="border: 1px solid black; padding: 5px;">\$ cd /usr/TKLC/smac/etc \$ screen \$ sudo fdconfig config --file=<Created_FD_File>.xml</pre>
<p>15</p> <p><input type="checkbox"/></p>	<p>DR-NOAM VIP GUI: Export the Initial Configuration</p>	<p>Navigate to Main Menu -> Configuration -> Servers.</p> <p>From the GUI screen, select the Failed NOAM server and then select Export to generate the initial configuration data for that server.</p> <p style="text-align: center;"> <input type="button" value="Insert"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Export"/> <input type="button" value="Report"/> </p>

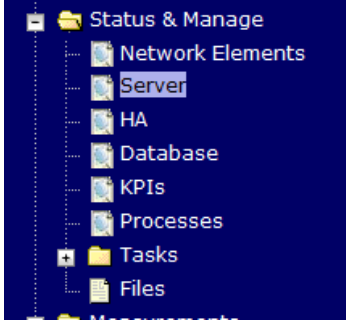
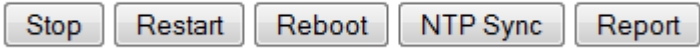
Procedure 5: Recovery Scenario 5

<p>16</p> <p><input type="checkbox"/></p>	<p>DR-NOAM VIP GUI: Copy Configuration File to Failed NOAM Server</p>	<p>Obtain a terminal session to the DR-NOAM VIP, login as the admusr user. Execute the following command to configure the failed NOAM server:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<Failed_NOAM_Hostname>.sh admusr@<Failed_NOAM_xmi_IP_address>:/var/tmp/TKLCConfigData.sh</pre>
<p>17</p> <p><input type="checkbox"/></p>	<p>Recovered NOAM Server: Verify configuration was called and Reboot the Server</p>	<p>Establish an SSH session to the Recovered NOAM server (Recovered_NOAM_xmi_IP_address)</p> <p>Login as the admusr user.</p> <p>The automatic configuration daemon will look for the file named “TKLCConfigData.sh” in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server.</p> <p>Verify awpushcfg was called by checking the following file</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> <p>Verify the following message is displayed:</p> <pre style="border: 1px solid black; padding: 5px;">[SUCCESS] script completed successfully!</pre> <p>Now Reboot the Server:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo init 6</pre> <p>Wait for the server to reboot</p>
<p>18</p> <p><input type="checkbox"/></p>	<p>Recovered NOAM Server: Configure Networking for Dedicated NetBackup Interface (Optional)</p>	<p>Note: You will only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP_Address> --netmask=<NO2_NetBackup_NetMask></pre> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NO1_NetBackup_Network_ID> --netmask=<NO2_NetBackup_NetMask> --gateway=<NO2_NetBackup_Gateway_IP_Address></pre>


Procedure 5: Recovery Scenario 5

<p>19</p> <p><input type="checkbox"/></p>	<p>Recovered NOAM Server: Verify Server Health</p>	<p>Execute the following command on the failed NOAM server and make sure that no errors are returned:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>
<p>20</p> <p><input type="checkbox"/></p>	<p>Repeat for Additional 2nd Failed NOAM</p>	<p>Repeat steps 15-19 for the 2nd failed NOAM server.</p>
<p>21</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 admusr user, exchange SSH keys for admusr between the active NOAM and the recovered NOAM servers using the keyexchange utility, using the host names of the recovered NOAMs.</p> <p>When prompted for the password, enter the password for the admusr user of the recovered NOAM servers.</p> <pre style="border: 1px solid black; padding: 5px;">\$ keyexchange admusr@<Recovered_NOAM Hostname></pre>
<p>22</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>

Procedure 5: Recovery Scenario 5

<p>23</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> 
<p>24</p> <p><input type="checkbox"/></p>	<p>Recovered Active NOAM: Activate Optional Features</p>	<p>Map-Diameter Interworking (MAP-IWF) and/or Policy and Charging Application (PCA) Only</p> <p>Establish an SSH session to the recovered active NOAM, login as admusr.</p> <ul style="list-style-type: none"> • Refer to [7] to activate Map-Diameter Interworking (MAP-IWF) • Refer to [13] to activate Policy and Charging Application (PCA) <p>Note: While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:</p> <pre>iload#31000{S/W Fault}</pre>

Procedure 5: Recovery Scenario 5

<p>25 <input type="checkbox"/></p>	<p>DR-NOAM VIP: Copy key file to recovered NOAM servers in Topology (RADIUS Only)</p>	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Establish an SSH session to any of the Active DR NOAM which is intact and operational. Login as <i>admusr</i>.</p> <p>Execute following commands to check if existing Key file on Active DR NOAM server is valid :</p> <pre style="border: 1px solid black; padding: 5px;">\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -validate</pre> <p>Note: If errors are present, stop and contact Appendix L: My Oracle Support (MOS)</p> <p>If key file is valid, Execute following commands to copy Key file from Active DR NOAM server to recovered NOAMs :</p> <pre style="border: 1px solid black; padding: 5px;">\$./sharedKrevo -copyKey -destServer <First NOAM> \$./sharedKrevo -copyKey -destServer <Second NOAM></pre>
<p>26 <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>27 <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>
<p>28 <input type="checkbox"/></p>	<p>NOAM VIP GUI: Recover Standby/Spare SOAM and C-Level Servers</p>	<p>If necessary, refer to Procedure 3 to recover any standby or Spare SOAMs as well as any C-Level servers.</p>

Procedure 5: Recovery Scenario 5

<p>29 <input type="checkbox"/></p>	<p>NOAM VIP: Verify all servers in Topology are accessible (RADIUS Only)</p>	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Establish an SSH session to the NOAM VIP. Login as admusr.</p> <p>Execute following commands to check if all the servers in the Topology are accessible :</p> <pre style="border: 1px solid black; padding: 5px;">\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -checkAccess</pre> <p>Note: If any of the servers are not accessible, stop and Appendix L: My Oracle Support (MOS)</p>
<p>30 <input type="checkbox"/></p>	<p>NOAM VIP: Copy key file to all the servers in Topology (RADIUS Only)</p>	<p>Establish an SSH session to the Active NOAM, login as admusr.</p> <p>Execute following command to copy the key file to all the servers in the Topology :</p> <pre style="border: 1px solid black; padding: 5px;">\$./sharedKrevo -synchronize \$./sharedKrevo -updateData</pre> <p>Note: If errors are present, stop and contact Appendix L: My Oracle Support (MOS)</p>
<p>31 <input type="checkbox"/></p>	<p>Recover IDIH</p>	<p>If IDIH were affected, refer to Section 0 to perform disaster recovery on IDIH.</p>

5.1.6 Recovery Scenario 6 (Database Recovery)

5.1.6.1 Recovery Scenario 6: Case 1

For a partial outage with

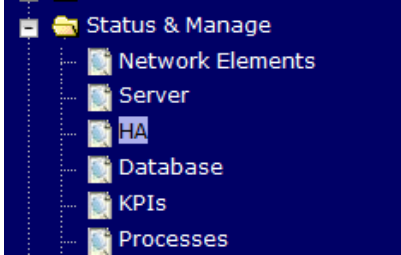
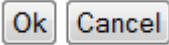
- Server having a corrupted database
- Replication channel from parent is inhibited because of upgrade activity or
- Server is in a different release than that of its Active parent because of upgrade activity.
- Verify that the Server Runtime backup files, performed at the start of the upgrade, are present 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 Server Runtime backup. Any configuration done after taking the backup will not be visible post recovery.

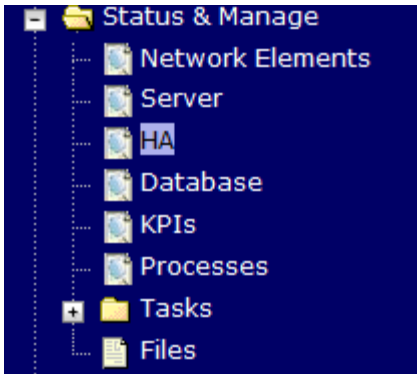
Procedure 6: Recovery Scenario 6 (Case 1)

S T E P #	This procedure performs recovery if database is corrupted in the system	
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.	
	If this procedure fails, contact Appendix L: My Oracle Support (MOS) and ask for assistance.	
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.

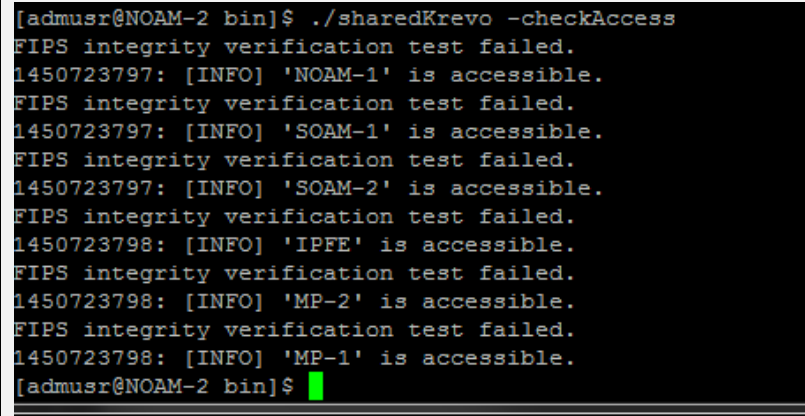
Procedure 6: Recovery Scenario 6 (Case 1)

<p>2</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: 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>3</p> <p><input type="checkbox"/></p>	<p>Server in Question: Login</p>	<p>Establish an SSH session to the server in question. Login as admusr.</p>
<p>4</p> <p><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</p> <p><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</p> <p><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>

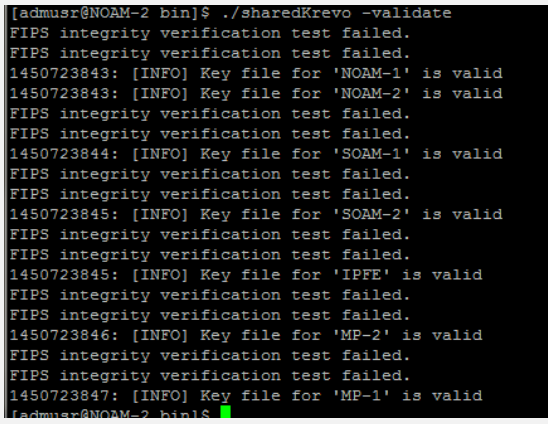
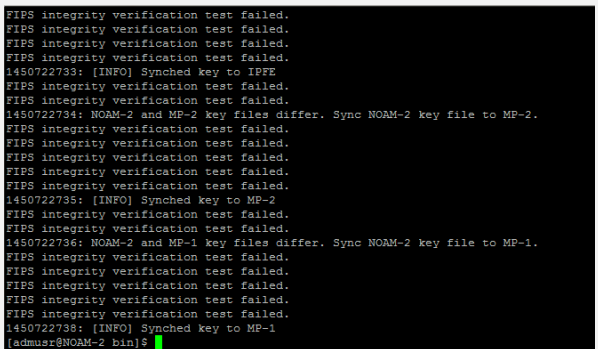
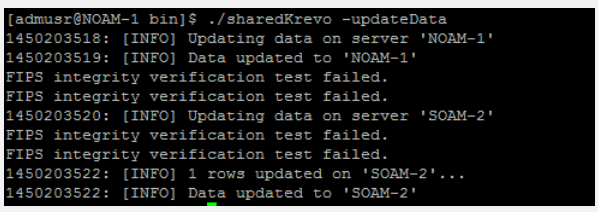
Procedure 6: Recovery Scenario 6 (Case 1)

<p>7</p> <p><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>Example Output:</p> <pre>A 5139 cmha Up 12/21 13:16:25 1 cmha A 5140 cmplatalarm Up 12/21 13:16:25 1 cmplatalarm A 5143 cmsnmpsa Up 12/21 13:16:25 1 cmsnmpsa -R 1.3.6.1.4.1.3 23.5.3.28.1 A 5145 cmsocapa Up 12/21 13:16:25 1 cmsocapa A 9969 eclipseHelp Up 12/21 13:16:39 1 eclipseHelp A 5149 idbsvc Up 12/21 13:16:25 1 idbsvc -M10 -ME204 -D40 - DE820 -W1 -S2 A 6149 idbunlock Up 12/21 13:16:36 1 idbunlock -f A 5151 inetmerge Up 12/21 13:16:25 1 inetmerge A 5155 inetrep Up 12/21 13:16:25 1 inetrep A 5160 oampAgent Up 12/21 13:16:25 1 oampAgent A 5164 pm.watchdog Up 12/21 13:16:25 1 pm.watchdog A 5167 raclerk Up 12/21 13:16:25 1 raclerk -r 6000 A 5171 re.portmap Up 12/21 13:16:25 1 re.portmap -c100 A 5174 statclerk Up 12/21 13:16:25 1 statclerk -s -0 A 5177 vipmgr Up 12/21 13:16:25 1 vipmgr A -1 AstateInit Done 12/21 13:16:36 1 AstateInit A -1 auditPTask Done 12/21 13:16:36 1 auditPeriodicTask A -1 auditTasks Done 12/21 13:16:36 1 auditDefunctTasks A -1 guiReqMapLoad Done 12/21 13:16:25 1 guiReqMapLoad A -1 mkdbhooks Done 12/21 13:16:25 1 mkdbhooks [root@MP-1 admusr]#</pre>
<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>

Procedure 6: Recovery Scenario 6 (Case 1)

<p>9 <input type="checkbox"/></p>	<p>NOAM VIP: Verify all servers in Topology are accessible (RADIUS Only)</p>	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Establish an SSH session to the NOAM VIP. Login as <i>admusr</i>.</p> <p>Execute following commands to check if all the servers in the Topology are accessible :</p> <pre>\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -checkAccess</pre>  <pre>[admusr@NOAM-2 bin]\$./sharedKrevo -checkAccess FIPS integrity verification test failed. 1450723797: [INFO] 'NOAM-1' is accessible. FIPS integrity verification test failed. 1450723797: [INFO] 'SOAM-1' is accessible. FIPS integrity verification test failed. 1450723797: [INFO] 'SOAM-2' is accessible. FIPS integrity verification test failed. 1450723798: [INFO] 'IPFE' is accessible. FIPS integrity verification test failed. 1450723798: [INFO] 'MP-2' is accessible. FIPS integrity verification test failed. 1450723798: [INFO] 'MP-1' is accessible. [admusr@NOAM-2 bin]\$</pre>
---------------------------------------	---	--

Procedure 6: Recovery Scenario 6 (Case 1)

10 <input type="checkbox"/>	NOAM VIP: Copy key file to all the servers in Topology (RADIUS Only)	If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)
Execute following commands to check if existing Key file on Active NOAM (The NOAM which is intact and was not recovered) server is valid :		
<pre>\$./sharedKrevo -validate</pre>  <pre>[admusr@NOAM-2 bin]\$./sharedKrevo -validate FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723843: [INFO] Key file for 'NOAM-1' is valid 1450723843: [INFO] Key file for 'NOAM-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723844: [INFO] Key file for 'SOAM-1' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723845: [INFO] Key file for 'SOAM-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723845: [INFO] Key file for 'IPFE' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723846: [INFO] Key file for 'MP-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723847: [INFO] Key file for 'MP-1' is valid [admusr@NOAM-2 bin]\$</pre>		
If output of above command shows that the existing key file is not valid, contact Appendix L: My Oracle Support (MOS)		
Execute following command to copy the key file to all the servers in the Topology :		
<pre>\$./sharedKrevo -synchronize</pre>  <pre>FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722733: [INFO] Synced key to IPFE FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722734: NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722736: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722738: [INFO] Synced key to MP-1 [admusr@NOAM-2 bin]\$</pre>		
<pre>\$./sharedKrevo -updateData</pre>  <pre>[admusr@NOAM-1 bin]\$./sharedKrevo -updateData 1450203518: [INFO] Updating data on server 'NOAM-1' 1450203519: [INFO] Data updated to 'NOAM-1' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203520: [INFO] Updating data on server 'SOAM-2' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203522: [INFO] 1 rows updated on 'SOAM-2'... 1450203522: [INFO] Data updated to 'SOAM-2'</pre>		
Note: If any errors are present, stop and contact Appendix L: My Oracle Support (MOS)		

Procedure 6: Recovery Scenario 6 (Case 1)

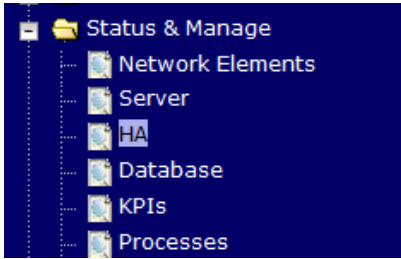
11 <input type="checkbox"/>	Backup and Archive All the Databases from the Recovered System	Execute Appendix A: DSR Database Backup to back up the Configuration databases:
--------------------------------	---	--

5.1.6.2 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 L: 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"/>	<p>NOAM VIP GUI: 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 style="text-align: center;"><input type="button" value="Ok"/> <input type="button" value="Cancel"/></p>

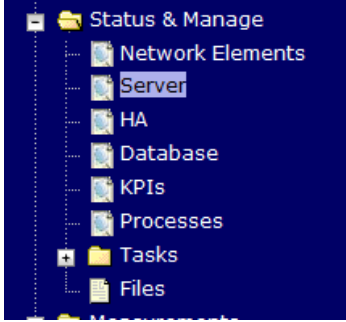
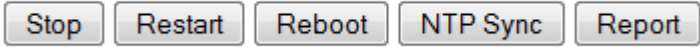
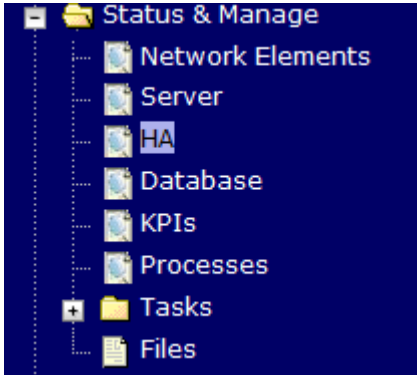
Procedure 7: Recovery Scenario 6 (Case 2)

3 <input type="checkbox"/>	Server in Question: Login	Establish an SSH session to the server in question. Login as admusr .
4 <input type="checkbox"/>	Server in Question: Take Server out of Service	Execute the following command to take the server out of service. <pre>\$ sudo bash -l \$ prod.clobber</pre>
5 <input type="checkbox"/>	Server in Question: Take Server to DbUp State and Start the Application	Execute the following commands to take the server to Dbup and start the DSR application: <pre>\$ prod.start</pre> Exit out of root: <pre>\$ exit</pre>

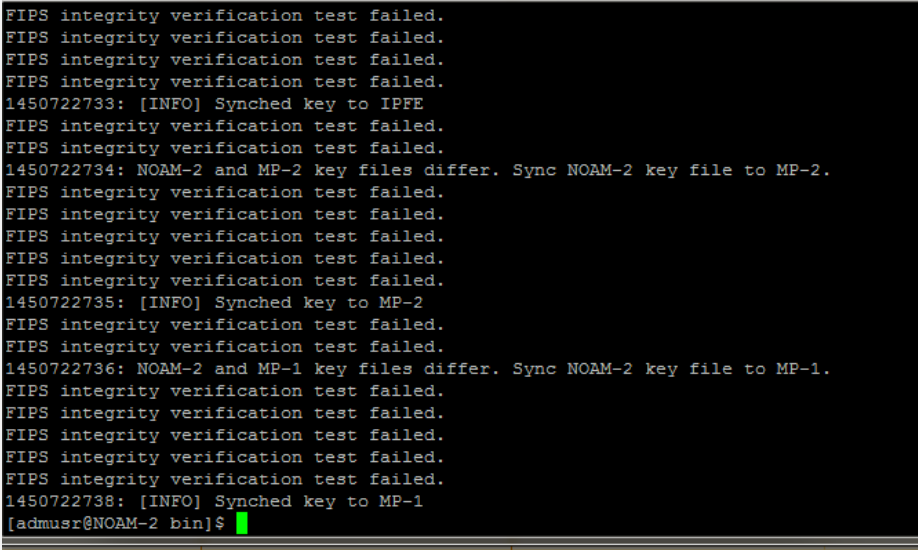
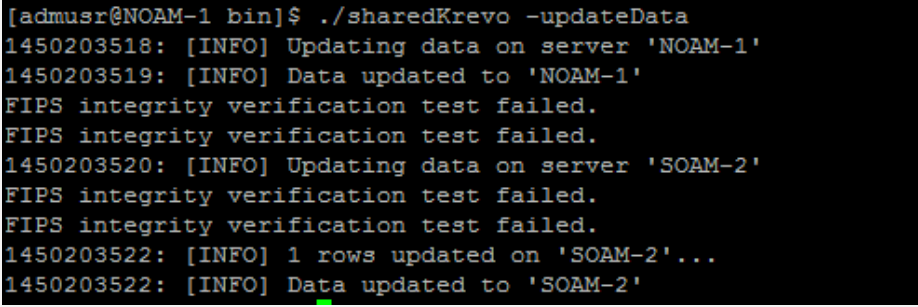
Procedure 7: Recovery Scenario 6 (Case 2)

<p>6</p> <p>□</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>Example Output:</p> <pre>A 5139 cmha Up 12/21 13:16:25 1 cmha A 5140 cmplatalarm Up 12/21 13:16:25 1 cmplatalarm A 5143 cmsnmpsa Up 12/21 13:16:25 1 cmsnmpsa -R 1.3.6.1.4.1.3 23.5.3.28.1 A 5145 cmsoapa Up 12/21 13:16:25 1 cmsoapa A 9969 eclipseHelp Up 12/21 13:16:39 1 eclipseHelp A 5149 idbsvc Up 12/21 13:16:25 1 idbsvc -M10 -ME204 -D40 - DE820 -W1 -S2 A 6149 idbunlock Up 12/21 13:16:36 1 idbunlock -f A 5151 inetmerge Up 12/21 13:16:25 1 inetmerge A 5155 inetrep Up 12/21 13:16:25 1 inetrep A 5160 oampAgent Up 12/21 13:16:25 1 oampAgent A 5164 pm.watchdog Up 12/21 13:16:25 1 pm.watchdog A 5167 raclerk Up 12/21 13:16:25 1 raclerk -r 6000 A 5171 re.portmap Up 12/21 13:16:25 1 re.portmap -c100 A 5174 statclerk Up 12/21 13:16:25 1 statclerk -s -0 A 5177 vipmgr Up 12/21 13:16:25 1 vipmgr A -1 AstateInit Done 12/21 13:16:36 1 AstateInit A -1 auditPTask Done 12/21 13:16:36 1 auditPeriodicTask A -1 auditTasks Done 12/21 13:16:36 1 auditDefunctTasks A -1 guiReqMapLoad Done 12/21 13:16:25 1 guiReqMapLoad A -1 mkdbhooks Done 12/21 13:16:25 1 mkdbhooks [root@MP-1 admusr]#</pre> <p>Execute the following command to verify if replication channels are up and running:</p> <pre>\$ sudo irepstat</pre> <p>Example Output:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- BC From SOAM-2 Active 0 0.50 ^0.04%cpu 34B/s A=C2713.145 CC From MP-2 Active 0 0.20 ^0.05 1.57%cpu 35B/s A=C2713.145 -- Policy 1001 DSR_SLDB_Policy [] ----- 1 CC From MP-2 Active 0 0.20 ^0.06 1.51%cpu 35B/s A=C2713.145</pre> <p>Execute the following command to verify if merging channels are up and running:</p> <pre>\$ sudo inetmstat</pre> <p>Example Output:</p> <pre>nodeId InetMerge State dir dSeq dTime updTime info SOAM-1 Standby To 0 0.00 13:19:33 SOAM-2 Active To 0 0.00 13:19:33 ~ ~</pre>
-------------------	---	---

Procedure 7: Recovery Scenario 6 (Case 2)

<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>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>NOAM VIP: Verify all servers in Topology are accessible (RADIUS Only)</p>	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Establish an SSH session to the NOAM VIP. Login as admusr.</p> <p>Execute following commands to check if all the servers in the Topology are accessible :</p> <pre style="border: 1px solid black; padding: 5px;">\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -checkAccess</pre>

Procedure 7: Recovery Scenario 6 (Case 2)

<p>10 <input type="checkbox"/></p>	<p>NOAM VIP: Copy key file to all the servers in Topology (RADIUS Only)</p>	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Execute following commands to check if existing Key file on Active NOAM (The NOAM which is intact and was not recovered) server is valid :</p> <pre>\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -validate</pre> <p>If output of above command shows that the existing key file is not valid, contact Appendix L: My Oracle Support (MOS)</p> <p>Execute following command to copy the key file to all the servers in the Topology :</p> <pre>\$./sharedKrevo -synchronize</pre>  <pre>\$./sharedKrevo -updateData</pre>  <p>Note: If any errors are present, stop and contact Appendix L: My Oracle Support (MOS)</p>
--	--	---

Procedure 7: Recovery Scenario 6 (Case 2)

12 <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:
--------------------------------	---	--

6.0 Resolving User Credential Issues after Database Restore

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


6.1 Restoring a Deleted User

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

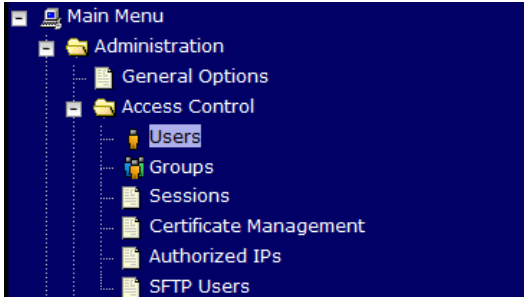

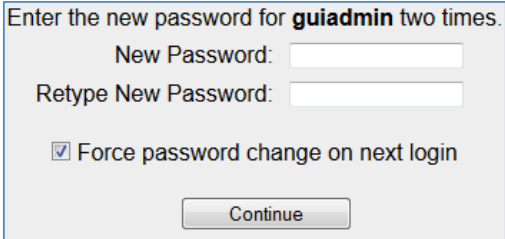
These users were removed prior to creation of the backup and archive file. They will be reintroduced by system restoration of that file.

6.2 Keeping a Restored user

Procedure 8: Keep Restored User

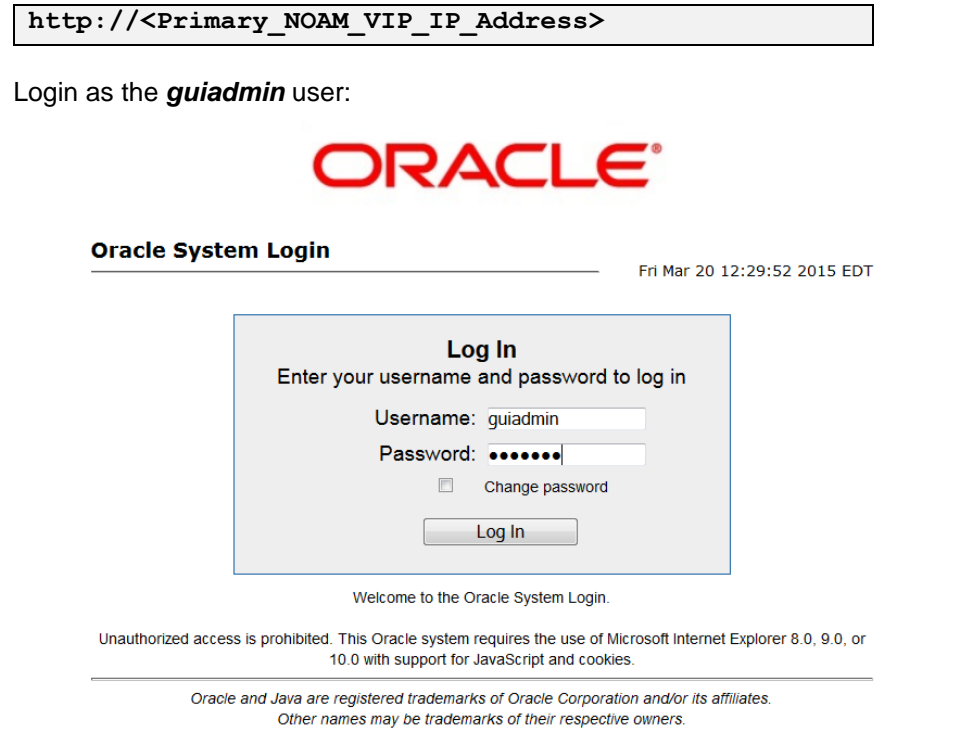
S T E P #	<p>Perform this procedure to keep users that will be restored by system restoration.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact Appendix L: My Oracle Support (MOS) and ask for assistance.</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

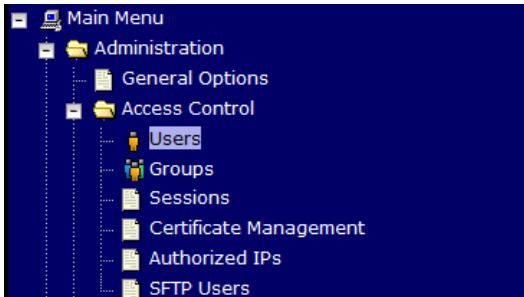
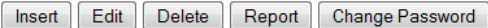
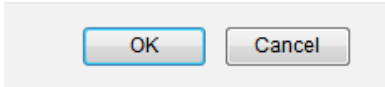
<p>3</p> <p>□</p>	<p>After Restoration: Reset User Passwords</p>	<p>Navigate to Administration -> Access Control -> Users</p>  <p>Select the user</p> <p>Click the Change Password button</p>  <p>Enter a new password</p>  <p>Click the Continue button</p>
-------------------	---	---

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 L: 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 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 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.

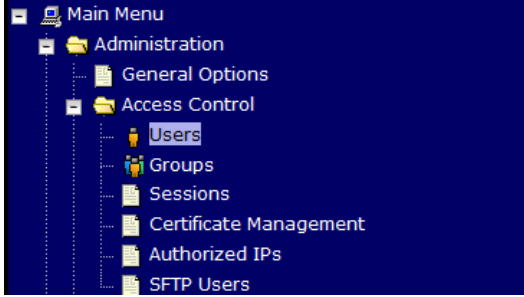

- User 'testuser' exists in current database but not in the selected backup file.

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

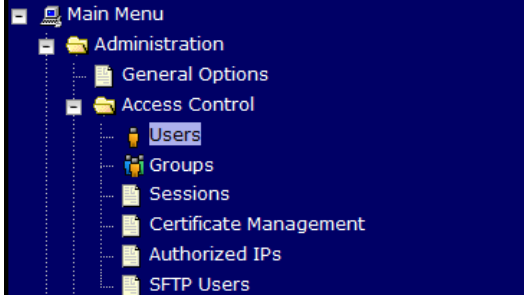
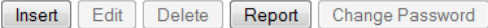

Procedure 10: Restoring an Archive that does not Contain a Current User

S T E P #	<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 L: 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>Before 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; 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> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> <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> <table border="1" data-bbox="488 800 1008 1220"> <tr> <td>Username</td> <td><input type="text"/></td> </tr> <tr> <td>Group</td> <td>admin</td> </tr> <tr> <td>Authentication Options</td> <td> <input type="checkbox"/> Allow Remote Auth <input checked="" type="checkbox"/> Allow Local Auth </td> </tr> <tr> <td>Access Allowed</td> <td><input checked="" type="checkbox"/> Account Enabled</td> </tr> <tr> <td>Maximum Concurrent Logins</td> <td><input type="text" value="0"/></td> </tr> <tr> <td>Session Inactivity Limit</td> <td><input type="text" value="120"/></td> </tr> <tr> <td>Comment</td> <td><input type="text"/></td> </tr> </table> <p>Click Ok</p> 	Username	<input type="text"/>	Group	admin	Authentication Options	<input type="checkbox"/> Allow Remote Auth <input checked="" type="checkbox"/> Allow Local Auth	Access Allowed	<input checked="" type="checkbox"/> Account Enabled	Maximum Concurrent Logins	<input type="text" value="0"/>	Session Inactivity Limit	<input type="text" value="120"/>	Comment	<input type="text"/>
Username	<input type="text"/>															
Group	admin															
Authentication Options	<input type="checkbox"/> Allow Remote Auth <input checked="" type="checkbox"/> Allow Local Auth															
Access Allowed	<input checked="" type="checkbox"/> Account Enabled															
Maximum Concurrent Logins	<input type="text" value="0"/>															
Session Inactivity Limit	<input type="text" value="120"/>															
Comment	<input type="text"/>															
<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>														

6.6 IDIH Disaster Recovery

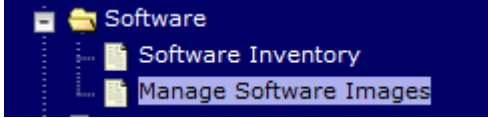
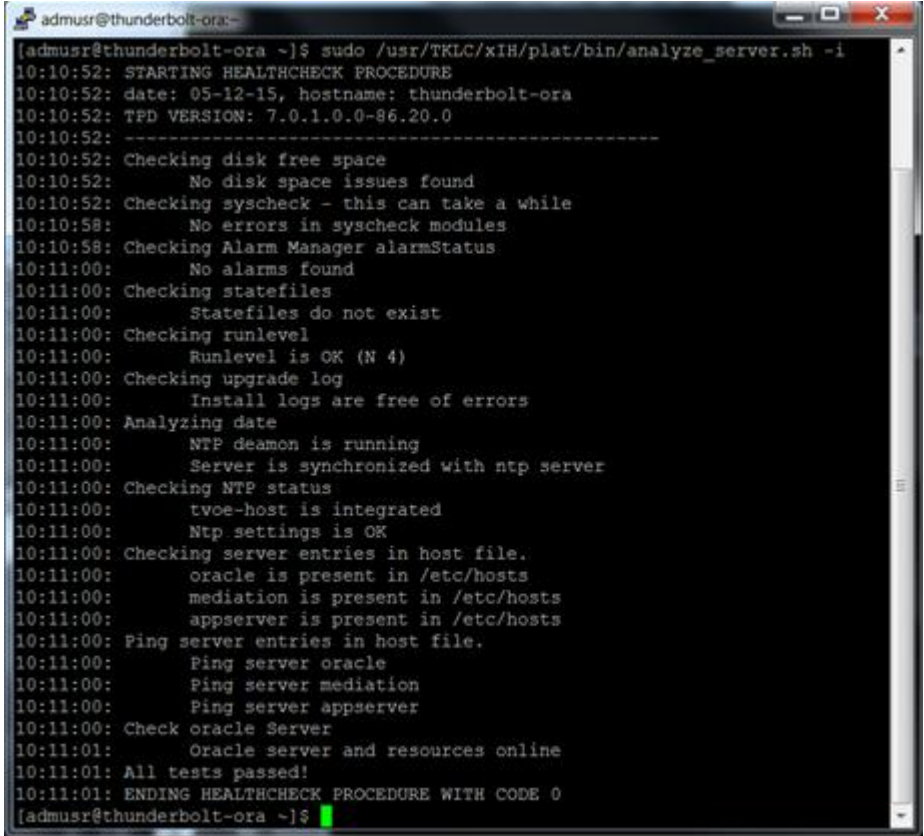
The fdconfig xml file you use for disaster recovery is different from the one used for fresh installation. The one for disaster recovery has hostname-**upgrade_xx-xx-xx.xml** file format. It took out the oracle server installation part since for disaster recovery it is not needed.

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.

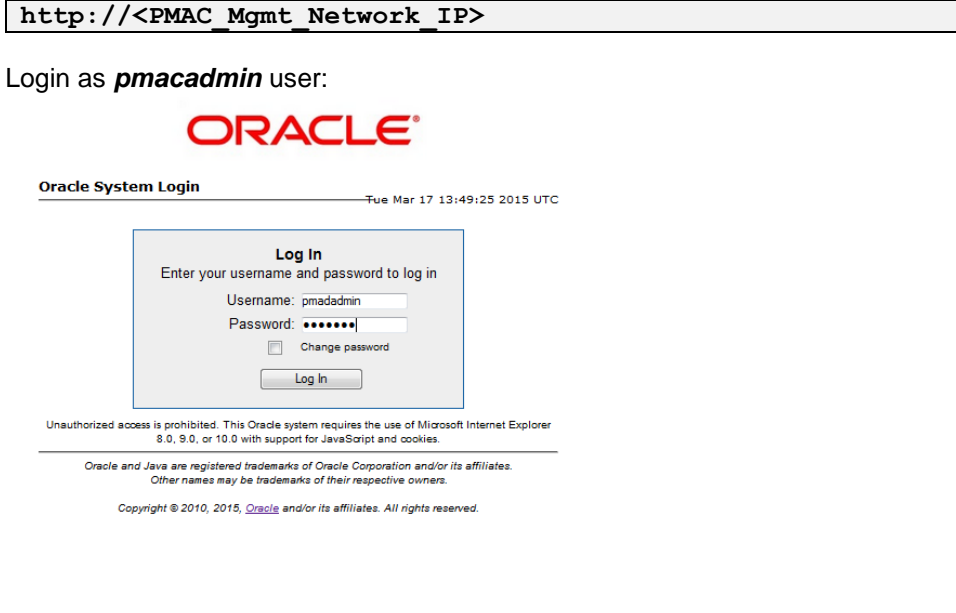
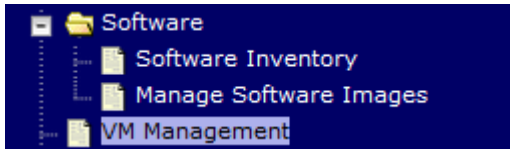

Procedure 11: IDIH Disaster Recovery Preparation

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 L: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	<p>PMAC GUI: Login</p>	<p>Open web browser and enter:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p>http://<PMAC Mgmt Network IP></p> </div> <p>Login as pmacadmin user:</p> 

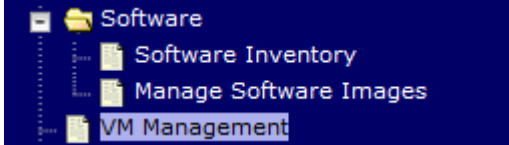


Procedure 11: IDIH Disaster Recovery Preparation

<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 procedure "Load Application and TPD ISO onto PMAC Server" and procedure "IDIH Configuration" steps 1-4 from [8] to acquire and transfer the images.</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>\$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i</pre> <p>Output:</p>  <pre>admusr@thunderbolt-ora:~\$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i 10:10:52: STARTING HEALTHCHECK PROCEDURE 10:10:52: date: 05-12-15, hostname: thunderbolt-ora 10:10:52: TPD VERSION: 7.0.1.0.0-86.20.0 10:10:52: ----- 10:10:52: Checking disk free space 10:10:52: No disk space issues found 10:10:52: Checking syscheck - this can take a while 10:10:58: No errors in syscheck modules 10:10:58: Checking Alarm Manager alarmStatus 10:11:00: No alarms found 10:11:00: Checking statefiles 10:11:00: Statefiles do not exist 10:11:00: Checking runlevel 10:11:00: Runlevel is OK (N 4) 10:11:00: Checking upgrade log 10:11:00: Install logs are free of errors 10:11:00: Analyzing date 10:11:00: NTP daemon is running 10:11:00: Server is synchronized with ntp server 10:11:00: Checking NTP status 10:11:00: tvoe-host is integrated 10:11:00: Ntp settings is OK 10:11:00: Checking server entries in host file. 10:11:00: oracle is present in /etc/hosts 10:11:00: mediation is present in /etc/hosts 10:11:00: appserver is present in /etc/hosts 10:11:00: Ping server entries in host file. 10:11:00: Ping server oracle 10:11:00: Ping server mediation 10:11:00: Ping server appserver 10:11:00: Check oracle Server 10:11:01: Oracle server and resources online 10:11:01: All tests passed! 10:11:01: ENDING HEALTHCHECK PROCEDURE WITH CODE 0 admusr@thunderbolt-ora ~]\$</pre>

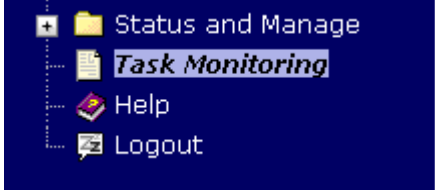
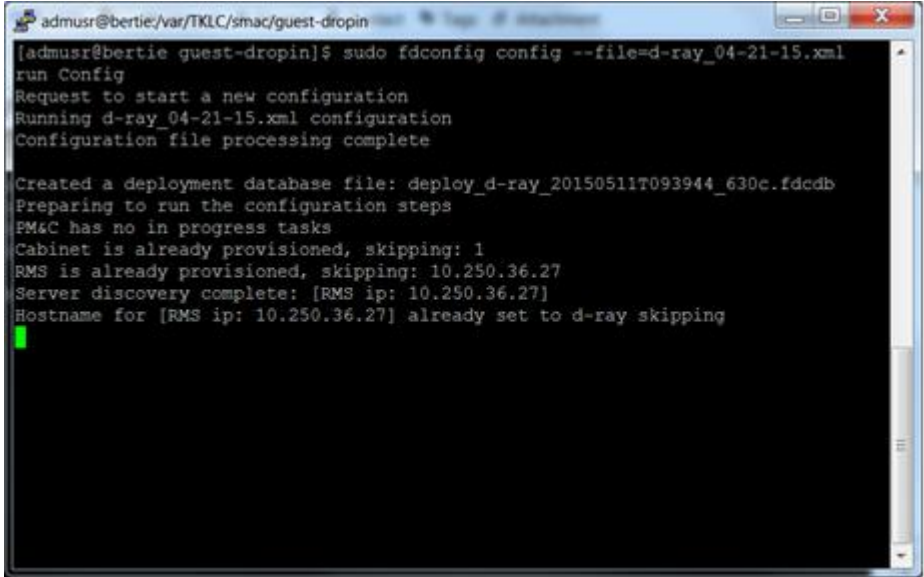
Procedure 12: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

<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 L: 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 1096"> \$ cd /var/TKLC/smac/guest-dropin \$ screen \$ 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> <p>Note: This is a long duration command (45-90 Minutes). If the screen command was run prior to executing the fdconfig, perform a “<i>screen -dr</i>” to resume the screen session in the event of a terminal timeout etc.</p>

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

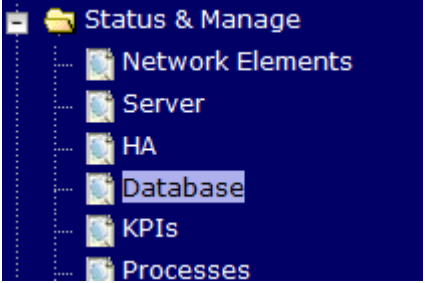
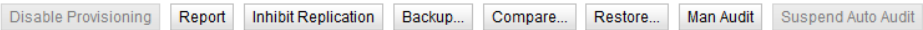
<p>6</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Monitor the Configuration</p>	<p>If not already done so, establish a GUI session on the PMAC server.</p> <p>Navigate to Main Menu -> Task Monitoring</p>  <p>Monitor the IDIH configuration to completion.</p> <p>Alternatively, you can monitor the fdconfig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

Appendix A: DSR Database Backup

Procedure 13: DSR Database Backup

<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 L: 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 style="border: 1px solid black; padding: 5px; width: fit-content; margin: 10px auto;"> <p>http://<Primary_NOAM/SOAM_VIP_IP_Address></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 13: DSR Database Backup

<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"><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_09311: *</td></tr><tr><td>Comment</td><td><input type="text"/></td></tr></tbody></table> <p>Ok 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_09311: *	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_09311: *													
Comment	<input type="text"/>													

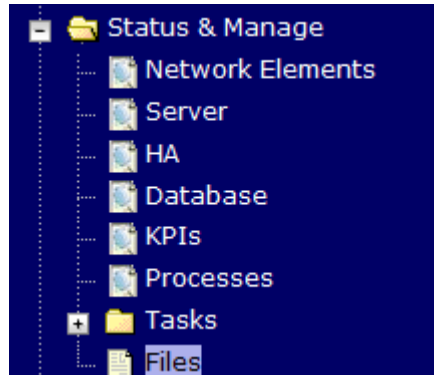
Procedure 13: DSR Database Backup

3

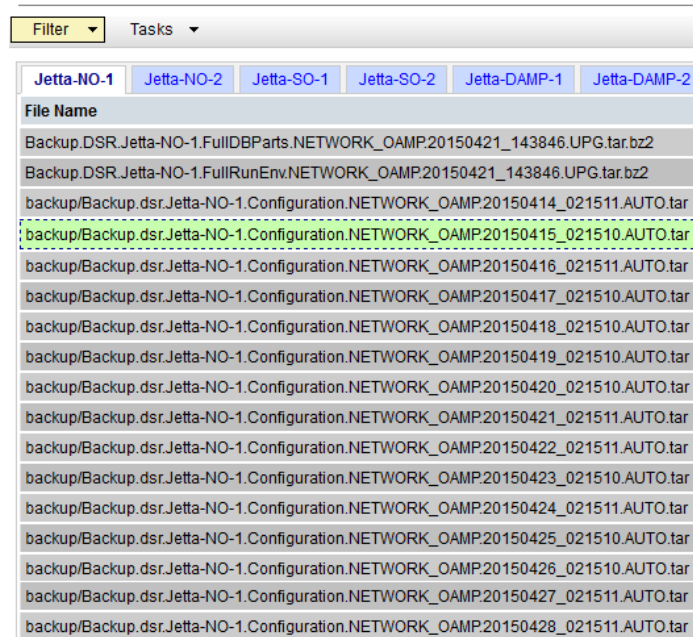


NOAM/SOAM VIP: Verify the backup file existence.

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



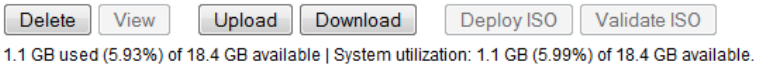
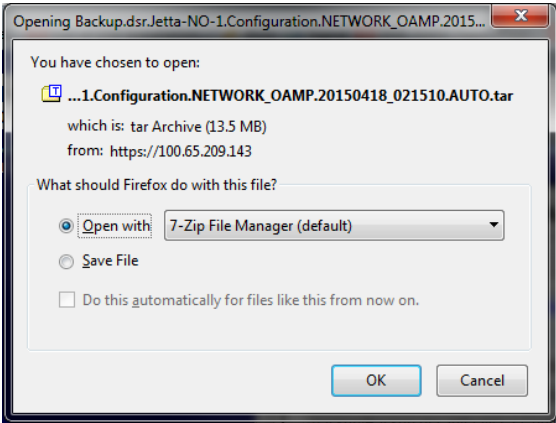
Main Menu: Status & Manage -> Files



Select the Active NOAM or SOAM tab.

The files on this server will be displayed. Verify the existence of the backup file.

Procedure 13: DSR Database Backup

<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>

Procedure 13: DSR Database Backup

<p>7</p> <p>□</p>	<p>Take Secured backup of key file (RADIUS Only)</p>	<p>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</p> <p>Login to ssh shell of Active NOAM server using user admusr</p> <p>Take secure backup of updated key file “RADIUS shared secret encryption key” for disaster scenarios.</p> <p>Execute following command to encrypt the key file before being backed up to secure customer setup :</p> <pre>\$./sharedKrevo -encr</pre> <p>Execute following command to copy the encrypted key file to secure customer setup :</p> <pre>\$ sudo scp /var/TKLC/db/filemgmt/DpiKf.bin.encr user@<customer IP>:<path of customer setup></pre> <p>Note: Access to backed up key file must be strictly controlled by the operator. If the operator wishes to further encrypt this key file using operator specified encryption techniques, the operator is recommended to do so, however the operator shall be responsible to decrypt this file using operator specific decryption techniques and copy the resulting DpiKf.bin.encr file securely to the file management folder if the key file needs to be restored for disaster recovery. Once the key file is backed up to the operator provided server and path, it is the responsibility of the operator to ensure access to the backed up key file is extremely selective and restricted</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 L: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	<p>Recover failed Aggregation Switches: Cisco 4948E/4948E-F</p>	<p>Login to the PMAC via SSH as admusr</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 from reference [2]</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 the information used to populate them can be obtained from the NAPD.</p>

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

S T E 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 L: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	<p>Recover failed Enclosure Switch: Cisco 3020</p>	<p>Login to the PMAC via SSH as <i>admusr</i></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>“Replace a failed 3020 switch (netConfig)”</i> to replace the failed enclosure switch from reference [2]</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 the information used to populate them can be obtained from the NAPD.</p>

Procedure 16: Recovering a Failed Enclosure Switch (HP 6120XG , HP 6125XLG, HP 6125G)

S T E P #	<p>The intent of this procedure is to recover a failed Enclosure (6120XG/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 L: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	<p>Recover failed Enclosure Switch: HP 6120XG/6125XLG/6125G</p>	<p>Login to the PMAC via SSH as <i>admusr</i></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>Replace a failed HP (6120XG, 6125G, 6125XLG switch (netConfig)</i>” to replace the failed enclosure switch from reference [2].</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 the information used to populate them can be obtained from the NAPD.</p>

Procedure 17: 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 L: My Oracle Support (MOS) and ask for assistance.	
1 <input type="checkbox"/>	Recover Failed Enclosure OA	Refer to procedure <i>“Restore OA Configuration from Management Server”</i> to replace a failed Enclosure OA from reference [2].

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.

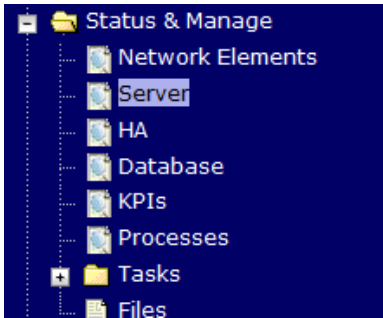
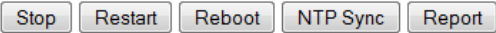
Preconditions:

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

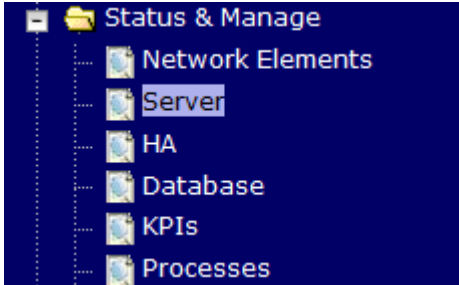
Procedure 18: Switching a DR NOAM Site to Primary

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 L: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	<p>Active DR-NOAM: Login</p>	<p>Establish a GUI session on the active DR-NOAM server by using the xmi 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> <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>

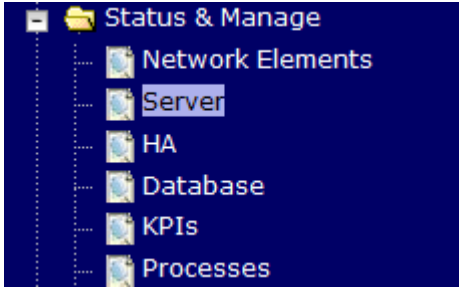
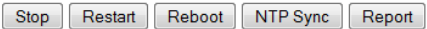
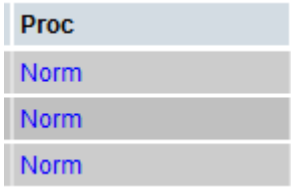
Procedure 18: Switching a DR NOAM Site to Primary

<p>2</p> <p><input type="checkbox"/></p>	<p>Active DR-NOAM: 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>4</p> <p><input type="checkbox"/></p>	<p>DR-NOAM: Repeat</p>	<p>Repeat steps 1-2 to disable the DSR application on the standby DR NOAM.</p> <p>Note: The DSR application should now be stopped on all DR-NOAMs.</p>
<p>5</p> <p><input type="checkbox"/></p>	<p>DR-NOAM: 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</p> <p><input type="checkbox"/></p>	<p>Primary DR-NOAM: Establish an SSH session</p>	<p>Login via SSH to the physical IP of the chosen primary DR-NOAM server as admusr user.</p>

Procedure 18: Switching a DR NOAM Site to Primary


<p>7 □</p>	<p>Primary DR-NOAM: Change Role to Primary</p>	<p>Execute the command</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo top.setPrimary</pre> <p>Note: This step makes the DR DSR take over as the Primary.</p> <p>Execute the following command to verify the role was changed to primary:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo top.myrole myNodeId=A1250.248 myMasterCapable=true myMateNodeId=A1250.249 myParentCluster=00000 myClusterRole=Primary myClusterTimestamp=02/26/16 09:35:58.922</pre> <p>System generates Several replication and collection alarms as replication/collection links to/from former Primary NOAM servers becomes inactive.</p>								
<p>8 □</p>	<p>Primary DR-NOAM: 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 1461 943 1604"> <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 18: Switching a DR NOAM Site to Primary

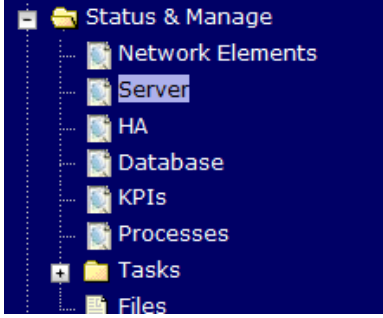
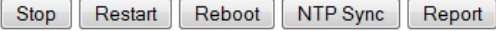
<p>9</p> <p><input type="checkbox"/></p>	<p>New Primary NOAM: Re-enable the application.</p>	<p>Navigate to Main Menu -> Status & Manage -> Server</p>  <p>Select the row that has the active New-Primary NOAM server.</p> <p>Click the Restart button and then click the OK button.</p>  <p>Verify that "PROC" 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: Repeat for standby of new-primary NOAM Server</p>	<p>Repeat steps 8-9 for standby of the new-Primary NOAM server.</p>

Appendix D: Returning a Recovered Site to Primary

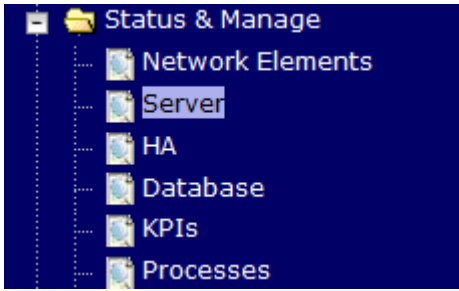
Procedure 19: Returning a Recovered Site to Primary

<p>S T E P #</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 L: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>Primary Active NOAM: 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 data-bbox="488 722 1346 764" style="border: 1px solid black; padding: 2px;"> <p>http://<Primary_NOAM_VIP_IP_Address></p> </div> <p>Login as the <i>guiadmin</i> user:</p> <div data-bbox="565 856 1349 1444" 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 on the left, and the date 'Fri Mar 20 12:29:52 2015 EDT' is on the right. A central box contains a 'Log In' form with the instruction 'Enter your username and password to log in'. The form has two input fields: 'Username' with 'guiadmin' entered and 'Password' with seven dots. There is a 'Change password' checkbox and a 'Log In' button. Below the form, it says 'Welcome to the Oracle System Login.' At the bottom, a disclaimer states: '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.' A footer line reads: '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 19: Returning a Recovered Site to Primary

<p>2</p> <p><input type="checkbox"/></p>	<p>Primary Active NOAM: 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>3</p> <p><input type="checkbox"/></p>	<p>Primary Standby NOAM: Repeat</p>	<p>Repeat steps 1-2 to disable the DSR application on the standby DR NOAM.</p> <p>Note: The DSR application should now be stopped on all DR-NOAMs.</p>
<p>4</p> <p><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>5</p> <p><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 admusr</p>
<p>6</p> <p><input type="checkbox"/></p>	<p>Primary NOAM VIP: Change Role to Secondary</p>	<p>Execute the command</p> <pre>\$ 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>\$ sudo top.myrole myNodeId=A1250.249 myMasterCapable=true myMateNodeId=A1250.248 myParentCluster=00000 myClusterRole=Secondary myClusterTimestamp=02/26/16 10:00:20.047</pre>

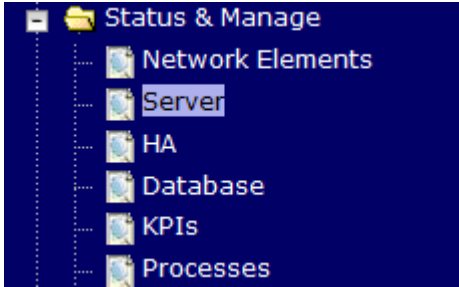
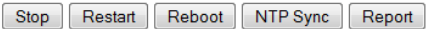
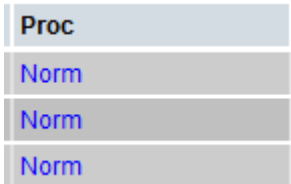
Procedure 19: Returning a Recovered Site to Primary

<p>7</p> <p><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="488 716 943 863"> <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									
<p>8</p> <p><input type="checkbox"/></p>	<p>To-Be-Primary NOAM VIP: Establish an SSH session</p>	<p>Login via SSH to the VIP of the chosen primary DR-NOAM server as admusr user.</p>								
<p>9</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 data-bbox="488 1077 883 1119">\$ 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 data-bbox="488 1272 1182 1539">\$ sudo top.myrole myNodeId=A1055.206 myMasterCapable=true myMateNodeId=A1055.214 myParentCluster=00000 myClusterRole=Primary myClusterTimestamp=02/26/16 10:01:52.162</pre> <p>System generates Several replication and collection alarms as replication/collection links to/from former Primary NOAM servers becomes inactive.</p>								

Procedure 19: Returning a Recovered Site to Primary

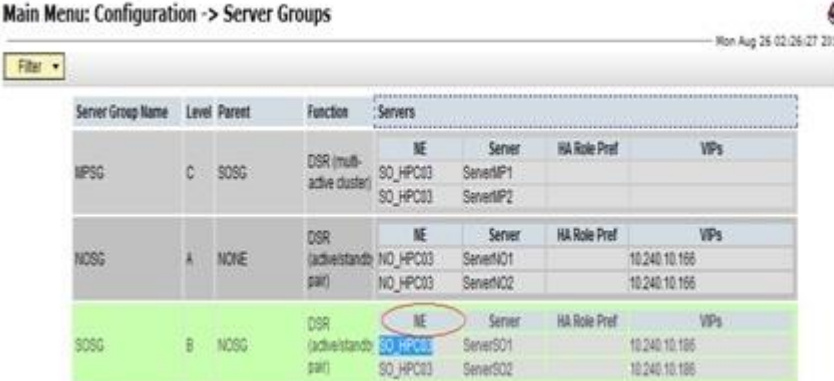
<p>10</p> <p><input type="checkbox"/></p>	<p>Primary Active NOAM: Login</p>	<p>Establish a GUI session on the primary NOAM server by using the VIP IP address of the primary NOAM.</p> <p>Open the web browser and enter a URL of:</p> <div data-bbox="492 396 1346 438" style="border: 1px solid black; padding: 2px;"><p><code>http://<Primary_NOAM_VIP_IP_Address></code></p></div> <p>Login as the <i>guiadmin</i> user:</p> <div data-bbox="565 531 1349 1119" style="text-align: center;"></div>
---	--	---

Procedure 19: Returning a Recovered Site to Primary

<p>11</p> <p><input type="checkbox"/></p>	<p>New Primary DSR NOAM VIP: Re-enable the application.</p>	<p>Navigate to Main Menu -> Status & Manage -> Server</p>  <p>Select the row that has the new primary active 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>12</p> <p><input type="checkbox"/></p>	<p>New Primary DSR NOAM VIP: Repeat on Standby NOAM</p>	<p>Repeat Step 11 on the standby primary NOAM server</p> <p>Provisioning can now resume to the VIP of the new-Primary DSR.</p>
<p>13</p> <p><input type="checkbox"/></p>	<p>New Primary DSR NOAM VIP: Repeat on DR-NOAMs</p>	<p>Repeat Step 11 on the active and standby DR-NOAMs</p>

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

Procedure 20: 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 L: 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 admusr</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 20: 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>\$ 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 21: Un-Inhibit A and B Level Replication on C-Level Servers

S T E P #	<p>The intent of this procedure is to Un-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 L: My Oracle Support (MOS) and ask for assistance.</p>																																													
1 <input type="checkbox"/>	Active NOAM: Login	Login to the Active NOAM server via SSH as admusr																																												
2 <input type="checkbox"/>	Active NOAM: Un-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>'); do iset -finhibitRepPlans='' NodeInfo where "nodeName='<i>\$i</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> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Server Group Name</th> <th>Level</th> <th>Parent</th> <th>Function</th> <th>NE</th> <th>Server</th> <th>HA Role Pref</th> <th>VIPs</th> </tr> </thead> <tbody> <tr> <td rowspan="2">NPSG</td> <td rowspan="2">C</td> <td rowspan="2">SOSG</td> <td rowspan="2">DSR (multi-active cluster)</td> <td>SO_HPC03</td> <td>ServerMP1</td> <td></td> <td></td> </tr> <tr> <td>SO_HPC03</td> <td>ServerMP2</td> <td></td> <td></td> </tr> <tr> <td rowspan="2">NOSG</td> <td rowspan="2">A</td> <td rowspan="2">NONE</td> <td rowspan="2">DSR (active/standby pair)</td> <td>NO_HPC03</td> <td>ServerNO1</td> <td></td> <td>10.240.10.166</td> </tr> <tr> <td>NO_HPC03</td> <td>ServerNO2</td> <td></td> <td>10.240.10.166</td> </tr> <tr> <td rowspan="2">SOSG</td> <td rowspan="2">B</td> <td rowspan="2">NOSG</td> <td rowspan="2">DSR (active/standby pair)</td> <td>SO_HPC03</td> <td>ServerSO1</td> <td></td> <td>10.240.10.166</td> </tr> <tr> <td>SO_HPC03</td> <td>ServerSO2</td> <td></td> <td>10.240.10.166</td> </tr> </tbody> </table>	Server Group Name	Level	Parent	Function	NE	Server	HA Role Pref	VIPs	NPSG	C	SOSG	DSR (multi-active cluster)	SO_HPC03	ServerMP1			SO_HPC03	ServerMP2			NOSG	A	NONE	DSR (active/standby pair)	NO_HPC03	ServerNO1		10.240.10.166	NO_HPC03	ServerNO2		10.240.10.166	SOSG	B	NOSG	DSR (active/standby pair)	SO_HPC03	ServerSO1		10.240.10.166	SO_HPC03	ServerSO2		10.240.10.166
Server Group Name	Level	Parent	Function	NE	Server	HA Role Pref	VIPs																																							
NPSG	C	SOSG	DSR (multi-active cluster)	SO_HPC03	ServerMP1																																									
				SO_HPC03	ServerMP2																																									
NOSG	A	NONE	DSR (active/standby pair)	NO_HPC03	ServerNO1		10.240.10.166																																							
				NO_HPC03	ServerNO2		10.240.10.166																																							
SOSG	B	NOSG	DSR (active/standby pair)	SO_HPC03	ServerSO1		10.240.10.166																																							
				SO_HPC03	ServerSO2		10.240.10.166																																							

Procedure 21: 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
Incorrect NodeID		
Inetsync alarms after performing disaster recovery	222828	Restart the Inetsync service on all affected servers using the following commands: <pre data-bbox="656 489 1135 564">\$ pm.set off inetsync \$ pm.set on inetsync</pre>

Appendix H: Restore TVOE Configuration from Backup Media

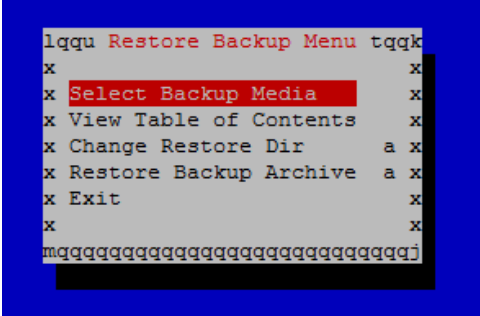
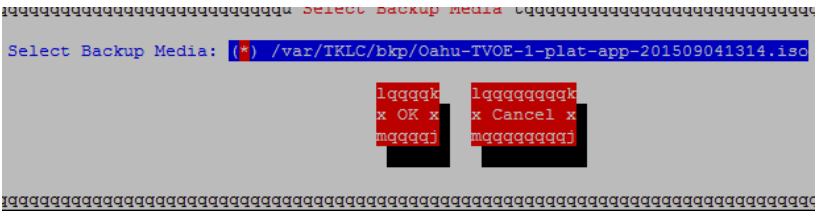
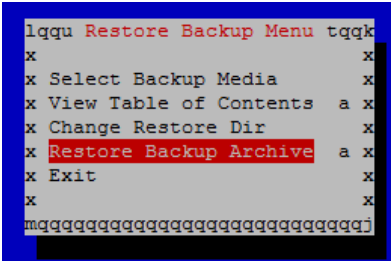
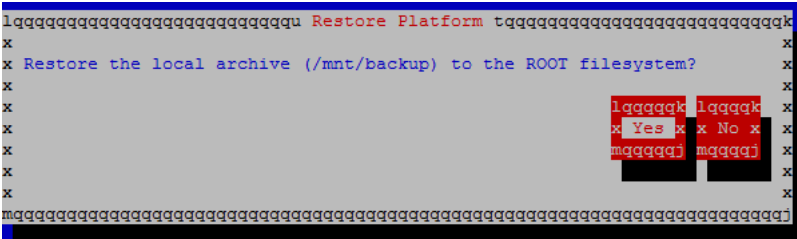
Procedure 22: Restore TVOE Configuration from Backup Media

S T E P #	<p>This procedure provides steps to restore the TVOE application configuration from backup media.</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 L: My Oracle Support (MOS) and ask for assistance</p>	
1 <input type="checkbox"/>	<p>Install TVOE Application</p>	<ul style="list-style-type: none"> • If the PMAC is NOT hosted on the failed rack mount server, follow procedure “<i>IPM Servers Using PM&C Application</i>” from reference [10] • If the PMAC is hosted on the failed rack mount server, follow procedure “<i>Installing TVOE on the Management Server</i>” from reference [10]
2 <input type="checkbox"/>	<p>Establish network connectivity</p>	<ul style="list-style-type: none"> • If the PMAC is NOT hosted on the failed rack mount server, skip this step • If the PMAC is hosted on the failed rack mount server, execute procedure “TVOE Network Configuration” steps 1-11 from reference [10] <p>Note: The IP address that is configured on the TVOE must be one that will be accessible via the network of the machine that currently holds the TVOE Backup ISO image. This could be a NetBackup Master Server, a Customer PC, etc.</p>
3 <input type="checkbox"/>	<p>Restore TVOE Backup ISO image to the TVOE host (NetBackup)</p>	<p>If using NetBackup to restore the TVOE backup ISO image execute this step, otherwise skip this step</p> <ol style="list-style-type: none"> 1. Execute Appendix “Application NetBackup Client Installation Procedures” from reference [8] 2. Interface with the NetBackup Master Server and initiate a restore of the TVOE backup ISO image. <p>Note: Once restored, the ISO image will be in <code>/var/TKLC/bkp/</code> on the TVOE server.</p>

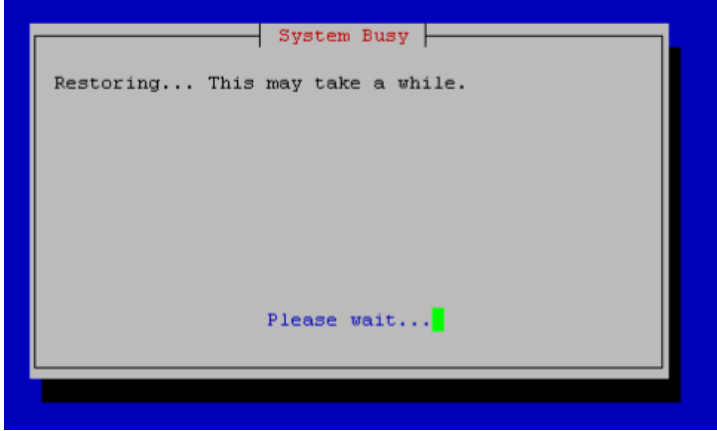

Procedure 22: Restore TVOE Configuration from Backup Media

<p>4</p> <p><input type="checkbox"/></p>	<p>Transfer TVOE Backup ISO image to the TVOE host</p>	<p style="text-align: center;">Restoring TVOE backup ISO using SCP</p> <p>Using the IP of the TVOE host, transfer the backup ISO image to the TVOE.</p> <p>Linux:</p> <p>From the command line of a Linux machine use the following command to copy the backup ISO image to the TVOE host:</p> <pre style="border: 1px solid black; padding: 5px;"># scp <path_to_image> tvoexfer@<TVOE_IP>:backup/</pre> <p>Note: where <path_to_image> is the path to the backup ISO image on the local system and <TVOE_IP> is the TVOE IP address.</p> <p>Note: If the IP is an IPv4 address then <TVOE_IP> will be a normal dot-decimal notation (e.g. "10.240.6.170").</p> <p>Note: If the IP is an IPv6 link local address then <TVOE_IP> will be need to be scoped such as "[fe80::21e:bff:fe76:5e1c%control]" where <i>control</i> is the name of the interface on the machine that is initiating the transfer and it must be on the same link as the interface on the TVOE host.</p> <p>Note: The control IP address of the TVOE can be used if the TVOE is NOT hosting the PMAC. This method requires first transferring the backup file to the PMAC, and then to the TVOE host.</p> <p>IPv4 Example:</p> <pre style="border: 1px solid black; padding: 5px;"># scp /path/to/image.iso tvoexfer@10.240.6.170:backup/</pre> <p>IPv6 Example:</p> <pre style="border: 1px solid black; padding: 5px;"># scp /path/to/image.iso tvoexfer@[fe80::21e:bff:fe76:5e1c%control]:backup/</pre> <p>Windows:</p> <p>Use WinSCP to copy the Backup ISO image into the <i>/var/TKLC/bkp</i> directory. Please refer to [10] procedure <i>Using WinSCP</i> to copy the backup image to the customer system.</p>
<p>5</p> <p><input type="checkbox"/></p>	<p>TVOE Server: Login</p>	<p>Establish an SSH session to the TVOE server, login as <i>admusr</i>.</p>

Procedure 22: Restore TVOE Configuration from Backup Media

<p>6</p> <p><input type="checkbox"/></p>	<p>Restore TVOE Backup ISO image</p>	<p>Restore the TVOE backup ISO by executing the following:</p> <pre>\$ sudo su - platcfg</pre> <p>Navigate to Maintenance -> Backup and Restore -> Restore Platform -> Select Backup Media</p>  <pre>lqqq Restore Backup Menu tqqq x x Select Backup Media x x View Table of Contents a x x Change Restore Dir a x x Restore Backup Archive a x x Exit x x x</pre> <p>Select the desired archive:</p>  <pre>lqqqqq lqqqqqqq x OK x x Cancel x mqqqqq mqqqqqqq</pre> <p>Select OK</p> <p>Select Restore Backup Archive</p>  <pre>lqqq Restore Backup Menu tqqq x x Select Backup Media x x View Table of Contents a x x Change Restore Dir x x Restore Backup Archive a x x Exit x x x</pre> <p>Confirm restore:</p>  <pre>lqqqqqqqqqqqqqqqqqqqqqqqqqqqq Restore Platform tqqqqqqqqqqqqqqqqqqqqqqqqqqqqq x x Restore the local archive (/mnt/backup) to the ROOT filesystem? x x x x lqqqqqqq lqqqqqqq x x Yes x x No x x x mqqqqqqq mqqqqqqq x x x x x</pre>
--	---	---

Procedure 22: Restore TVOE Configuration from Backup Media


<p>7 □</p>	<p>Monitor TVOE Backup process</p>	<p>Wait for the restore to complete.</p>  <p>Note: This will typically take less than 5 minutes</p> <p>Restore complete:</p>  <p>Exit Platcfg</p>
<p>8 □</p>	<p>PMAC: Login</p>	<p>If PMAC is NOT located on the this TVOE host, execute this step</p> <p>Establish an SSH session to the PMAC server, login as <i>admusr</i>.</p>
<p>9 □</p>	<p>PMAC: Remove Old TVOE Host Key</p>	<p>If PMAC is NOT located on the this TVOE host, execute this step</p> <p>Remove the old TVOE host key by executing the following command:</p> <pre>\$ sudo pmacadm removeHostKeys --ip=<TVOE Host Control IPv6 Address></pre>
<p>10 □</p>	<p>TVOE Server: Reboot</p>	<p>Restart the TVOE server by executing the following command:</p> <pre>\$ sudo init 6</pre>

Appendix I: Restore PMAC from Backup

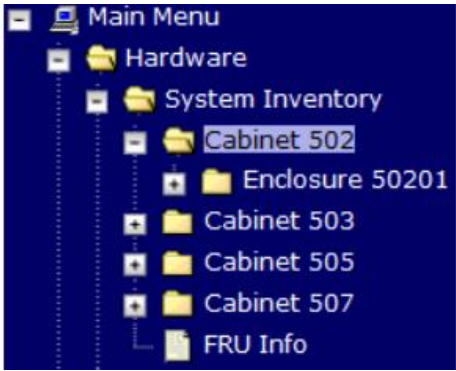
Procedure 23: Restore PMAC from Backup Media

S T E P #	<p>This procedure provides steps to restore the PMAC application configuration from backup media.</p> <p>Prerequisite: TVOE management server has been restored.</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 L: My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Deploy the PMAC Guest	Execute section “ <i>Install PM&C</i> ” from reference [10]
2 <input type="checkbox"/>	PMAC: Login	Establish an SSH session to the PMAC server, login as <i>admusr</i> .
3 <input type="checkbox"/>	Restore PMAC Backup image to the TVOE host	<p>From the remote backup location, copy the backup file to the deployed PMAC. There are too many possible backup scenarios to cover them all here.</p> <p>The example below is a simple scp from a redundant PM&C backup location. If using IPv6 addresses, command requires shell escapes, e.g. admusr@[<ipV6addr>]:/<file></p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/bin/scp -p \ admsur@<remoteserver>:/var/TKLC/smac/backup/*.pef \ /var/TKLC/smac/backup/</pre> <p>Note: It is important to copy the correct backup file to use in the restore. The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PMAC prior to the restoration of the data.</p>
4 <input type="checkbox"/>	PMAC: Verify no Alarms are present	<p>Verify no alarms are present by executing the following command:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre>

Procedure 23: Restore PMAC from Backup Media

<p>5</p> <p><input type="checkbox"/></p>	<p>Restore the PMAC Data from Backup</p>	<p>Restore the PMAC data from backup by executing the following command:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/smac/bin/pmacadm restore</pre> <p>PM&C Restore been successfully initiated as task ID 1</p> <p>To check the status of the background task, issue the following command:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</pre> <p>Note: The result will eventually display <i>PMAC Restore successful</i>.</p>
<p>6</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Login</p>	<p>Open web browser and navigate to the PMAC GUI, Login as PMACadmin user:</p> <pre style="border: 1px solid black; padding: 5px;">https://<pmac_network_ip></pre> 
<p>7</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Verify Restore Task completed</p>	<p>Navigate to Task Monitoring</p> <p>Verify the restore background task completed successfully.</p> <p>Note: After the restore is complete, you should see “Add Enclosure” tasks start for all previously provisioning servers. These should be allowed to complete before continuing.</p> <p>Note: After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior, ISO images will be added in the next step.</p>

Procedure 23: Restore PMAC from Backup Media

<p>8</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Verify System Inventory</p>	<p>Navigate to Main Menu -> System Inventory</p>  <p>Verify previously provisioned enclosures are present</p>
<p>9</p> <p><input type="checkbox"/></p>	<p>PMAC: Verify PMAC</p>	<p>Perform a system health check on the PMAC</p> <pre>\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre> <p>This command should return no output on a healthy system.</p> <pre>\$ sudo /usr/TKLC/smac/bin/sentry status</pre> <p>All Processes should be running, displaying output similar to the following:</p> <pre>PM&C Sentry Status ----- sentryd started: Mon Jul 23 17:50:49 2012 Current activity mode: ACTIVE Process PID Status StartTS NumR ----- smacTalk 9039 running Tue Jul 24 12:50:29 2012 2 smacMon 9094 running Tue Jul 24 12:50:29 2012 2 hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2 snmpEventHandler 9176 running Tue Jul 24 12:50:29 2012 2 Fri Aug 3 13:16:35 2012 Command Complete.</pre>
<p>10</p> <p><input type="checkbox"/></p>	<p>PMAC: Add ISO images to the PMAC</p>	<p>Re-add any needed ISO images to the PMAC by executing procedure <i>“Load Application and TPD ISO onto PMAC Server”</i> from reference [8]</p>

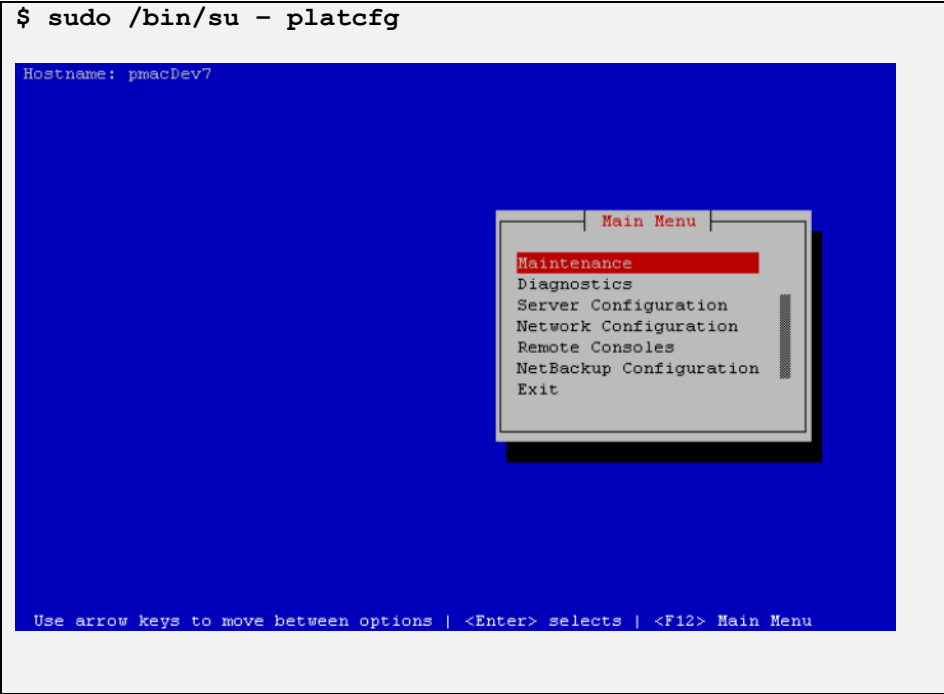
Procedure 24: Restore PMAC from Backup Server

<p>S T E P #</p>	<p>This procedure provides steps to restore the PMAC application configuration from backup server.</p> <p>Prerequisite: TVOE management server has been restored.</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 L: My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>Deploy the PMAC Guest</p>	<p>Execute section “<i>Install PM&C</i>” from reference [10]</p> <p>Note: This procedure is for restoring from a NetBackup server, so specify the appropriate options when deploying PM&C for use with NetBackup.</p>
<p>2</p> <p><input type="checkbox"/></p>	<p>PMAC TVOE Host: Login</p>	<p>Establish an SSH session to the PMAC TVOE Host, login as admusr.</p>
<p>3</p> <p><input type="checkbox"/></p>	<p>PMAC TVOE Host: Login to PMAC Guest Console</p>	<p>On the TVOE host, execute the following command:</p> <pre style="border: 1px solid black; padding: 2px; width: fit-content;">\$sudo virsh list</pre> <p>This will produce a listing of currently running virtual machines.</p> <pre style="background-color: black; color: white; padding: 5px;">[admusr@Oahu-TVOE-1 ~]\$ sudo virsh list Id Name State ----- 1 Oahu-PMAC running</pre> <p>Find the VM name for your PMAC and note its ID number in the first column.</p>
<p>4</p> <p><input type="checkbox"/></p>	<p>Connect to console of the VM using the VM number obtained in Step 3.</p>	<p>On the TVOE host, execute:</p> <pre style="border: 1px solid black; padding: 2px; width: fit-content;">\$sudo virsh console <PMAC-VMID></pre> <p>Where PMAC-VMID is the VM ID you obtained in Step 3:</p> <pre style="background-color: black; color: white; padding: 5px;">[admusr@Oahu-TVOE-1 ~]\$ sudo virsh console 1 Connected to domain Oahu-PMAC Escape character is ^] Oracle Linux Server release 6.7 Kernel 2.6.32-573.3.1.el6prere17.0.3.0.0_86.37.0.x86_64 on an x86_64 Oahu-PMAC login: █</pre> <p>You are now connected to the PMAC guest console.</p> <p>If you wish to return to the TVOE host, you can exit the session by pressing CTRL +]</p>

Procedure 24: Restore PMAC from Backup Server

<p>5</p> <p><input type="checkbox"/></p>	<p>PMAC: Prepare PMAC guest to transfer the appropriate backup from Backup Server. Disable iptables, and enable the TPD platcfg backup configuration menus.</p>	<p>Run the following commands on the PMAC:</p> <pre>\$ sudo /sbin/service iptables stop iptables: Flushing firewall rules: [OK] iptables: Setting chains to policy ACCEPT: filter [OK] \$ sudo /usr/TKLC/smac/etc/services/netbackup start Modified menu NBConfig -- show Set the following menus: NBConfig to visible=1 Modified menu NBInit -- show Set the following menus: NBInit to visible=1 Modified menu NBDeInit -- show Set the following menus: NBDeInit to visible=1 Modified menu NBInstall -- show Set the following menus: NBInstall to visible=1 Modified menu NBVerifyEnv -- show Set the following menus: NBVerifyEnv to visible=1 Modified menu NBVerify -- show Set the following menus: NBVerify to visible=1</pre>
--	--	---


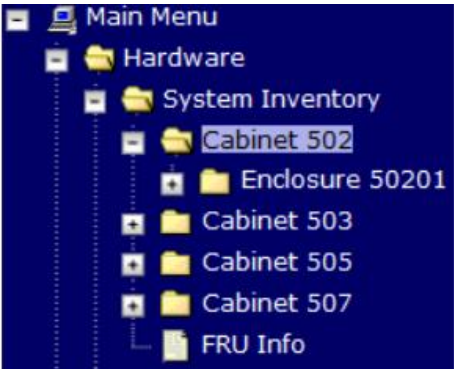
Procedure 24: Restore PMAC from Backup Server

<p>6 □</p>	<p>PMAC: Verify the TPD platcfg backup menus are visible, then exit the TPD platcfg Utility</p>	<p>Issue the following command to verify the TPD platcfg backup menus are visible:</p> <pre>\$ sudo /bin/su - platcfg</pre>  <p>Note: In the example image above of the TPD platcfg utility Main Menu the backup menu is identified as “NetBackup Configuration”.</p>
<p>7 □</p>	<p>PMAC: Verify the iptables rules are disabled on the PMAC guest</p>	<p>Verify the iptables rules are disabled on the PMAC guest by executing the following command:</p> <pre>\$ sudo /sbin/iptables -nL</pre> <pre>INPUT (policy ACCEPT) target prot opt source destination Chain FORWARD (policy ACCEPT) target prot opt source destination Chain OUTPUT (policy ACCEPT) target prot opt source destination</pre>
<p>8 □</p>	<p>PMAC: Install backup utility client software on the PMAC Guest</p>	<p>Execute section “<i>PM&C NetBackup Client Installation and Configuration</i>” from [10] - Start at step 4.</p> <p>Note: The “<i>Initialize PM&C Application</i>” and “<i>Configure PM&C application</i>” prerequisites can be ignored.</p>

Procedure 24: Restore PMAC from Backup Server

<p>9 <input type="checkbox"/></p>	<p>Backup Server: Verify appropriate PMAC backup exists.</p>	<p>This step will likely be executed by customer IT personnel.</p> <p>Log in to the Backup Server as the appropriate user, using the user password.</p> <p>Execute the appropriate commands to verify the PMAC backup exists for the desired date.</p> <p>Note: The actions and commands required to verify that the PM&C backups exist and the commands required to perform backup and restore on the Backup Server are the responsibility of the site customer.</p> <p>Note: It is important to choose the correct backup file to use in the restore. The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PM&C prior to the restoration of the data.</p>
<p>10 <input type="checkbox"/></p>	<p>Backup Server: Verify appropriate PMAC backup exists.</p>	<p>This step will likely be executed by customer IT personnel.</p> <p>Log in to the Backup Server as the appropriate user, using the user password.</p> <p>Execute the appropriate commands to verify the PMAC backup exists for the desired date.</p> <p>Execute the appropriate commands to restore the PM&C Management Server backup for the desired date.</p> <p>Note: The actions, and commands, required to verify the PM&C backups exist, and the commands required to perform backup and restore on the Backup Server are the responsibility of the site customer.</p>
<p>11 <input type="checkbox"/></p>	<p>PMAC: Verify no Alarms are present</p>	<p>Verify no alarms are present by executing the following command:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre>
<p>12 <input type="checkbox"/></p>	<p>Restore the PMAC Data from Backup</p>	<p>Restore the PMAC data from backup by executing the following command:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/smac/bin/pmacadm restore</pre> <pre style="border: 1px solid black; padding: 5px;">PM&C Restore been successfully initiated as task ID 1</pre> <p>To check the status of the background task, issue the following command:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</pre> <p>Note: The result will eventually display <i>PMAC Restore successful</i>.</p>

Procedure 24: Restore PMAC from Backup Server

<p>13</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Login</p>	<p>Open web browser and navigate to the PMAC GUI, Login as PMACadmin user:</p> <p><code>https://<pmac_network_ip></code></p> 
<p>14</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Verify Restore Task completed</p>	<p>Navigate to Task Monitoring</p> <p>Verify the restore background task completed successfully.</p> <p>Note: After the restore is complete, you should see “Add Enclosure” tasks start for all previously provisioning servers. These should be allowed to complete before continuing.</p> <p>Note: After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior, ISO images will be added in the next step.</p>
<p>15</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Verify System Inventory</p>	<p>Navigate to Main Menu -> System Inventory</p>  <p>Verify previously provisioned enclosures are present</p>

Procedure 24: Restore PMAC from Backup Server

<p>16</p> <p><input type="checkbox"/></p>	<p>PMAC: Verify PMAC</p>	<p>Perform a system health check on the PMAC</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre> <p>This command should return no output on a healthy system.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo /usr/TKLC/smac/bin/sentry status</pre> <p>All Processes should be running, displaying output similar to the following:</p> <pre>PM&C Sentry Status ----- sentryd started: Mon Jul 23 17:50:49 2012 Current activity mode: ACTIVE Process PID Status StartTS NumR ----- smacTalk 9039 running Tue Jul 24 12:50:29 2012 2 smacMon 9094 running Tue Jul 24 12:50:29 2012 2 hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2 snmpEventHandler 9176 running Tue Jul 24 12:50:29 2012 2 Fri Aug 3 13:16:35 2012 Command Complete.</pre>
<p>17</p> <p><input type="checkbox"/></p>	<p>PMAC: Add ISO images to the PMAC</p>	<p>Re-add any needed ISO images to the PMAC by executing procedure <i>“Load Application and TPD ISO onto PMAC Server”</i> from reference [8]</p>

Appendix J: Configure TVOE Hosts

Procedure 25: Configure TVOE

S	This procedure will configure networking on TVOE Hosts
T	
E	Prerequisite: Server has been IPM'ed with TVOE OS as described in [10]
P	
#	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 L: My Oracle Support (MOS) and ask for assistance.

Procedure 25: Configure TVOE

<p>1 □</p>	<p>Determine Bridge names and interfaces for XMI and IMI, and NetBackup (if used) networks.</p>	<p>Determine the bridge names and physical bridge interfaces to be used on the TVOE server for the NOAM XMI and IMI networks. Based on the site survey, you will need to determine if you are using VLAN tagging or not, what bonds will be used, and also the actual Ethernet interfaces that will make up those bonds.</p> <p>If the NetBackup bridge and interface were not previously configured on this server when PMAC was installed, determine those values as well.</p> <p>Fill in the appropriate values in the table below:</p>															
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e0e0e0;"> <th style="width: 20%; text-align: center;">NOAM Guest Interface Name</th> <th style="width: 15%; text-align: center;">TVOE Bridge Name</th> <th style="text-align: center;">TVOE Bridge Interface</th> </tr> </thead> <tbody> <tr> <td style="text-align: center; vertical-align: middle;">xmi</td> <td style="text-align: center; vertical-align: middle;">xmi</td> <td> <p>Interface Bond (e.g- bond0, bond1, etc)</p> <p style="text-align: center;">_____</p> <p><TVOE_XMI_Bridge_Interface_Bond></p> <p>Interface Name (e.g. - bond0.3, bond1, bond0.100):</p> <p style="text-align: center;">_____</p> <p><TVOE_XMI_Bridge_Interface></p> </td> </tr> <tr> <td style="text-align: center; vertical-align: middle;">imi</td> <td style="text-align: center; vertical-align: middle;">imi</td> <td> <p>Interface Bond:(e.g. - bond0, bond1, etc)</p> <p style="text-align: center;">_____</p> <p><TVOE_IMI_Bridge_Interface_Bond></p> <p>Interface Name: (e.g. - bond0.4, bond1, bond0.100)</p> <p style="text-align: center;">_____</p> <p><TVOE_IMI_Bridge_Interface</p> </td> </tr> <tr> <td style="text-align: center; vertical-align: middle;">NetBackup</td> <td style="text-align: center; vertical-align: middle;">NetBackup</td> <td> <p>Interface Name (e.g. - eth11, eth04, eth03, etc)</p> <p style="text-align: center;">_____</p> <p><TVOE_NetBackup_Bridge_Interface></p> </td> </tr> <tr> <td style="text-align: center; vertical-align: middle;">management</td> <td style="text-align: center; vertical-align: middle;">management</td> <td> <p>Interface Name (e.g. bond0.2, bond0.37, etc)</p> <p style="text-align: center;">_____</p> <p><TVOE_Mgmt_Bridge_Interface></p> </td> </tr> </tbody> </table>			NOAM Guest Interface Name	TVOE Bridge Name	TVOE Bridge Interface	xmi	xmi	<p>Interface Bond (e.g- bond0, bond1, etc)</p> <p style="text-align: center;">_____</p> <p><TVOE_XMI_Bridge_Interface_Bond></p> <p>Interface Name (e.g. - bond0.3, bond1, bond0.100):</p> <p style="text-align: center;">_____</p> <p><TVOE_XMI_Bridge_Interface></p>	imi	imi	<p>Interface Bond:(e.g. - bond0, bond1, etc)</p> <p style="text-align: center;">_____</p> <p><TVOE_IMI_Bridge_Interface_Bond></p> <p>Interface Name: (e.g. - bond0.4, bond1, bond0.100)</p> <p style="text-align: center;">_____</p> <p><TVOE_IMI_Bridge_Interface</p>	NetBackup	NetBackup	<p>Interface Name (e.g. - eth11, eth04, eth03, etc)</p> <p style="text-align: center;">_____</p> <p><TVOE_NetBackup_Bridge_Interface></p>	management	management	<p>Interface Name (e.g. bond0.2, bond0.37, etc)</p> <p style="text-align: center;">_____</p> <p><TVOE_Mgmt_Bridge_Interface></p>
NOAM Guest Interface Name	TVOE Bridge Name	TVOE Bridge Interface															
xmi	xmi	<p>Interface Bond (e.g- bond0, bond1, etc)</p> <p style="text-align: center;">_____</p> <p><TVOE_XMI_Bridge_Interface_Bond></p> <p>Interface Name (e.g. - bond0.3, bond1, bond0.100):</p> <p style="text-align: center;">_____</p> <p><TVOE_XMI_Bridge_Interface></p>															
imi	imi	<p>Interface Bond:(e.g. - bond0, bond1, etc)</p> <p style="text-align: center;">_____</p> <p><TVOE_IMI_Bridge_Interface_Bond></p> <p>Interface Name: (e.g. - bond0.4, bond1, bond0.100)</p> <p style="text-align: center;">_____</p> <p><TVOE_IMI_Bridge_Interface</p>															
NetBackup	NetBackup	<p>Interface Name (e.g. - eth11, eth04, eth03, etc)</p> <p style="text-align: center;">_____</p> <p><TVOE_NetBackup_Bridge_Interface></p>															
management	management	<p>Interface Name (e.g. bond0.2, bond0.37, etc)</p> <p style="text-align: center;">_____</p> <p><TVOE_Mgmt_Bridge_Interface></p>															

Procedure 25: Configure TVOE

2 □	RMS Server: Login	Log in to the TVOE prompt of the RMS Server as <i>admusr</i> using the iLO facility.
--------	-----------------------------	--

Procedure 25: Configure TVOE

4 <input type="checkbox"/>	RMS Server: Configure XMI Bridge Interface Bond	<p>Verify the xmi bridge interface bond by running the following command:</p> <p>Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm query --device=<TVOE_XMI_Bridge_Interface_Bond> Protocol: none On Boot: yes Persistent: yes Bonded Mode: active-backup Enslaving: eth01 eth02</pre> <p>If the bond has already been configured you will see output similar to what you see above. If this is so, skip to the next step. Otherwise, continue with this step.</p> <p>Create bonding interface and associate subordinate interfaces with bond:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_XMI_Bridge_Interface_Bond> --onboot=yes --type=Bonding --mode=active-backup --miimon=100 Interface <TVOE_XMI_Bridge_Bond> added \$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_XMI_Bridge_Bond_Ethernet1> --type=Ethernet --master=<TVOE_XMI_Bridge_Interface_Bond> --slave=yes --onboot=yes Interface <TVOE_XMI_Bridge_Bond_Ethernet1> updated \$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_XMI_Bridge_Bond_Ethernet2> --type=Ethernet --master=<TVOE_XMI_Bridge_Interface_Bond> --slave=yes --onboot=yes Interface <TVOE_XMI_Bridge_Bond_Ethernet2> updated \$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES -- val=<TVOE_XMI_Bridge_Interface_Bond>, [bondX,bondX+1, ...,bondN]</pre> <p>Note: All other existing bonds should be included in the 'val=' statement. E.g. if TVOE_XMI_Bridge_Bond = bond1, val=bond0,bond1</p> <pre>\$ sudo syscheckAdm net ipbond -enable</pre>
-------------------------------	--	---

Procedure 25: Configure TVOE

4 <input type="checkbox"/>	RMS Server: Create XMI Bridge Interface, If needed. (Only for VLAN tagging interfaces)	If you are using VLAN tagging for the XMI bridge interface, then you must create the VLAN interface first. Execute the following command: <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_XMI_Bridge_Interface> --onboot=yes</pre> Interface <TVOE_XMI_Bridge_Interface> created.
5 <input type="checkbox"/>	RMS Server: Create XMI Bridge	Now , create the XMI bridge: <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=xmi --onboot=yes --bridgeInterfaces=<TVOE_XMI_Bridge_Interface></pre> Interface <TOE_XMI_Bridge_Interface> updated. Bridge xmi created.

Procedure 25: Configure TVOE

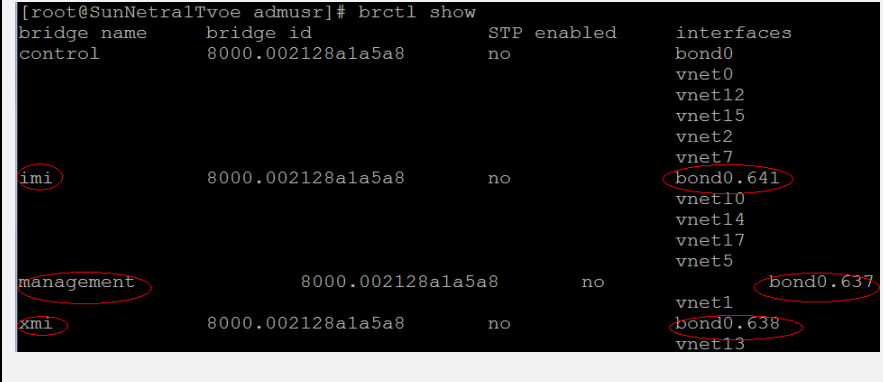
<p>6 <input type="checkbox"/></p>	<p>RMS Server: Configure IMI Bridge Interface Bond</p>	<p>Verify the imi bridge interface bond by running the following command:</p> <p>Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm query --device=<TVOE_IMI_Bridge_Interface_Bond> Protocol: none On Boot: yes Persistent: yes Bonded Mode: active-backup Enslaving: eth01 eth02</pre> <p>If the bond has already been configured you will see output similar to what you see above. If this is so, skip to the next step. Otherwise, continue with this step.</p> <p>Create bonding interface and associate subordinate interfaces with bond:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_IMI_Bridge_Interface_Bond> --onboot=yes --type=Bonding --mode=active-backup --miimon=100 Interface <TVOE_IMI_Bridge_Bond> added \$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_IMI_Bridge_Bond_Ethernet1> --type=Ethernet --master=<TVOE_IMI_Bridge_Bond> --slave=yes --onboot=yes Interface <TVOE_IMI_Bridge_Bond_Ethernet1> updated \$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_IMI_Bridge_Bond_Ethernet2> --type=Ethernet --master=<TVOE_IMI_Bridge_Bond> --slave=yes --onboot=yes Interface <TVOE_IMI_Bridge_Bond_Ethernet2> updated</pre> <p>Execute the following 2 commands ONLY IF <TVOE_XMI_Bridge_Bond> is different from <TVOE_IMI_Bridge_Bond></p> <pre>\$ sudo syscheckAdm net ipbond --set --var=DEVICES --val=<TVOE_XMI_Bridge_Interface_Bond>, <TVOE_IMI_Bridge_Interface_Bond>,[other bonds...]</pre> <pre>\$ sudo syscheckAdm net ipbond -enable</pre>
---------------------------------------	---	---

Procedure 25: Configure TVOE

7 <input type="checkbox"/>	RMS Server: Create IMI Bridge Interface	If you are using VLAN tagging for the IMI bridge interface, then you must create the VLAN interface first. Execute the following command: <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_IMI_Bridge_Interface> --onboot=yes</pre> Interface <TVOE_IMI_Bridge_Interface> created.
8 <input type="checkbox"/>	RMS Server: Create IMI Bridge	Create the IMI bridge: <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge -- name=imi --onboot=yes --bridgeInterfaces=<TVOE_IMI_Bridge_Interface></pre> Interface <TVOE_IMI_Bridge_Interface> updated. Bridge imi created.

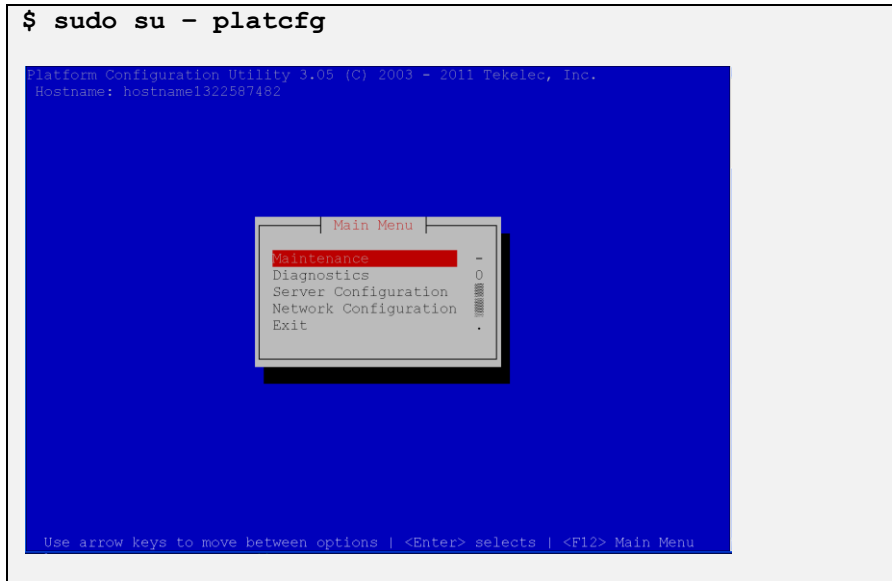
<p>9 □</p>	<p>RMS server iLO: Create management bridge and assign TVOE Management IP</p>	<p>Execute this Step only if the TVOE Host is a rack mount server and is NOT the PMAC server.</p> <p>Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (<i>network devices, bonds, and bond enslaved devices</i>), to configure.</p> <p>If <TVOE_Management_Bridge_Interface> or the bond it is based on (if using tagged interface) has not yet been created, then execute the next 3 commands. Otherwise, skip to the “EXAMPLE...” section:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Mgmt_Bridge_Interface_Bond> --onboot=yes --type=Bonding --mode=active-backup --miimon=100 Interface <TVOE_Management_Bridge_Interface> added</pre> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_Mgmt_Bridge_Bond_Interface1> --type=Ethernet --master=<TVOE_Mgmt_Bridge_Interface_Bond> --slave=yes --onboot=yes Interface <mgmt_ethernet_interface1> updated</pre> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_Mgmt_Bridge_Bond_Interface2> --type=Ethernet --master=<TVOE_Mgmt_Bridge_Interface_Bond> --slave=yes --onboot=yes Interface <mgmt_ethernet_interface2> updated</pre> <p>EXAMPLE 1: Create Management bridge using untagged interfaces</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=management --bootproto=none --onboot=yes --address=<TVOE_Mgmt_IP_Address> --netmask=<TVOE_Mgmt_Netmask/Prefix> --bridgeInterfaces=<TVOE_Mgmt_Bridge_Interface></pre> <p>EXAMPLE 2: Create Management bridge using tagged interfaces</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Management_Bridge_Interface> \$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=management --address=<TVOE_Mgmt_IP_Address> --netmask=<TVOE_Mgmt_Netmask/Prefix> --onboot=yes --bridgeInterfaces=<TVOE_Mgmt_Bridge_Interface></pre>
----------------	--	---

Procedure 25: Configure TVOE

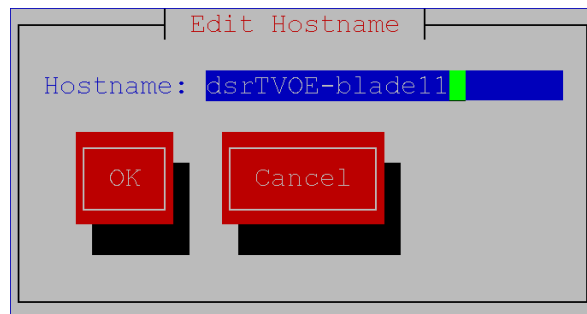
<p>10 <input type="checkbox"/></p>	<p>RMS server iLO: Add Default route</p>	<p>Add a default route using the xmi or management address (if configured)</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=default --gateway=<TVOE_Mgmt_gateway_IP_address> --device=<management or xmi> Route to management created.</pre>
<p>11 <input type="checkbox"/></p>	<p>RMS Server: Verify bridge creation status</p>	<p>Verify that the XMI and IMI bridges have been created successfully (Example output for illustrative purposes only):</p> <pre>\$ brctl show</pre>  <pre>[root@SunNetralTvoe admusr]# brctl show bridge name bridge id STP enabled interfaces control 8000.002128a1a5a8 no bond0 vnet0 vnet12 vnet15 vnet2 vnet7 imi 8000.002128a1a5a8 no bond0.641 vnet10 vnet14 vnet17 vnet5 management 8000.002128a1a5a8 no bond0.637 vnet1 xmi 8000.002128a1a5a8 no bond0.638 vnet13</pre> <ul style="list-style-type: none"> • Verify that "imi" and "xmi" are listed under the bridge name column. • Verify that <TVOE_XMI_Bridge_Interface> is listed under the interfaces column for xmi. • Verify that <TVOE_IMI_Bridge_Interface> is listed under the interfaces column for imi. • Verify that the <TVOE_Mgmt_Bridge_Interface> is listed under the interface column for <TVOE_Mgmt_Bridge_Interface>
<p>12 <input type="checkbox"/></p>	<p>RMS Server iLO: Create NetBackup bridge (Optional)</p>	<p>Perform the following command if you will have a dedicated NetBackup interface within your NOAM guests (and if the NetBackup bridge was NOT configured when setting up the PMAC earlier)</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=NetBackup --onboot=yes --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface></pre>

Procedure 25: Configure TVOE

13 RMS Server iLO: Set Hostname



Navigate to **Server Configuration->Hostname-> Edit** and enter a new hostname for your server:



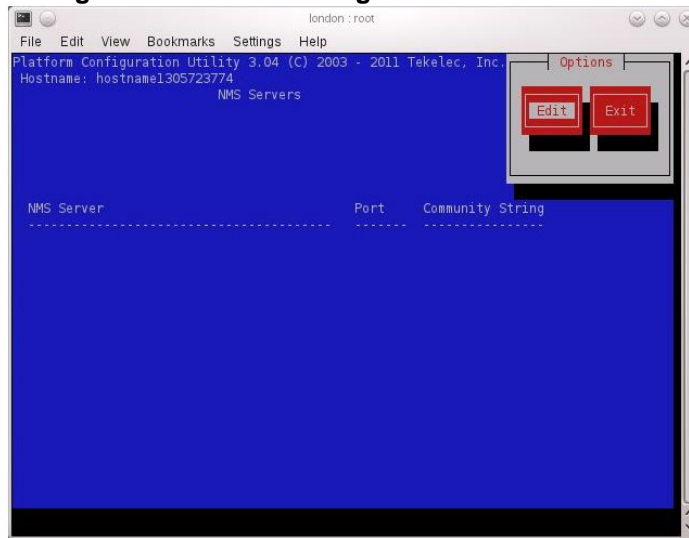
Press **OK** and select and continue to press Exit until you are at the placfg main menu again.

Note: Although the new hostname has been properly configured and committed at this point, it will not appear on your command prompt unless you log out and log back in again.

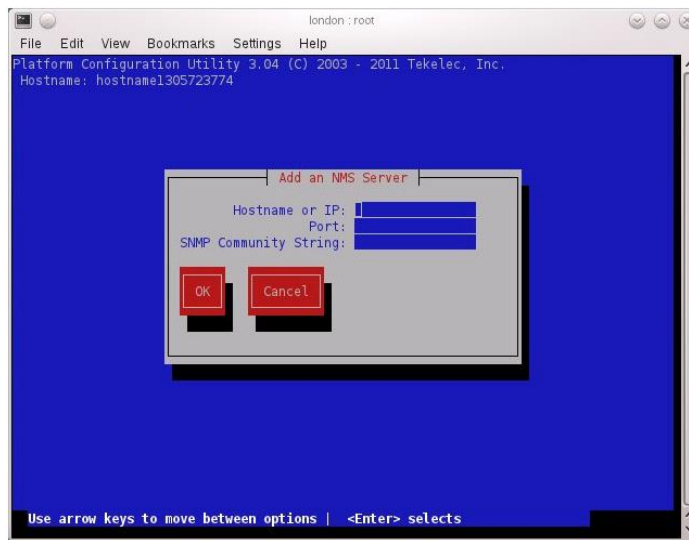
Procedure 25: Configure TVOE

14 RMS Server iLO: Configure SNMP

From the platcfg main menu, navigate to **Network Configuration -> SNMP Configuration -> NMS Configuration**



Press **Edit**.
Choose **Add a New NMS Server**



Enter the following NMS servers, pressing **OK** after each one and then selecting the **Add NMS** option again:

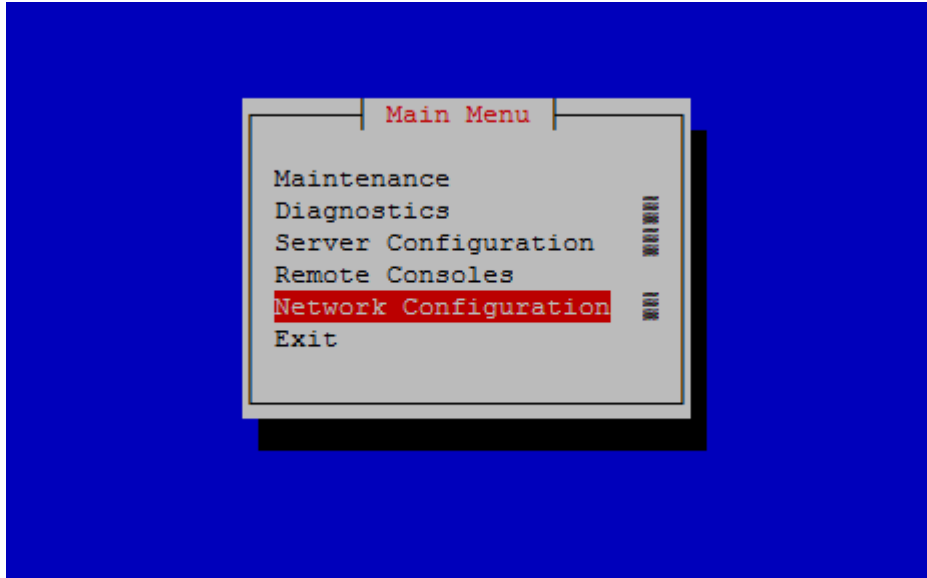
1. Enter the Hostname/IP of the Customer NMS Server, for port enter 162, and for Community String enter the community string provided in the customer NAPD Document.
2. Enter the IP of the NOAM VIP, for port enter 162, and for Community String enter the community string provided in the customer NAPD Document

Press **Exit**.
Select **Yes** when prompted to restart the Alarm Routing Service.
Once Done, press **Exit** to quit to the platcfg main menu.

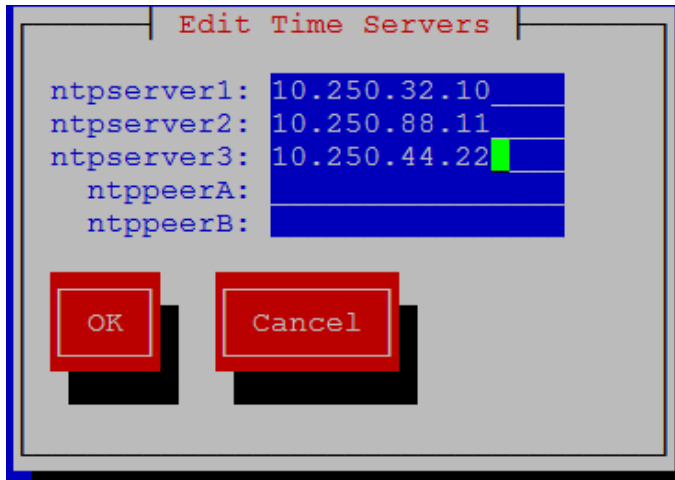
Procedure 25: Configure TVOE

15 **RMS Server iLO:**
□ Configure NTP

Navigate to **Network Configuration**



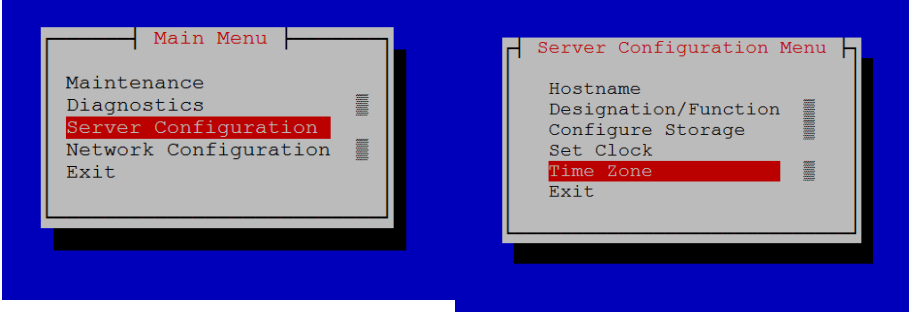
Navigate to **NTP**
Click **Edit**



- ntpserver1: Enter customer provided NTP server #1 IP address.
- ntpserver2: Enter customer provided NTP server #2 IP address.
- ntpserver3: Enter customer provided NTP server #3 IP address.


Press **OK**
Press **Exit** to return to the platcfg menu.

Procedure 25: Configure TVOE

<p>16</p> <p>☐</p>	<p>RMS Server iLO: Configure Time Zone</p>	<pre>\$ sudo su - platcfg</pre> <p>Navigate to Server Configuration->Time Zone</p>   <p>If the time zone displayed matches the time zone you desire, then you can continue to hit Exit until you are out of the platcfg program. If you want a different time zone, then proceed with this instruction.</p> <p>Click Edit</p>  <p>Select the desired time zone from the list and press Enter Continue pressing Exit until you are out of the platcfg program.</p>
<p>17</p> <p>☐</p>	<p>RMS Server iLO: Reboot Server</p>	<p>Reboot the server by executing the following command:</p> <pre>\$ sudo su - platcfg</pre>

Appendix K: Create NOAM/SOAM Virtual Machines

Procedure 26: Create NOAM Guest VMs

<p>S T E P #</p>	<p>This procedure will provide the steps needed to create a DSR NOAM virtual machine (referred to as a “guest”) on a TVOE server blade or TVOE RMS. It must be repeated for every NOAM server you wish to install.</p> <p>Prerequisite: TVOE has been installed and configured on the target blade server or RMS</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 L: My Oracle Support (MOS) and ask for assistance.</p>
<p>1 <input type="checkbox"/></p>	<p>PMAC GUI:</p> <p>Login</p> <p>Open web browser and enter:</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p><a href="http://<PMAC Mgmt Network IP>">http://<PMAC Mgmt Network IP></p> </div> <p>Login as <i>pmacadmin</i> user:</p> 

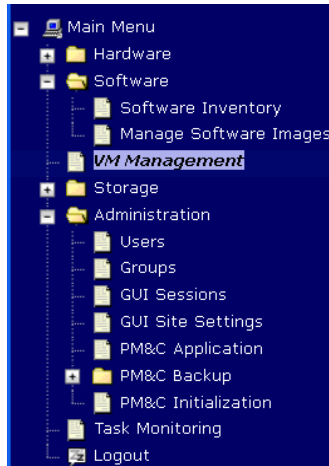
Procedure 26: Create NOAM Guest VMs

2

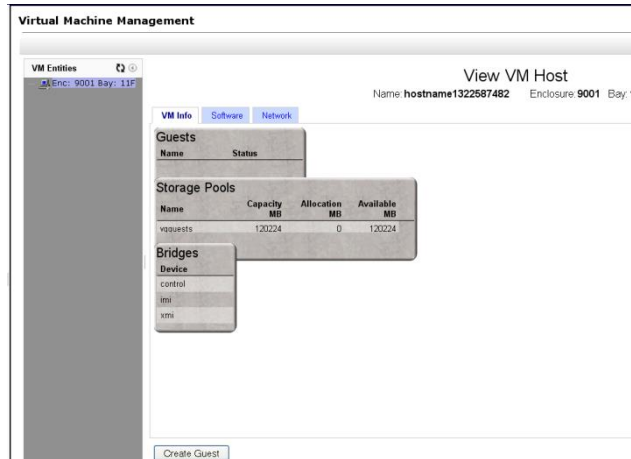


PMAC GUI:
Navigate to
VM
Management
of the Target
Server Blade

Navigate to **Main Menu -> VM Management**



Select the TVOE server blade or rack mounted server from the **VM Entities** listing on the left side of the screen. The selected server's guest machine configuration will then be displayed in the remaining area of the window.



Click **Create Guest**



Procedure 26: Create NOAM Guest VMs

3



PMAC GUI:
Configure
VM Guest
Parameters

Select **Import Profile**

Import Profile

ISO/Profile: DSR-7.2.0.0.0_72.8.0-x86_64 => DSR_NOAMP_LARGE

Num CPUs: 12

Memory (MBs): 24576

Virtual Disks:	Pri m	Size (MB)	Pool	TPD Dev
	✓	102400	vguests	

NICs:	Bridge	TPD Dev
	control	control
	imi	imi
	xmi	xmi

Select Profile

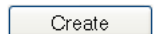
From the **“ISO/Profile”** drop-down box, select the entry that matches depending on the hardware that your NOAM VM TVOE server is running on and your preference for NetBackup interfaces:

NOAM VM TVOE Hardware Type(s)	Dedicated Netbackup Interface?	Choose Profile (<Application ISO NAME>→)
HP DL380 Gen 8 RMS, HP BL460 Gen 9 RMS, HP BL460 Gen 8 Blade, HP BL460 Gen 9 Blade	No	DSR_NOAMP_LARGE
HP DL380 Gen 8 RMS, HP BL460 Gen 9 RMS, HP BL460 Gen 8 Blade, HP BL460 Gen 9 Blade	Yes	DSR_NOAMP_LARGE_NBD

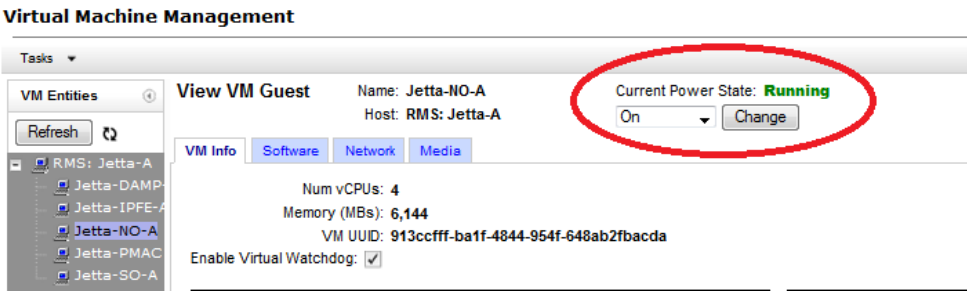
Note: Application_ISO_NAME is the name of the DSR Application ISO to be installed on this NOAM

Press **Select Profile**.


Press **Create**



Procedure 26: Create NOAM Guest VMs

<p>4 □</p>	<p>PMAC GUI: Wait for Guest Creation to Complete</p>	<p>Navigate to Main Menu -> Task Monitoring to monitor the progress of the guest creation task. A separate task will appear for each guest creation that you have launched.</p> <p>Wait or refresh the screen until you see that the guest creation task has completed successfully.</p> <table border="1" data-bbox="451 525 1339 609"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>Running Time</th> <th>Start Time</th> <th>Progress</th> </tr> </thead> <tbody> <tr> <td>1739</td> <td>VirtAction: Create</td> <td>Enc:9001 Bay:11F Guest: DSR_NOAMP</td> <td>Guest creation completed (DSR_NOAMP)</td> <td>0:00:04</td> <td>2011-11-29 20:36:11</td> <td>100%</td> </tr> </tbody> </table>	ID	Task	Target	Status	Running Time	Start Time	Progress	1739	VirtAction: Create	Enc:9001 Bay:11F Guest: DSR_NOAMP	Guest creation completed (DSR_NOAMP)	0:00:04	2011-11-29 20:36:11	100%
ID	Task	Target	Status	Running Time	Start Time	Progress										
1739	VirtAction: Create	Enc:9001 Bay:11F Guest: DSR_NOAMP	Guest creation completed (DSR_NOAMP)	0:00:04	2011-11-29 20:36:11	100%										
<p>5 □</p>	<p>PMAC GUI: Verify Guest Machine is Running</p>	<p>Navigate to Main Menu -> VM Management</p> <p>Select the TVOE server blade on which the guest machine was just created.</p> <p>Look at the list of guests present on the blade and verify that you see a guest that matches the name you configured and that its status is “Running”.</p>  <p>VM Creation for this guest is complete. Repeat from Step 2 for any remaining NOAM VMs (<i>for instance, the standby NOAM</i>) that must be created.</p>														

Procedure 27: Create SOAM Guest VMs

<p>S T E P #</p>	<p>This procedure will provide the steps needed to create a DSR SOAM virtual machine (referred to as a "guest") on a TVOE server blade. It must be repeated for every SOAM server you wish to install.</p> <p>Prerequisite: TVOE has been installed and configured on the target blade 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 L: 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> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <p>http://<PMAC Mgmt Network IP></p> </div> <p>Login as <i>pmacadmin</i> user:</p> 

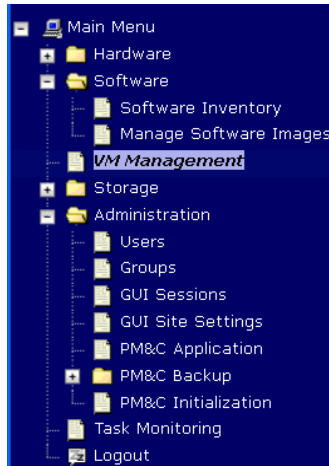
Procedure 27: Create SOAM Guest VMs

2

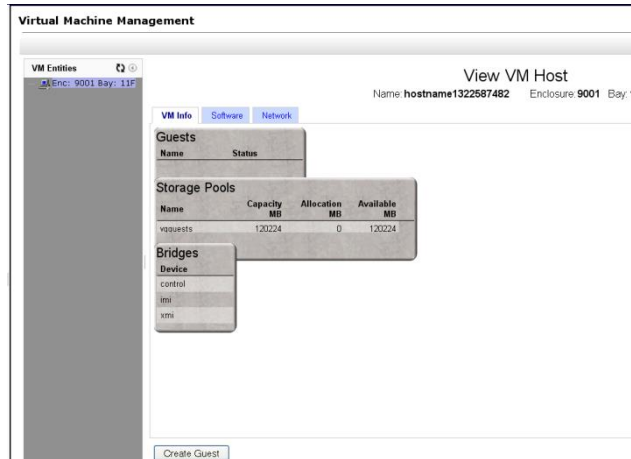


PMAC GUI:
Navigate to VM Management of the Target Server Blade

Navigate to **Main Menu -> VM Management**



Select the TVOE server blade or rack mounted server from the **VM Entities** listing on the left side of the screen. The selected server's guest machine configuration will then be displayed in the remaining area of the window.



Click **Create Guest**



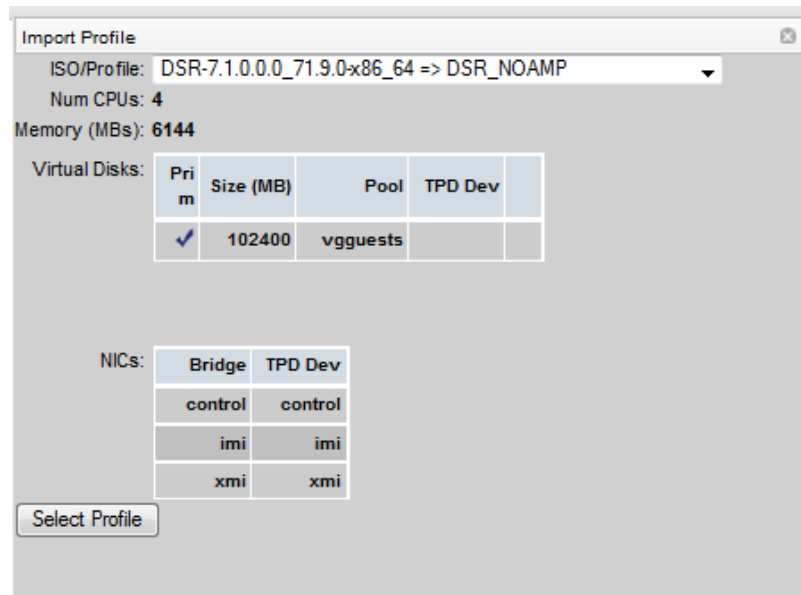
Procedure 27: Create SOAM Guest VMs

3



PMAC GUI:
Configure
VM Guest
Parameters

Select **Import Profile**



From the **“ISO/Profile”** drop-down box, select the entry that matches depending on the hardware that your SOAM VM TVOE server is running on and your preference for NetBackup interfaces:

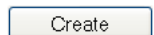
SOAM VM TVOE Hardware Type(s)	Dedicated Netbackup Interface?	Choose Profile (<Application ISO NAME>→)
HP BL460 Gen 8 Blade, HP BL460 Gen 6 Blade, HP BL460 Gen 9 Blade	No	DSR_SOAM
HP BL460 Gen 8 Blade, HP BL460 Gen 6 Blade, HP BL460 Gen 9 Blade	Yes	DSR_SOAM_NBD

Note: Application_ISO_NAME is the name of the DSR Application ISO to be installed on this SOAM

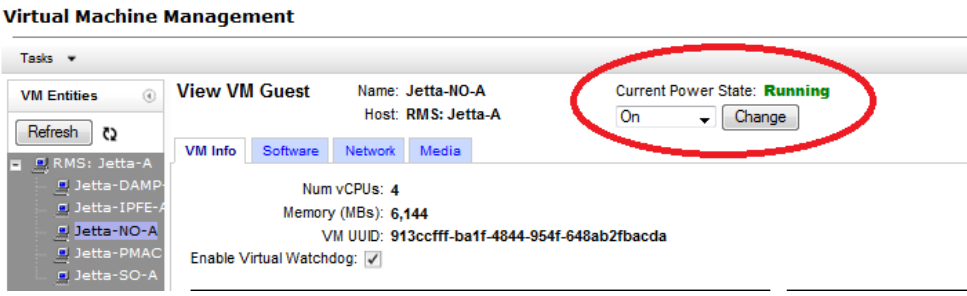
Press **Select Profile**.

You can edit the name, if you wish. For instance: **“DSR_SOAM_A,”** or **DSR_SOAM_B”**. (This will not become the ultimate hostname. It is just an internal tag for the VM host manager.)

Press **Create**



Procedure 27: Create SOAM Guest VMs

<p>4</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Wait for Guest Creation to Complete</p>	<p>Navigate to Main Menu -> Task Monitoring to monitor the progress of the guest creation task. A separate task will appear for each guest creation that you have launched.</p> <p>Wait or refresh the screen until you see that the guest creation task has completed successfully.</p> <table border="1" data-bbox="451 525 1339 609"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>Running Time</th> <th>Start Time</th> <th>Progress</th> </tr> </thead> <tbody> <tr> <td>1739</td> <td>VirtAction: Create</td> <td>Enc:9001 Bay:11F Guest: DSR_NOAMP</td> <td>Guest creation completed (DSR_NOAMP)</td> <td>0:00:04</td> <td>2011-11-29 20:36:11</td> <td>100%</td> </tr> </tbody> </table>	ID	Task	Target	Status	Running Time	Start Time	Progress	1739	VirtAction: Create	Enc:9001 Bay:11F Guest: DSR_NOAMP	Guest creation completed (DSR_NOAMP)	0:00:04	2011-11-29 20:36:11	100%
ID	Task	Target	Status	Running Time	Start Time	Progress										
1739	VirtAction: Create	Enc:9001 Bay:11F Guest: DSR_NOAMP	Guest creation completed (DSR_NOAMP)	0:00:04	2011-11-29 20:36:11	100%										
<p>5</p> <p><input type="checkbox"/></p>	<p>PMAC GUI: Verify Guest Machine is Running</p>	<p>Navigate to Main Menu -> VM Management</p> <p>Select the TVOE server blade on which the guest machine was just created.</p> <p>Look at the list of guests present on the blade and verify that you see a guest that matches the name you configured and that its status is “Running”.</p>  <p>VM Creation for this guest is complete. Repeat from Step 2 for any remaining NOAM VMs (for instance, the standby SOAM) that must be created.</p>														

Appendix L: 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.