Oracle® Communications

Diameter Signaling Router

DSR Disaster Recovery Guide

Release 7.2

E69612 Revision 01

April 2016

Oracle Communications Diameter Signaling Router DSR 3-tier Disaster Recovery Procedure, Release 7.2

⚠ **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

List of Procedures

List of Tables

List of Figures

1.0 Introduction

1.1 Purpose and Scope

This document is a guide to describe procedures used to execute disaster recovery for DSR 7.2. 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. 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 Software Installation and Configuration Procedure Part 2/2, E69409
[9] DSR GLA Feature Activation Procedure, E58659
[10] DSR 7.1/7.2 Hardware and Software Installation, E53488
[11] PM&C 5.7/6.0 Disaster Recovery Guide, E54388
[12] SDS 7.1/7.2 Disaster Recovery Guide. E59145
[13] DSR 7.2 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 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	• All NOAM servers failed • All SOAM servers failed
Recovery of one or more servers with at least one NOAM server intact	• 1 or more NOAM servers intact • 1 or more SOAM or MP servers failed
Recovery of the NOAM pair with one or more SOAM servers intact	• All NOAM servers failed • 1 or more SOAM servers intact
Recovery of one or more server with at least one NOAM and one SOAM server intact.	• 1 or more NOAM servers intact • 1 or more SOAM servers intact • 1 SOAM or 1 or more MP servers failed
Recovery of one or more server with corrupt databases that cannot be restored via replication from the active parent node.	

Note: 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 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

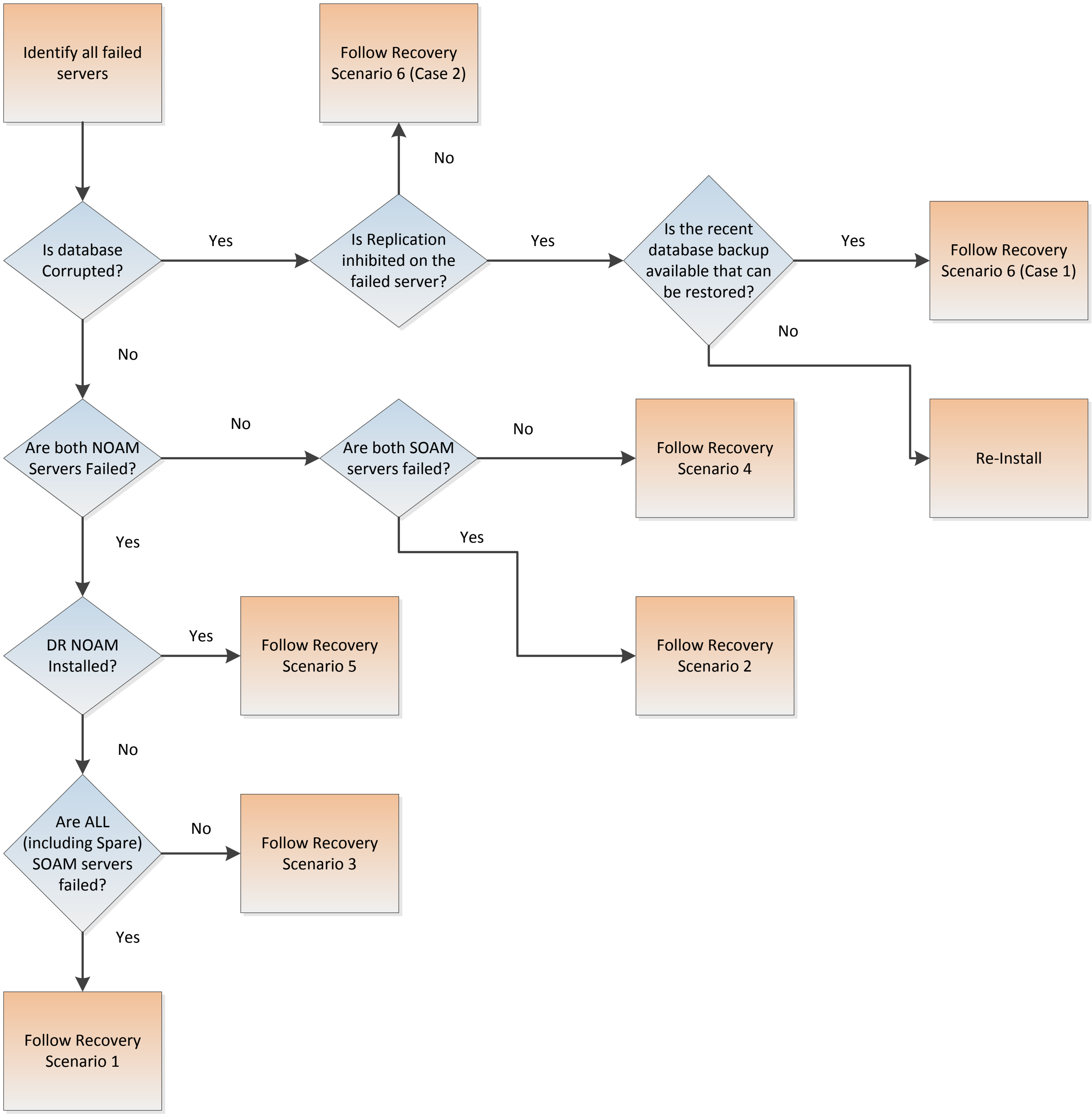
As a non-root user (***admusr***), many commands (*when run as admusr*) now require the use of ***'sudo'.***

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


Identify all failed servers
Is database Corrupted?
Yes
Is Replication inhibited on the failed server?
No
Follow Recovery Scenario 6 (Case 2)
Yes
Is the recent database backup available that can be restored?
Yes
Follow Recovery Scenario 6 (Case 1)
No
Re-Install
No
Are both NOAM Servers Failed?
No
Are both SOAM servers failed?
No
Follow Recovery Scenario 4
Yes
Follow Recovery Scenario 2
Yes
DR NOAM Installed?
Yes
Follow Recovery Scenario 5
No
Are ALL (including Spare) SOAM servers failed?
No
Follow Recovery Scenario 3
Yes
Follow Recovery Scenario 1

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	• All NOAM servers failed. • All SOAM servers failed. • MP servers may or may not be failed.	Section 5.1.1 Recovery Scenario 1 (Complete Server Outage)
2	• At least 1 NOAM server is intact and available. • All SOAM servers failed. • MP servers may or may not be failed.	Section5.1.2 Recovery Scenario 2 (Partial Server Outage with one NOAM server intact and ALL SOAMs failed)
3	• All NOAM servers failed. • At least 1 SOAM server out of Active, StandBy, Spare is intact and available. • MP servers may or may not be failed.	Section 5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact)
4	• At least 1 NOAM server is intact and available. • At least 1 SOAM server out of Active, StandBy, Spare is intact and available. • 1 or more MP servers have failed.	Section 5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)

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

5.0 Disaster Recovery Procedure

Call Appendix 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 actual detailed steps are in **Procedure 1**. 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 11** for IDIH disaster recovery and [12] for SDS 7.2 disaster recovery

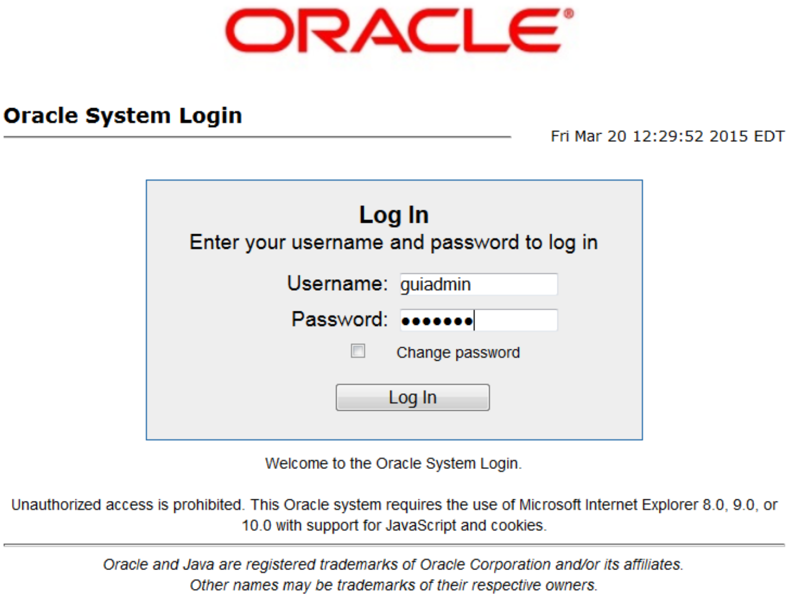
Procedure 1: Recovery Scenario 1

S T E P #	This procedure performs recovery if both NOAM servers are failed and all SOAM servers are failed. This procedure also caters the C-Level Sever failure 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 □	**Workarounds**	Refer to **Appendix G**: Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
2 □	**Gather Required Materials**	Gather the documents and required materials listed in **Section 3.1** Required Materials
3 □	**Replace Failed Equipment**	HW vendor to replace the failed equipment
4 □	**Recover PMAC and PMAC TVOE Host:** Configure BIOS Settings and Update Firmware	1. Configure and verify the BIOS settings by executing procedure *"Configure the RMS Server BIOS Settings"* from reference [10] 2. Verify and/or upgrade server firmware by executing procedure *"Upgrade Management Server Firmware"* from reference[10] **Note:** As indicated in [10], repeat for additional rack mount servers if equipped.
5 □	**PMAC, TVOE Hosts, and Switch Recovery:** Backups Available	This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, **skip this step**. 1. Restore the PMAC TVOE host backup by executing Appendix H: Restore TVOE Configuration from Backup Media Restore the PMAC backup by executing 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 *"Server Blades Installation Preparation"* from reference [10]. 5. Execute Install TVOE on ALL failed TVOE servers as needed by executing section *"Install TVOE on Blade Servers"* 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. **Proceed to Step 7**

Procedure 1: Recovery Scenario 1

6 □	**PMAC, TVOE Hosts, and Switch Recovery:** Backups **NOT** Available	This step assumes that TVOE and PMAC backups **NOT** are available, if the TVOE and PMAC have already been restored, **skip this step** 1. Execute section *“Configure and IPM Management Server”* from reference [10]. 2. Execute section *“Install PM&C”* from reference [10]. 3. Execute section “Configure Aggregation Switches” from reference [10] to recover Cisco 4948 aggregation switches if needed. 4. Execute section *“Configure PM&C”* from reference [10]. 5. Execute section *“HP C-7000 Enclosure Configuration”* from reference [10] to recover and configure any failed OAs if needed. 6. Execute section “Enclosure and Blades Setup” from reference [10]. 7. Execute section “Configure Enclosure Switches” from reference [10] to recover enclosure switches if needed. 8. Verify/Update Blade server firmware by executing section *“Server Blades Installation Preparation”* from reference [10]. 9. Install and configure TVOE on failed rack mount servers by executing section *“Installing TVOE on Rack Mount Server(s)”* from reference [10]. 10. Install and configure TVOE on failed TVOE blade servers by executing section *“Install TVOE on Blade Servers”* from reference [10]. **Proceed to Next Step**
7 □	**Execute Fast Deployment File for NOAMs**	The backup fdconfig file used during the initial DSR 7.2 installation, this file will be available on the PMAC if a database backup was restored on the PMAC. If a backup fast deployment xml is NOT available, execute procedure *“Configure NOAM Servers”* from reference [8]. If a backup fast deployment xml is already present on the PMAC, execute the following procedure: 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: **`$ cd /usr/TKLC/smac/etc`** **`$ screen`** **`$ sudo fdconfig config --file=<Created_FD_File>.xml`**

Procedure 1: Recovery Scenario 1

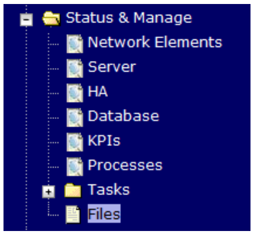
8 □	**Obtain Latest Database Backup and Network Configuration Data.**	1. Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. 2. Obtain most recent "RADIUS shared secret encryption key" file DpiKf.bin.encr from external backup sources. (Only when the RADIUS Key Revocation MOP has been executed on the system) **Note:** Shared secret encryption key file needs to be handled by someone authorized to handle shared secrets information. **Note:** From required materials list in **Section 3.1** `Required Materials`; use site survey documents and Network Element report (if available), to determine network configuration data.
9 □	**Execute DSR Installation Procedure for the First NOAM**	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]. **Note:** Use the backup copy of network configuration data and site surveys (Step 2)
10 □	**NOAM GUI:** Login	Login to the NOAM GUI as the ***guiadmin*** user:  **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password 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 1: Recovery Scenario 1

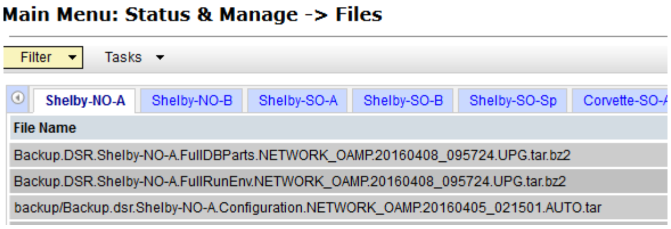
11 □

NOAM GUI: Upload the Backed up Database File

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



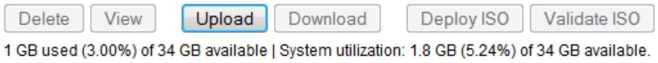
Select the Active NOAM server. The following screen will appear:



Main Menu: Status & Manage -> Files

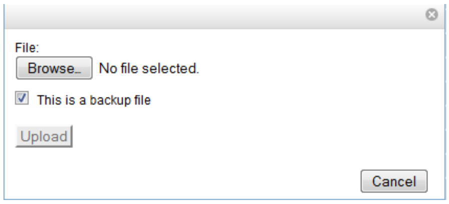
File Name
Backup.DSR.Shelby-NO-A.FullDBParts.NETWORK_OAMP.20160408_095724.UPG.tar.bz2
Backup.DSR.Shelby-NO-A.FullRunEnv.NETWORK_OAMP.20160408_095724.UPG.tar.bz2
backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160405_021501.AUTO.tar

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.

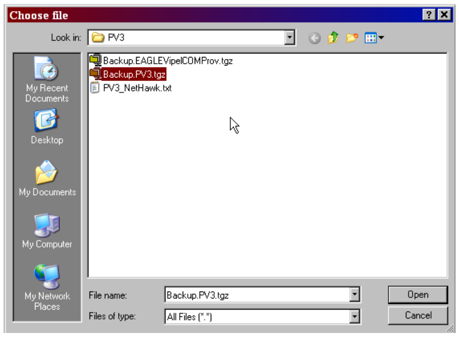
1. Click on **Browse** and locate the backup file
2. Check **This is a backup file** Box
3. Click on Open as shown below.



File:

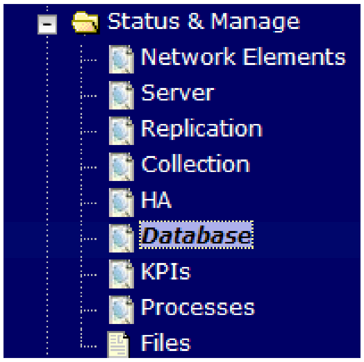
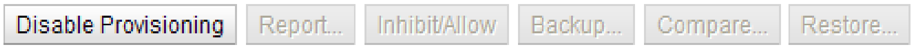
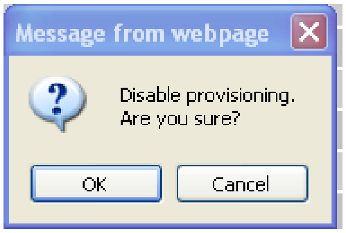
Browse... No file selected.

☑ This is a backup file



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

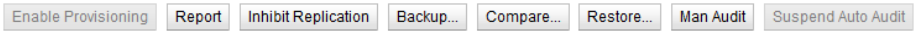
Procedure 1: Recovery Scenario 1

13

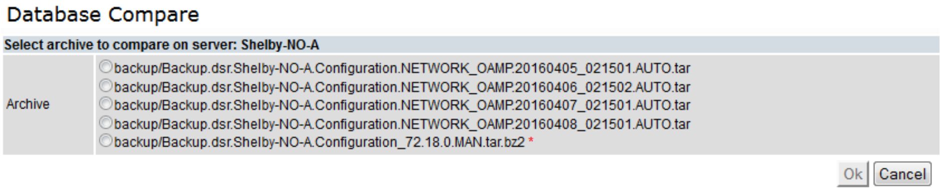
□

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.

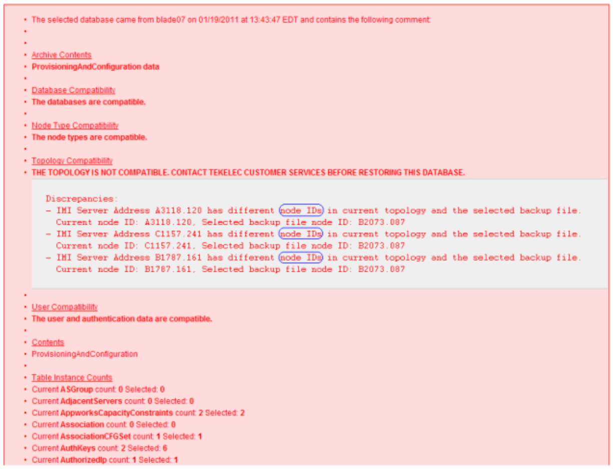

Database Compare

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

Archive
- ○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160405_021501.AUTO.tar
- ○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160406_021502.AUTO.tar
- ○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160407_021501.AUTO.tar
- ○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160408_021501.AUTO.tar
- ○ backup/Backup.dsr.Shelby-NO-A.Configuration_72.18.0.MAN.tar.bz2 *

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.


- The selected database came from blade07 on 01/19/2011 at 13:43:47 EDT and contains the following comment:
-
-
- Archive Contents
- ProvisioningAndConfiguration data
-
- Database Compatibility
- The databases are compatible.
-
- Node Type Compatibility
- The node types are compatible.
-
- Topology Compatibility
- THE TOPOLOGY IS NOT COMPATIBLE. CONTACT TEKELEC CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE.

```
Discrepancies:
- IMI Server Address A3118.120 has different node IDs in current topology and the selected backup file.
  Current node ID: A3118.120, Selected backup file node ID: B2073.087
- IMI Server Address C1157.241 has different node IDs in current topology and the selected backup file.
  Current node ID: C1157.241, Selected backup file node ID: B2073.087
- IMI Server Address B1787.161 has different node IDs in current topology and the selected backup file.
  Current node ID: B1787.161, Selected backup file node ID: B2073.087
```

-
- User Compatibility
- The user and authentication data are compatible.
-
- Contents
- ProvisioningAndConfiguration
-
- Table Instance Counts
- Current ASGroup count: 0 Selected: 0
- Current AdjacentServers count: 0 Selected: 0
- Current AppworksCapacityConstraints count: 2 Selected: 2
- Current Association count: 0 Selected: 0
- Current AssociationCFGSet count: 1 Selected: 1
- Current AuthKeys count: 2 Selected: 6
- Current AuthorizedIp count: 1 Selected: 1

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

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

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

Topology Compatibility
THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.

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

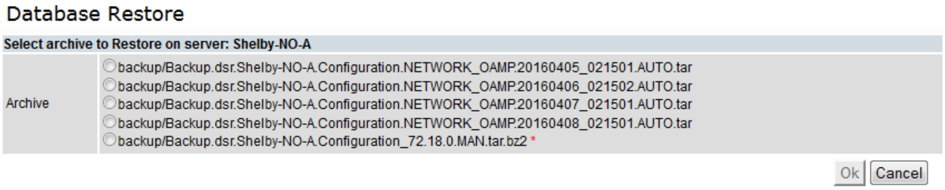
If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.

Procedure 1: Recovery Scenario 1

<table>
<tr>
<td>14
□</td>
<td><b>ACTIVE NOAM:</b> Restore the Database</td>
<td>
Click on <b>Main Menu->Status & Manage->Database</b>

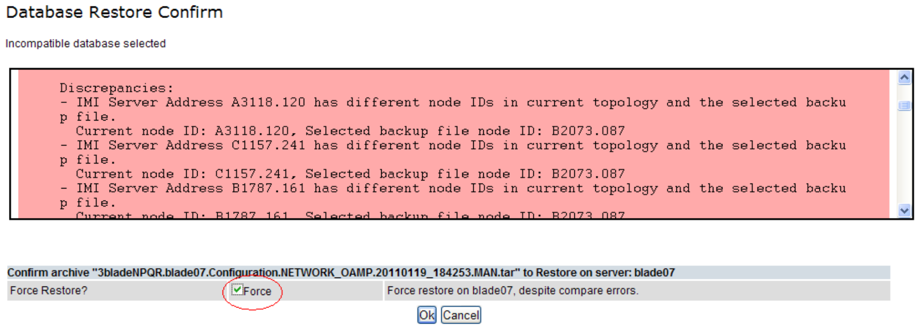
Select the <b>Active NOAM</b> server, and click on <b>Restore</b> as shown below.

The following screen will be displayed. Select the proper back up provisioning and configuration file.

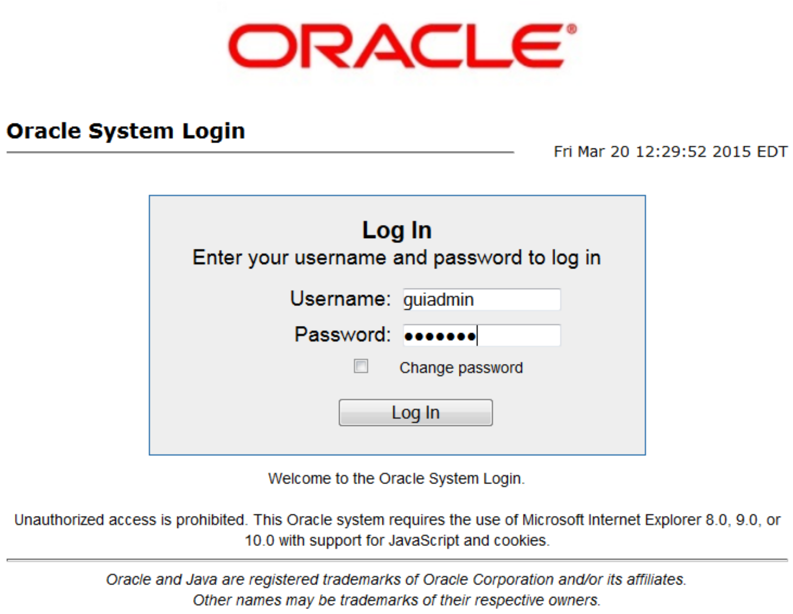

Database Restore
Select archive to Restore on server: Shelby-NO-A
Archive
○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160405_021501.AUTO.tar
○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160406_021502.AUTO.tar
○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160407_021501.AUTO.tar
○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160408_021501.AUTO.tar
○ backup/Backup.dsr.Shelby-NO-A.Configuration_72.18.0.MAN.tar.bz2 *

Click <b>OK</b> Button. The following confirmation screen will be displayed.

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 <b>Force</b> checkbox as shown above and Click <b>OK</b> to proceed with the DB restore.


Database Restore Confirm
Incompatible database selected
<pre>
Discrepancies:
- IMI Server Address A3118.120 has different node IDs in current topology and the selected backu
p file.
  Current node ID: A3118.120, Selected backup file node ID: B2073.087
- IMI Server Address C1157.241 has different node IDs in current topology and the selected backu
p file.
  Current node ID: C1157.241, Selected backup file node ID: B2073.087
- IMI Server Address B1787.161 has different node IDs in current topology and the selected backu
p file.
  Current node ID: B1787.161, Selected backup file node ID: B2073.087
</pre>
Confirm archive "3bladeNPQR.blade07.Configuration.NETWORK_OAMP.20110119_184253.MAN.tar" to Restore on server: blade07
Force Restore? ☑ Force — Force restore on blade07, despite compare errors.

<b>Note:</b> After the restore has started, the user will be logged out of XMI NO GUI since the restored Topology is old data.
</td>
</tr>
</table>

15 □	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:  **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ●●●●●●● □ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*
16 □	**NOAM VIP GUI:** Monitor and Confirm database restoral	Wait for **5-10 minutes** for the System to stabilize with the new topology: Monitor the Info tab for **"Success"**. This will indicate that the restore is complete and the system is stabilized. Following alarms **must** be ignored for NOAM and MP Servers until all the Servers are configured: Alarms with Type Column as **"REPL"** , **"COLL", "HA"** (with mate NOAM), **"DB"** (about Provisioning Manually Disabled) **Note:** Do not pay attention to alarms until all the servers in the system are completely restored. **Note:** The Configuration and Maintenance information will be in the same state it was backed up during initial backup.
17 □	**ACTIVE NOAM:** Login	Login to the recovered Active NOAM via SSH terminal as ***admusr*** user.

Procedure 1: Recovery Scenario 1

<table>
<tr>
<td>18
□</td>
<td><strong>NOAM VIP GUI:</strong> Recover Standby NOAM</td>
<td>

1. Install the second NOAM server by executing procedure *“Configure the Second NOAM Server”,* steps 3-5, 7 from reference [8].

   Note: Execute step 6 if NetBackup is used.

2. If NetBackup is used, execute procedure *“Install NetBackup Client”* from reference [8].

</td>
</tr>
<tr>
<td>19
□</td>
<td><strong>Active NOAM:</strong> Correct the RecognizedAuthority table</td>
<td>

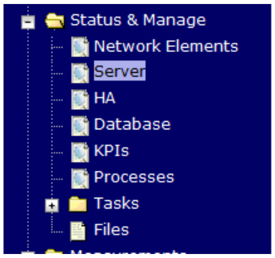
Establish an SSH session to the active NOAM, login as ***admusr***.

Execute the following command:

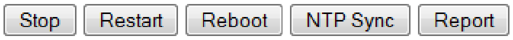
```
$ sudo top.setPrimary
- Using my cluster: A1789
- New Primary Timestamp: 11/09/15 20:21:43.418
- Updating A1789.022: <DSR_NOAM_B_hostname>
- Updating A1789.144: <DSR_NOAM_A_hostname>
```

</td>
</tr>
<tr>
<td>20
□</td>
<td><strong>NOAM VIP GUI:</strong> Restart DSR application</td>
<td>

Navigate to **Main Menu->Status & Manage->Server**,

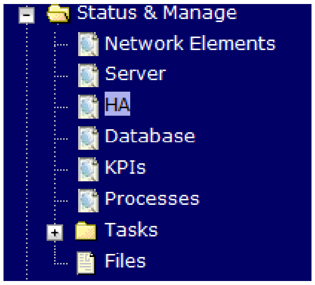


Select the recovered standby NOAM server and click on **Restart**.



</td>
</tr>
<tr>
<td>21
□</td>
<td><strong>NOAM VIP GUI:</strong> Set HA on Standby NOAM</td>
<td>

Navigate to **Status & Manage -> HA**



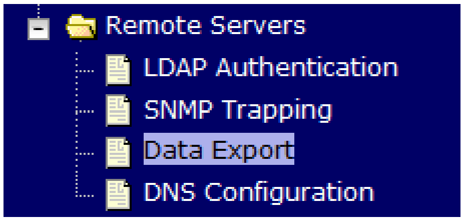
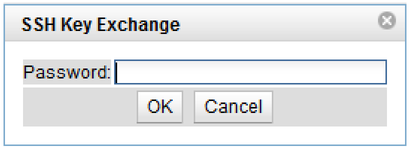
Click on **Edit** at the bottom of the screen

Select the standby NOAM server, set it to **Active**

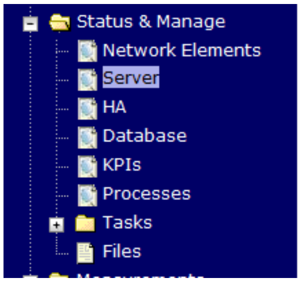
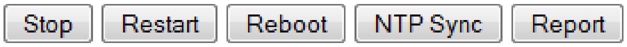
Press **OK**

</td>
</tr>
</table>

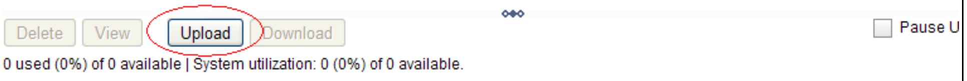
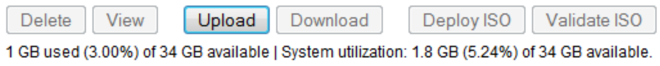
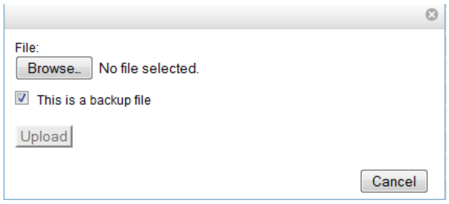
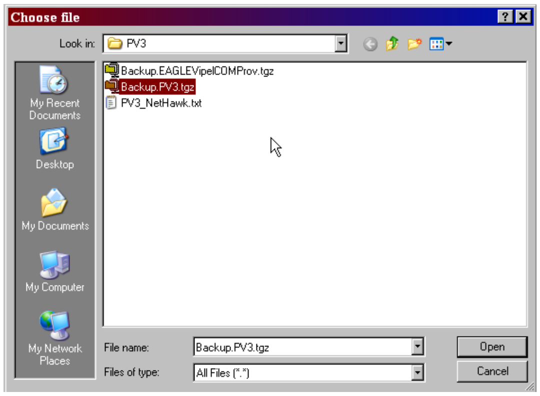
Procedure 1: Recovery Scenario 1

22 □	**NOAM VIP GUI:** Perform Keyexchange with Export Server	Navigate to **Main Menu -> Administration -> Remote Servers -> Data Export**  Remote Servers LDAP Authentication SNMP Trapping Data Export DNS Configuration Click on **SSH Key Exchange** at the bottom of the screen Enter the Password and press **OK** 
23 □	**NOAM VIP GUI:** Stop Replication to the C-Level Servers of this Site.	 ***!! !! Warning !! !!*** Prior to continuing this procedure, replication to C Level servers at the SOAM site being recovered ***MUST*** be inhibited. **Failure to inhibit replication to the working c-level servers will result in their database being destroyed!** Execute **Appendix E**: Inhibit A and B Level Replication on C-Level Servers to inhibit replication to working C Level servers before continuing.
24 □	**Configure SOAM TVOE Server Blades**	**If the TVOE backup has already been executed (step 5), skip this step** If a TVOE backup of the SOAM server blades is not available, execute procedure *"Configure SOAM TVOE Server Blades"* from reference [8]

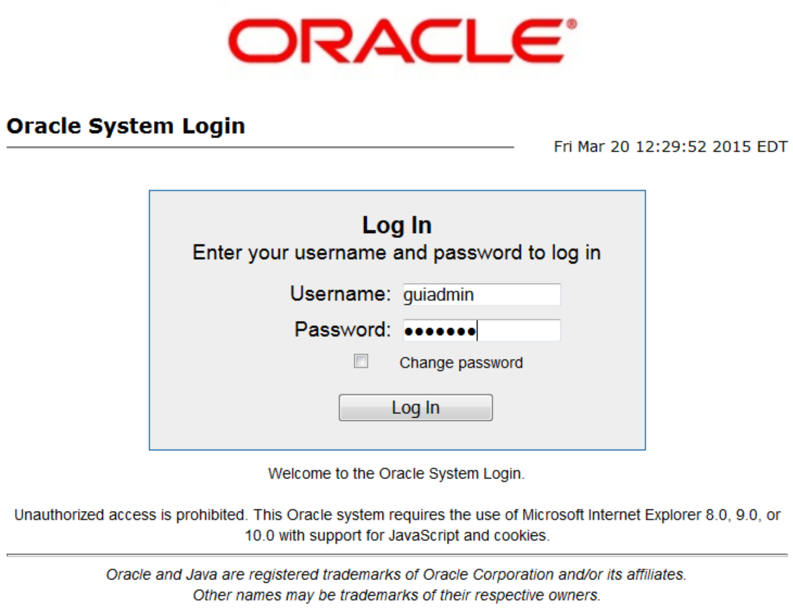
Procedure 1: Recovery Scenario 1

25 □	**Create and IPM SOAM VMs**	1. Execute procedure *“Create SOAM Guest VMs”* for the failed SOAM VMs and MP blades from reference [8]. 2. Execute procedure *“IPM Blades and VMs”* for the failed SOAM VMs and MP blades from reference [8]. 3. Execute procedure *“Install the Application”* for the failed SOAM VMs and MP blades from reference [8].
26 □	**Recover Active SOAM Server**	1. Execute procedure “Configure the SOAM Servers”, steps 1-3, and 5-8 from reference [8]. **Note:** If you are using NetBackup, also execute step 10 2. If you are using NetBackup, execute procedure *“Install NetBackup Client”* from reference [8].
27 □	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered Active SOAM server and click on **Restart**. 

Procedure 1: Recovery Scenario 1

28 □	**NOAM VIP GUI:** Upload the Backed up SOAM Database File	Navigate to **Main Menu->Status & Manage->Files** 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.  0 used (0%) of 0 available | System utilization: 0 (0%) of 0 available.  Delete View Upload Download Deploy ISO Validate ISO 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.  File: Browse... No file selected. ☑ This is a backup file  Choose file Look in: PV3 My Recent Documents Desktop My Documents My Computer My Network Places Open Cancel Backup.EAGLEVipelCOMProv.tgz Backup.PV3.tgz PV3_NetHawk.txt File name: Backup.PV3.tgz Files of type: All Files (*.*) Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.

Procedure 1: Recovery Scenario 1

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® **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*

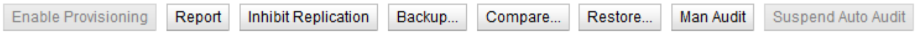
Procedure 1: Recovery Scenario 1

30 □

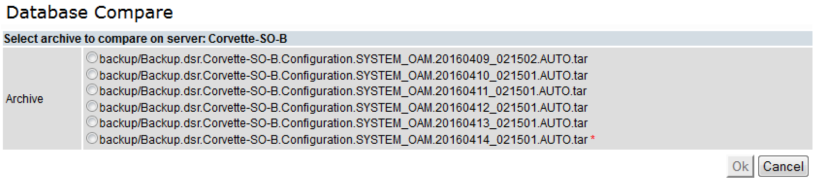
Recovered SOAM GUI: Verify the Archive Contents and Database Compatibility

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.



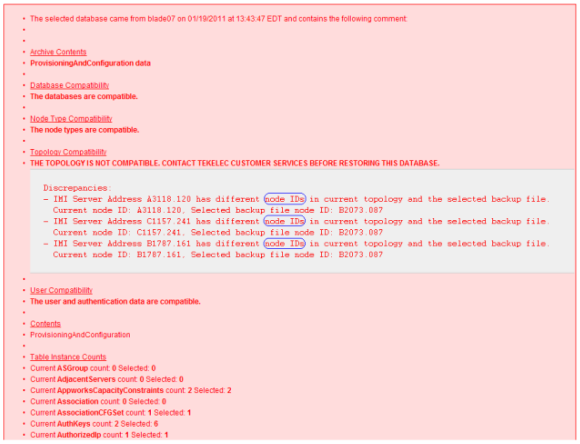
Database Compare

Select archive to compare on server: Corvette-SO-B

Archive	○ backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160409_021502.AUTO.tar ○ backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160410_021501.AUTO.tar ○ backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160411_021501.AUTO.tar ○ backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160412_021501.AUTO.tar ○ backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160413_021501.AUTO.tar ○ backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160414_021501.AUTO.tar *

Verify that the output window matches the screen below.

Note: You will get a database mismatch regarding the NodeIDs of the blades. That is expected. If that is the only mismatch, proceed, otherwise stop and contact **Appendix L: My Oracle** Support (MOS)



- The selected database came from blade07 on 01/19/2011 at 13:43:47 EDT and contains the following comment:
-
-
- Archive Contents
- **ProvisioningAndConfiguration data**
-
- Database Compatibility
- **The databases are compatible.**
-
- Node Type Compatibility
- **The node types are compatible.**
-
- Topology Compatibility
- **THE TOPOLOGY IS NOT COMPATIBLE. CONTACT TEKELEC CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE.**

```
Discrepancies:
- IMI Server Address A3118.120 has different node IDs in current topology and the selected backup file.
  Current node ID: A3118.120, Selected backup file node ID: B2073.087
- IMI Server Address C1157.241 has different node IDs in current topology and the selected backup file.
  Current node ID: C1157.241, Selected backup file node ID: B2073.087
- IMI Server Address B1787.161 has different node IDs in current topology and the selected backup file.
  Current node ID: B1787.161, Selected backup file node ID: B2073.087
```

-
- User Compatibility
- **The user and authentication data are compatible.**
-
- Contents
- ProvisioningAndConfiguration
-
- Table Instance Counts
- Current **ASGroup** count: **0** Selected: **0**
- Current **AdjacentServers** count: **0** Selected: **0**
- Current **AppworksCapacityConstraints** count: **2** Selected: **2**
- Current **Association** count: **0** Selected: **0**
- Current **AssociationCFGSet** count: **1** Selected: **1**
- Current **AuthKeys** count: **2** Selected: **6**
- Current **AuthorizedIp** count: **1** Selected: **1**

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

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

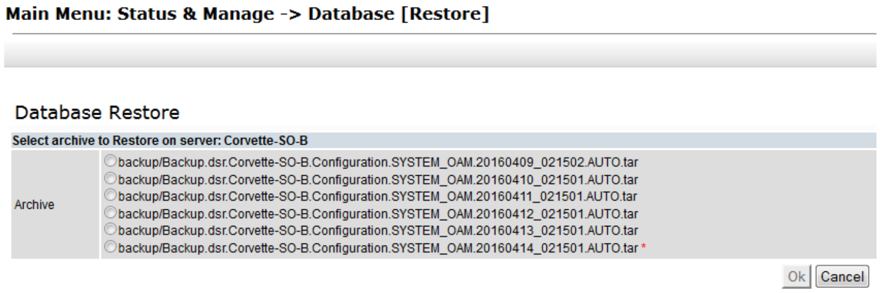
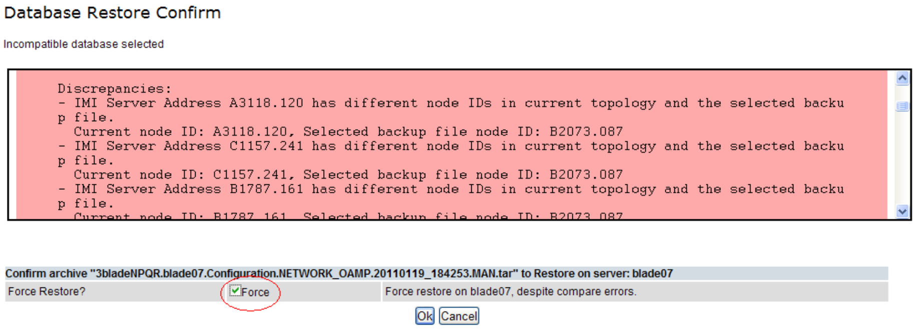
Note: The following is expected Output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM:

Topology Compatibility
THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.

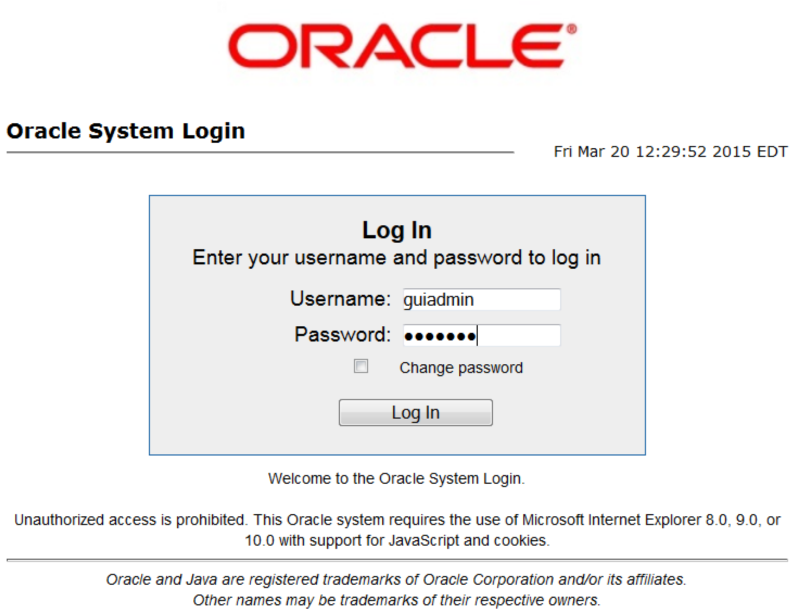
Note: We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility.

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

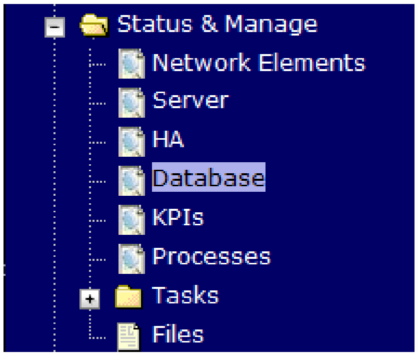
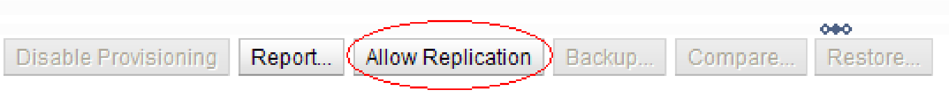
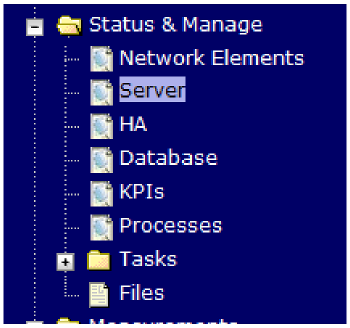
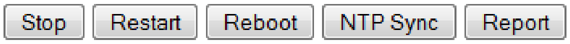
Procedure 1: Recovery Scenario 1

31
□
	Recovered SOAM GUI: Restore the Database	Select the **Active SOAM** server, and click on **Restore** as shown below.
		
		The following screen will be displayed. Select the proper back up provisioning and configuration file.
		
		Main Menu: Status & Manage -> Database [Restore]
		Database Restore
		Select archive to Restore on server: Corvette-SO-B
		Archive
		○backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160409_021502.AUTO.tar
		○backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160410_021501.AUTO.tar
		○backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160411_021501.AUTO.tar
		○backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160412_021501.AUTO.tar
		○backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160413_021501.AUTO.tar
		○backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160414_021501.AUTO.tar *
		Ok Cancel
		Click **OK** Button. The following confirmation screen will be displayed.
		
		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.
		
		Database Restore Confirm
		Incompatible database selected
		`Discrepancies:`
		`- IMI Server Address A3118.120 has different node IDs in current topology and the selected backu`
		`p file.`
		`  Current node ID: A3118.120, Selected backup file node ID: B2073.087`
		`- IMI Server Address C1157.241 has different node IDs in current topology and the selected backu`
		`p file.`
		`  Current node ID: C1157.241, Selected backup file node ID: B2073.087`
		`- IMI Server Address B1787.161 has different node IDs in current topology and the selected backu`
		`p file.`
		`  Current node ID: B1787.161, Selected backup file node ID: B2073.087`
		Confirm archive "3bladeNPQR.blade07.Configuration.NETWORK_OAMP.20110119_184253.MAN.tar" to Restore on server: blade07
		Force Restore? ☑Force Force restore on blade07, despite compare errors.
		Ok Cancel
		Note: After the restore has started, the user will be logged out of XMI SOAM GUI since the restored Topology is old data.

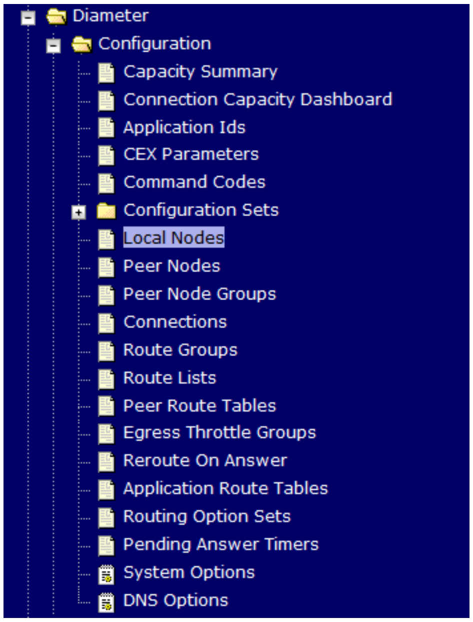
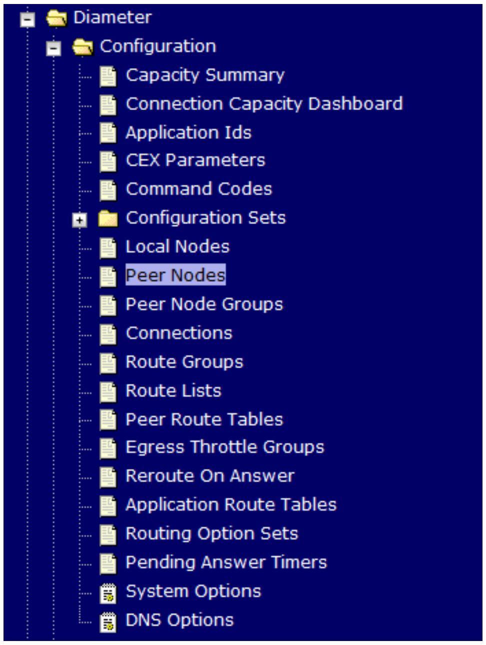
32 □	**Recovered SOAM GUI**: Monitor and Confirm database restoral	Wait for **5-10 minutes** for the System to stabilize with the new topology: Monitor the Info tab for **"Success"**. This will indicate that the restore is complete and the system is stabilized. **Note:** Do not pay attention to alarms until all the servers in the system are completely restored. **Note:** The Configuration and Maintenance information will be in the same state it was backed up during initial backup.

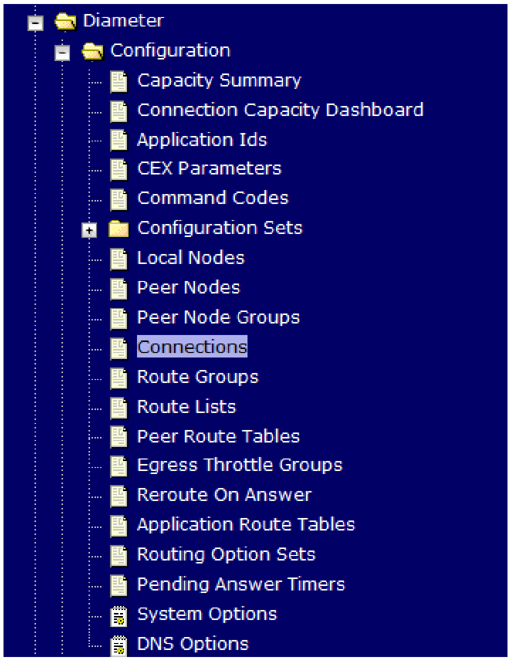
33 □	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:  **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*
34 □	**NOAM VIP GUI:** Recover the Remaining SOAM Servers	Recover the **remaining** SOAM servers (**standby, spare**) by repeating the **following steps** for each SOAM server: 1. Execute procedure “Configure the SOAM Servers”, steps 1-3, and 5-8 from reference [8]. **Note:** If you are using NetBackup, also execute step 10 2. If you are using NetBackup, execute procedure *“Install NetBackup Client”* from reference [8].

Procedure 1: Recovery Scenario 1

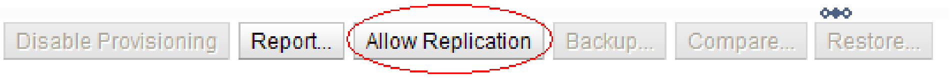
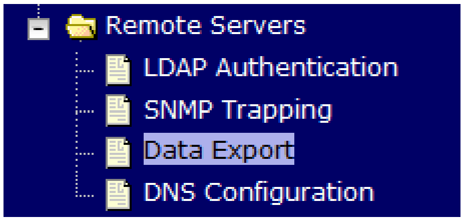
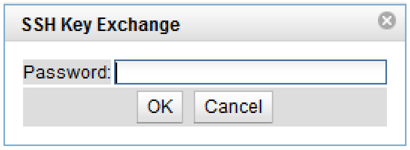
35 □	**NOAM VIP GUI:** Start replication on the recovered standby SOAM	Un-Inhibit *(Start)* Replication to the recovered **Standby SOAM** Navigate to **Status & Manage -> Database**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click on the Allow Replication button as shown below on the recovered standby SOAM server. Verify that the replication on all servers is allowed. This can be done by clicking on each server and checking that the button below shows “Inhibit Replication”, and **NOT** “Allow Replication”.  Disable Provisioning Report... Allow Replication Backup... Compare... Restore...
36 □	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered standby SOAM server and click on **Restart**. 

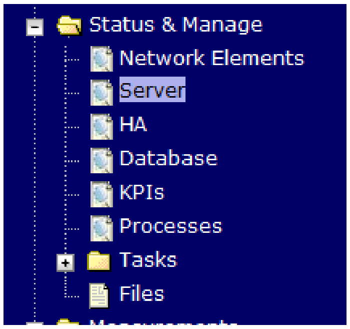
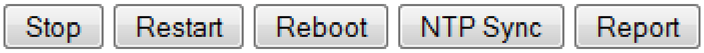
Procedure 1: Recovery Scenario 1

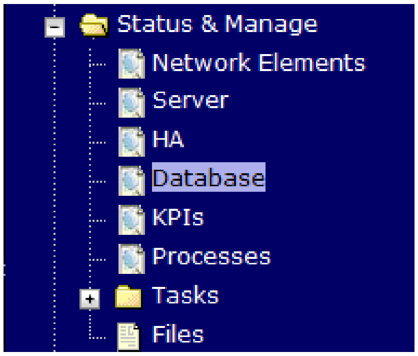
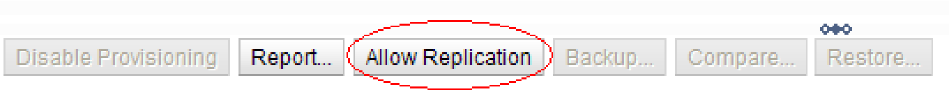
37 □	**SOAM VIP GUI:** Verify the Local Node Info	Navigate to **Main Menu->Diameter->Configuration->Local Node**  Diameter Configuration Capacity Summary Connection Capacity Dashboard Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes Peer Node Groups Connections Route Groups Route Lists Peer Route Tables Egress Throttle Groups Reroute On Answer Application Route Tables Routing Option Sets Pending Answer Timers System Options DNS Options Verify that all the local nodes are shown.
38 □	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Diameter Configuration Capacity Summary Connection Capacity Dashboard Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes Peer Node Groups Connections Route Groups Route Lists Peer Route Tables Egress Throttle Groups Reroute On Answer Application Route Tables Routing Option Sets Pending Answer Timers System Options DNS Options Verify that all the peer nodes are shown.

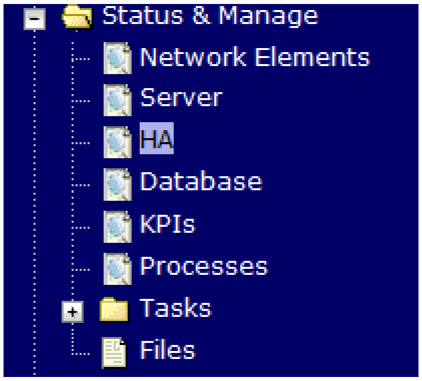
39 □	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections**  Diameter Configuration Capacity Summary Connection Capacity Dashboard Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes Peer Node Groups Connections Route Groups Route Lists Peer Route Tables Egress Throttle Groups Reroute On Answer Application Route Tables Routing Option Sets Pending Answer Timers System Options DNS Options Verify that all the connections are shown.
40 □	**ACTIVE NOAM:** Activate Optional Features	Establish an SSH session to the active NOAM, login as ***admusr.*** Refer to **section** 1.5 Optional Features to activate any features that were previously activated.

Procedure 1: Recovery Scenario 1

41 □	**NOAM VIP GUI:** Start Replication on Working C-Level Servers	Un-Inhibit *(Start)* Replication to the **working** C-Level Servers which belong to the same site as of the failed SOAM servers. Execute **Appendix F**: Un-Inhibit A and B Level Replication on C-Level Servers If the *"Repl Status"* is set to "Inhibited", click on the **Allow Replication** button as shown below using the following order, otherwise if none of the servers are inhibited, skip this step and continue with the next step: • Active NOAM Server • Standby NOAM Server • Active SOAM Server • Standby SOAM Server • Spare SOAM Server *(if applicable)* • Active DR NOAM Server • Standby DR NOAM Server • MP/IPFE Servers *(if MPs are configured as Active/Standby, start with the Active MP, otherwise the order of the MPs does not matter)* • SBRS *(if SBR servers are configured, start with the active SBR, then standby, then spare)* Verify that the replication on all the working servers is allowed. This can be done by clicking on each server and checking that the button below shows "Inhibit Replication", and **NOT** "Allow Replication".  Disable Provisioning Report... Allow Replication Backup... Compare... Restore...
42 □	**SOAM VIP GUI:** Perform Key Exchange with Export Server	Navigate to **Main Menu -> Administration -> Remote Servers -> Data Export**  Remote Servers LDAP Authentication SNMP Trapping Data Export DNS Configuration Click on **SSH Key Exchange** at the bottom of the screen Enter the Password and press **OK** 

43 □	**(PCA Only) Activate PCA Feature**	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. **Note:** If not all SOAM sites are ready at this point, then you should repeat activation for each *new* SOAM site that comes online.
44 □	**NOAM VIP GUI:** Recover the C-Level Server (DA-MP, SBRs, IPFE, SS7-MP)	Execute procedure *“Configure MP Blade Servers”*, Steps 1, 7, 11-14, and 17 from reference [8]. **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. Repeat this step for any remaining failed MP servers.
45 □	**NOAM VIP GUI:** Restart DSR Application on recovered C-Level Servers.	Navigate to **Main Menu->Status & Manage->Server**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered C-Level servers and click on **Restart**. 

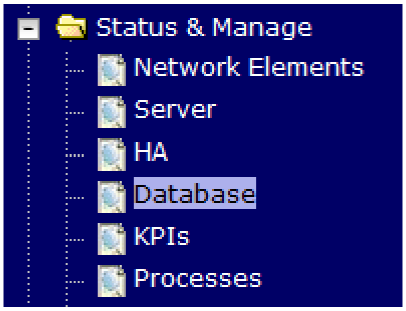
46 □	**NOAM VIP GUI:** Start replication on all C-Level Servers	Un-Inhibit *(Start)* Replication to the **ALL** C-Level Servers Navigate to **Status & Manage -> Database**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files If the *"Repl Status"* is set to "Inhibited", click on the Allow Replication button as shown below using the following order: • Active NOAM Server • Standby NOAM Server • Active SOAM Server • Standby SOAM Server • Spare SOAM Server *(if applicable)* • Active DR NOAM Server • Standby DR NOAM Server • MP/IPFE Servers *(if MPs are configured as Active/Standby, start with the Active MP, otherwise the order of the MPs does not matter)* Verify that the replication on all servers is allowed. This can be done by clicking on each server and checking that the button below shows "Inhibit Replication", and **NOT** "Allow Replication".  Disable Provisioning Report... Allow Replication Backup... Compare... Restore...

47 □	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click on **Edit** at the bottom of the screen For each server whose Max Allowed HA Role is set to Standby, set it to **Active** Press **OK**
48 □	**ACTIVE NOAM:** Activate Optional Features	Establish an SSH session to the active NOAM, login as ***admusr.*** Refer to **section** 1.5 Optional Features to activate any features that were previously activated.
49 □	**ACTIVE NOAM:** Perform key exchange between the active-NOAM and recovered servers.	Establish an SSH session to the Active NOAM, login as ***admusr.*** Execute the following command to perform a keyexchange from the active NOAM to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>` **Note:** If an export server is configured, perform this step.

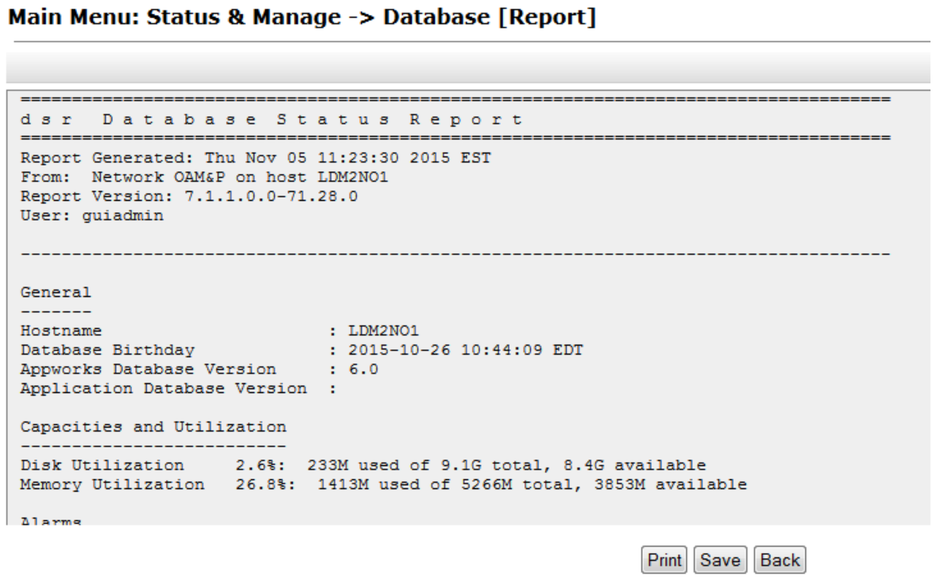
50 □

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]

```
=====================================================================================
dsr  Database Status Report
=====================================================================================
Report Generated: Thu Nov 05 11:23:30 2015 EST
From:  Network OAM&P on host LDM2NO1
Report Version: 7.1.1.0.0-71.28.0
User: guiadmin

-------------------------------------------------------------------------------------


General
-------
Hostname                      : LDM2NO1
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
```

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

Procedure 1: Recovery Scenario 1

51 □	**ACTIVE NOAM:** Verify Replication Between Servers.	Login to the Active NOAM via SSH terminal as ***admusr***. Execute the following command:

```
$ sudo irepstat –m
```

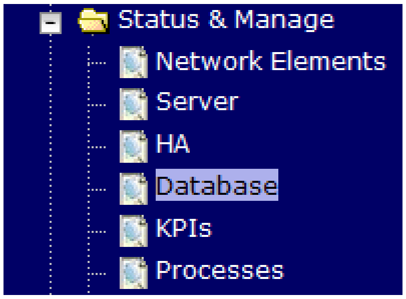
Output like below shall be generated:

```
-- 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
```

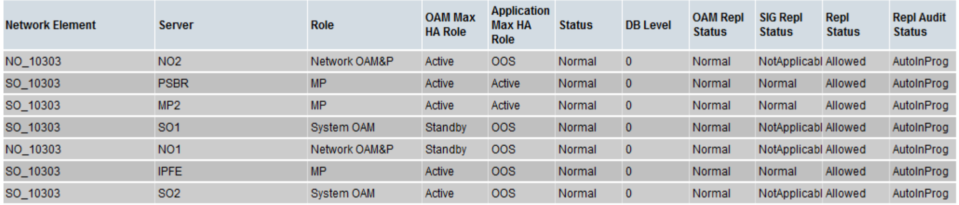
52 □

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:

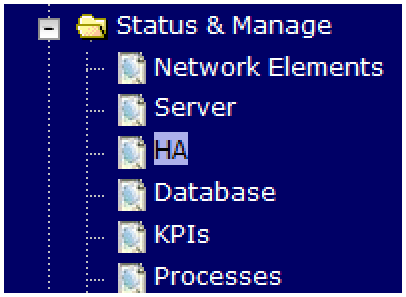


Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
NO_10303	NO2	Network OAM&P	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg
SO_10303	PSBR	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg
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

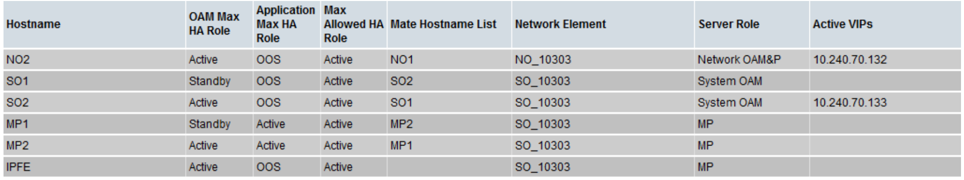
53 □

NOAM VIP GUI: Verify the HA Status

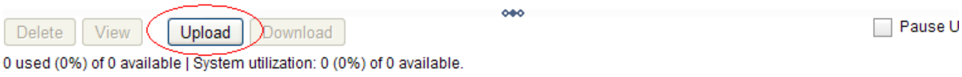
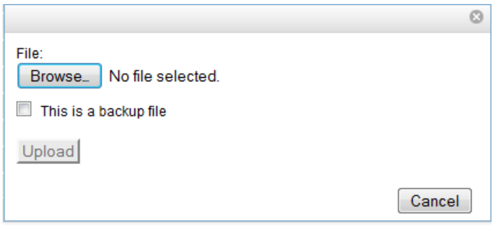
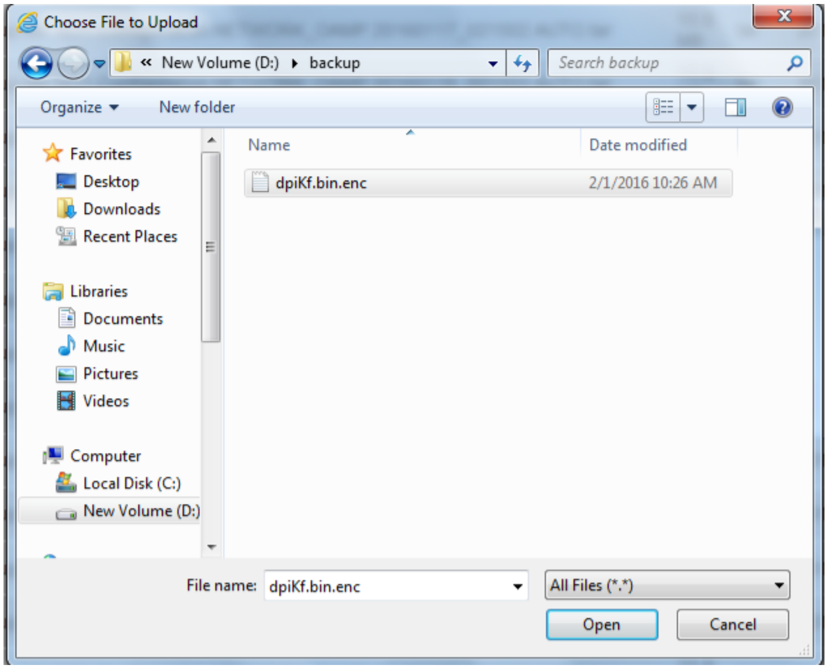
Click on **Main Menu->Status and Manage->HA**



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



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

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.  0 used (0%) of 0 available | System utilization: 0 (0%) of 0 available. Click on Browse and Locate the DpiKf.bin.encr file and click on Open as shown below.  File: No file selected. □ This is a backup file  Choose File to Upload « New Volume (D:) ▸ backup Search backup Organize ▾ New folder Favorites Desktop Downloads Recent Places Libraries Documents Music Pictures Videos Computer Local Disk (C:) New Volume (D:) Name Date modified All Files (*.*) Open Cancel dpiKf.bin.enc 2/1/2016 10:26 AM File name: dpiKf.bin.enc 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.

55

□

NOAM VIP: Copy and distribute RADIUS Key file on Active NOAM (RADIUS Only)-Part 1

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)

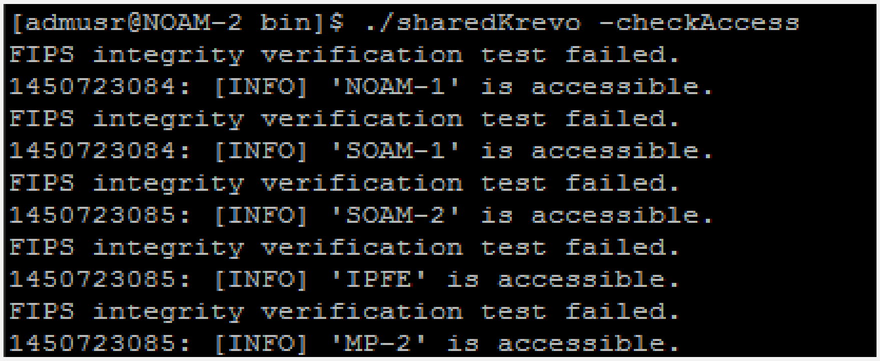
Login to the Active NOAM VIP via SSH terminal as ***admusr*** user.

Execute the following commands to copy the key file:

```
$ cd /usr/TKLC/dpi/bin

$ ./sharedKrevo -decr

$ sudo rm /var/TKLC/db/filemgmt/<backed up key file
name>
```

Execute following command to check if all the servers in topology are accessible:

```
$ ./sharedKrevo –checkAccess
```



```
[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.
```

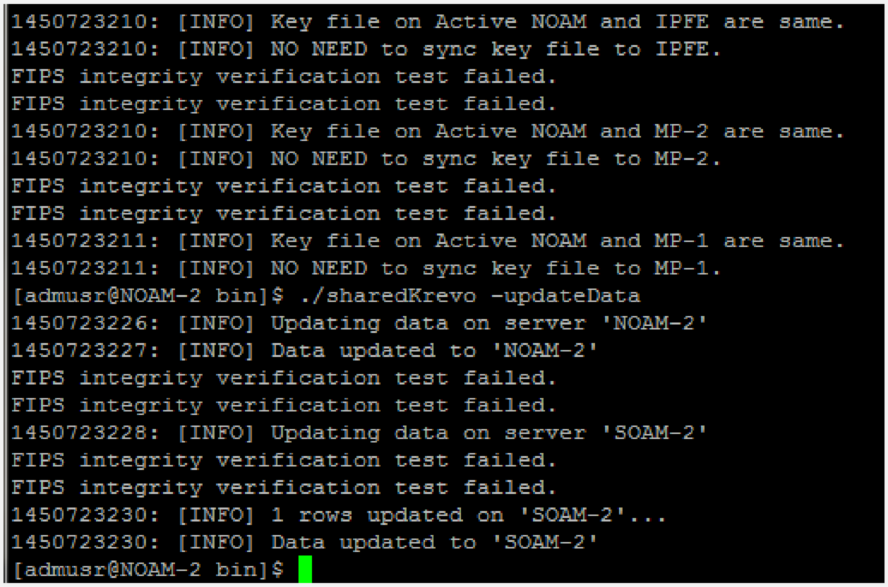
Note: If all the servers are not accessible then refer Appendix L: My Oracle Support (MOS).

Procedure 1: Recovery Scenario 1

56 □	**NOAM VIP:** Copy and distribute RADIUS Key file on Active NOAM (RADIUS Only)-Part 2	Execute following command to distribute key file to all the servers in the topology :

```
$ ./sharedKrevo -synchronize

$ ./sharedKrevo -updateData
```

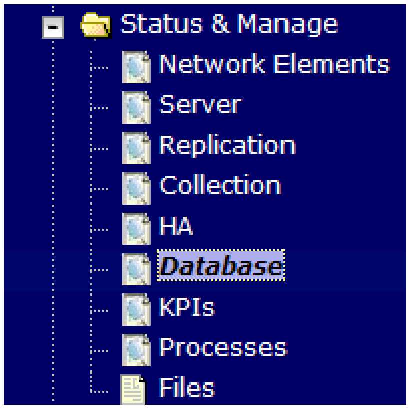
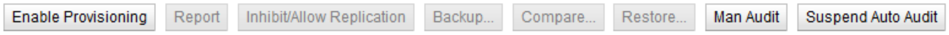
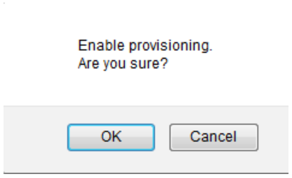
Example output:



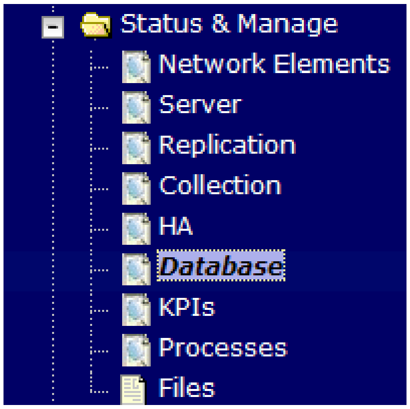
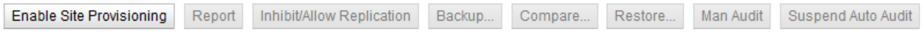
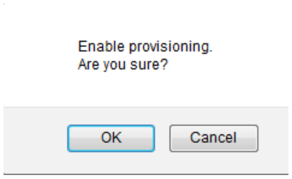
```
1450723210: [INFO] Key file on Active NOAM and IPFE are same.
1450723210: [INFO] NO NEED to sync key file to IPFE.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723210: [INFO] Key file on Active NOAM and MP-2 are same.
1450723210: [INFO] NO NEED to sync key 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]$
```

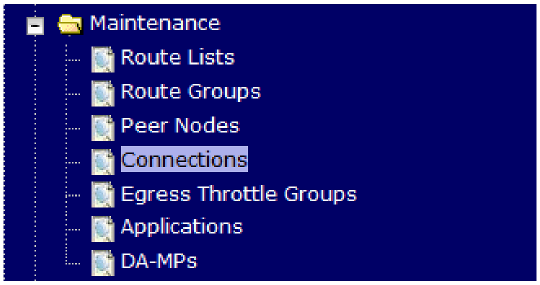
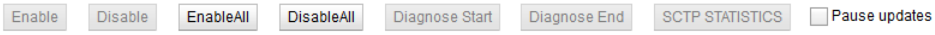
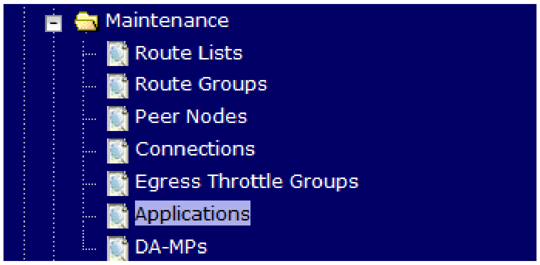
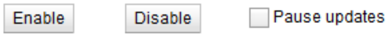
Note: For any errors refer **Appendix L: My Oracle Support (MOS).**

Procedure 1: Recovery Scenario 1

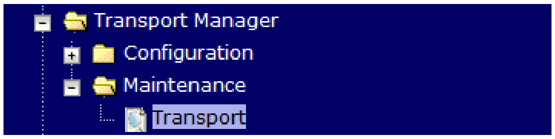
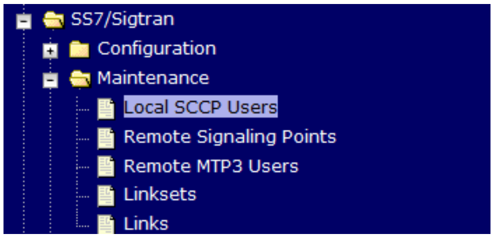
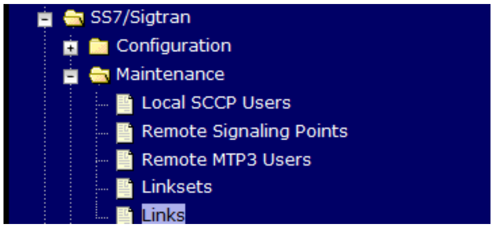
57 □	**NOAM GUI:** Enable Provisioning	Click on **Main Menu->Status & Manage->Database**  Status & Manage Network Elements Server Replication Collection HA Database KPIs Processes Files Enable Provisioning by clicking on **Enable Provisioning** button at the bottom of the screen as shown below.  Enable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

Procedure 1: Recovery Scenario 1

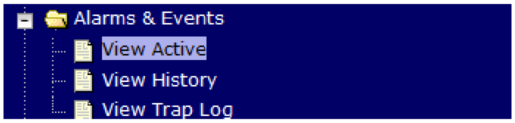
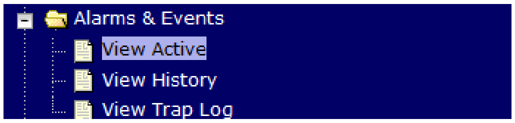
58 □	**SOAM GUI:** Enable Site Provisioning	Click on **Main Menu->Status & Manage->Database**  Status & Manage Network Elements Server Replication Collection HA Database KPIs Processes Files Enable Site Provisioning by clicking on **Enable Site Provisioning** button at the bottom of the screen as shown below.  Enable Site Provisioning Report Inhibit/Allow Replication Backup... Compare... Restore... Man Audit Suspend Auto Audit A confirmation window will appear, press **OK** to enable Provisioning.  Enable provisioning. Are you sure?
59 □	**MP Servers:** Disable SCTP Auth Flag	For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [14] Execute this procedure on all Failed MP Servers.

60 □	**SOAM VIP GUI:** Enable Connections if needed	Navigate to **Main Menu->Diameter->Maintenance->Connections**  Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups Applications DA-MPs Select each connection and click on the **Enable** button. Alternatively you can enable all the connections by selecting the **EnableAll** button.  Enable Disable EnableAll DisableAll Diagnose Start Diagnose End SCTP STATISTICS □ Pause updates Verify that the Operational State is Available. **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
61 □	**SOAM VIP GUI:** Enable Optional Features	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups Applications DA-MPs Select the optional feature application configured in **step 42**. Click the **Enable** button. 

Procedure 1: Recovery Scenario 1

62 □	**SOAM VIP GUI:** Re-enable Transports if Needed	Navigate to **Main Menu->Transport Manager -> Maintenance -> Transport**  Transport Manager Configuration Maintenance Transport Select each transport and click on the **Enable** button Verify that the Operational Status for each transport is Up.
63 □	**SOAM VIP GUI:** Re-enable MAPIWF application if needed	Navigate to **Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users**  SS7/Sigtran Configuration Maintenance Local SCCP Users Remote Signaling Points Remote MTP3 Users Linksets Links Click on the **Enable** button corresponding to MAPIWF Application Name. Verify that the SSN Status is Enabled.
64 □	**SOAM VIP GUI:** Re-enable links if needed	Navigate to **Main Menu->SS7/Sigtran->Maintenance->Links**  SS7/Sigtran Configuration Maintenance Local SCCP Users Remote Signaling Points Remote MTP3 Users Linksets Links Click on **Enable** button for each link. Verify that the Operational Status for each link is Up.

Procedure 1: Recovery Scenario 1

65 □	**SOAM VIP GUI:** Examine All Alarms	Navigate to **Main Menu->Alarms & Events->View Active**  Alarms & Events View Active View History View Trap Log Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix L: My Oracle** Support (MOS).
66 □	**NOAM VIP GUI:** Examine All Alarms	Login to the NOAM VIP if not already logged in. Navigate to **Main Menu->Alarms & Events->View Active**  Alarms & Events View Active View History View Trap Log Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix L: My Oracle** Support (MOS).
67 □	**Restore GUI Usernames and Passwords**	If applicable, Execute steps in **Section 6.0** Resolving User Credential Issues after Database Restore to recover the user and group information restored.
68 □	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**: DSR Database Backup to back up the Configuration databases:
69 □	**Recover IDIH**	If IDIH were affected, refer to **Section 11** to perform disaster recovery on IDIH.

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.

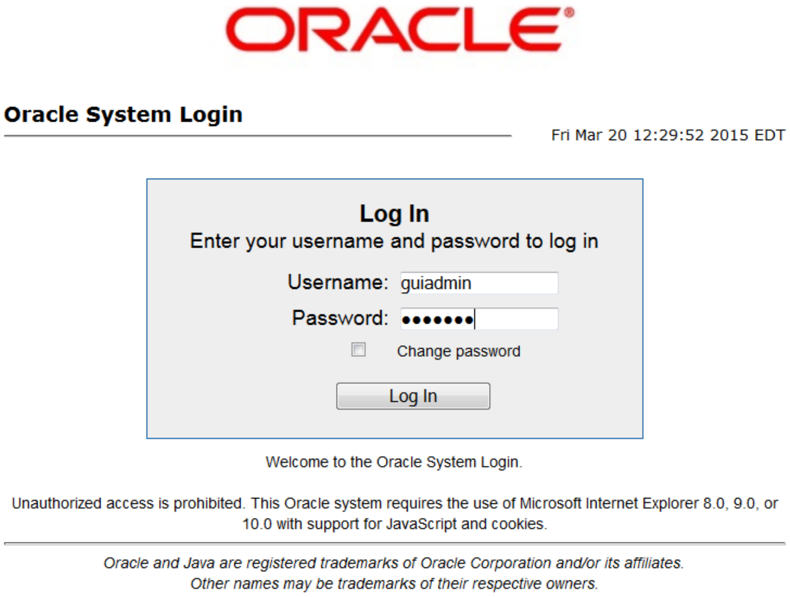
Recover **Active SOAM** server by recovering base hardware and software.

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

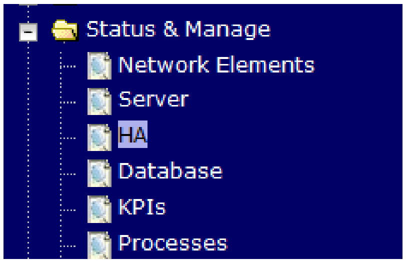
Recover any failed **SOAM and MP** servers by recovering base hardware and software.

- 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

S T E 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. 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 □	**Workarounds**	Refer to **Appendix G**: Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
2 □	**Gather Required Materials**	Gather the documents and required materials listed in **Section 3.1** Required Materials
3 □	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:  Oracle System Login Fri Mar 20 12:29:52 2015 EDT Log In Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*

Procedure 2: Recovery Scenario 2

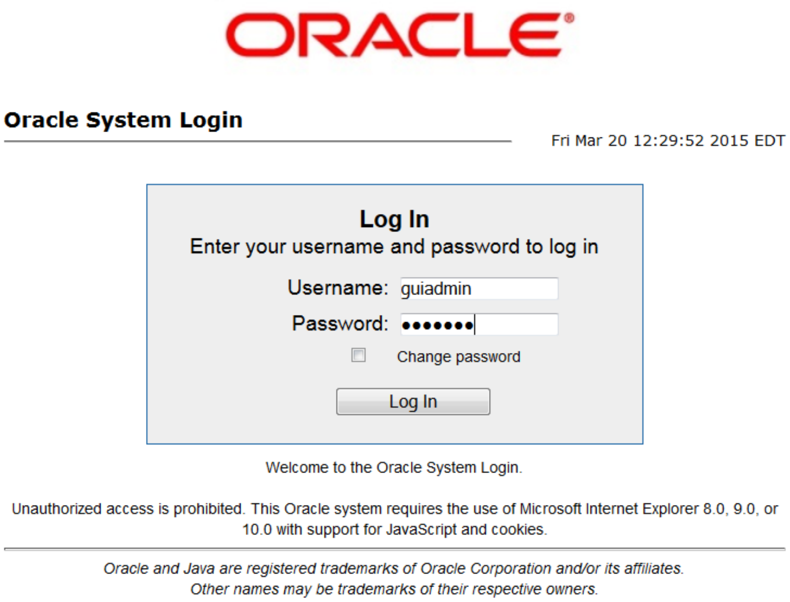
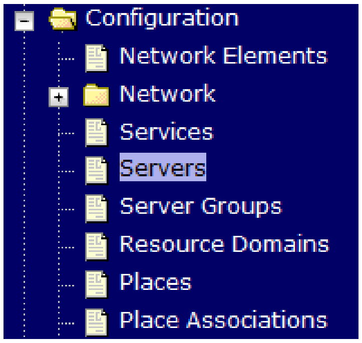
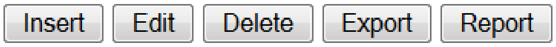
4 □	**Active NOAM:** Set Failed Servers to Standby	Navigate to **Main Menu -> Status & Manage -> HA**  Status & Manage Network Elements Server HA Database KPIs Processes Select **Edit** Set the Max Allowed HA Role drop down box to **Standby** for the failed servers. Select **Ok**
5 □	**Replace Failed Equipment**	HW vendor to replace the failed equipment
6 □	**RMS NOAM Failure:** Configure BIOS Settings and Update Firmware	If the failed server is **NOT** a rack mount server, **skip to step 9.** 1. Configure and verify the BIOS settings by executing procedure *"Configure the RMS Server BIOS Settings"* from reference [10] 2. Verify and/or upgrade server firmware by executing procedure *"Upgrade Management Server Firmware"* from reference[10] **Note:** Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.
7 □	**RMS NOAM Failure:** Backups Available	If the failed server is **NOT** a rack mount server, **skip to step 9.** This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, **skip this step**. 1. Restore the TVOE backup by executing Appendix H: Restore TVOE Configuration from Backup Media If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing 2. Appendix I: Restore PMAC from Backup

Procedure 2: Recovery Scenario 2

8 □	**Recover Failed Aggregation/ Enclosure Switches, and OAs**	Recover failed OAs, aggregation and enclosure switches if needed. Backups Available: 1. Refer to Appendix B: Recovering/Replacing Failed 3rd Party Components (Switches, OAs)to recover failed OAs, aggregation, and enclosure switches Backups **NOT** Available: 1. Execute section *"HP C-7000 Enclosure Configuration"* 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.
9 □	**RMS NOAM Failure:** Backups **NOT** Available	If the failed server is **NOT** a rack mount server, **skip to step 9.** This step assumes that TVOE and PMAC backups **NOT** are available, if the TVOE and PMAC have already been restored, **skip this step.** If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. Section *"Configure and IPM Management Server"* from reference [10]. 2. Section *"Install PM&C"* from reference [10]. 3. Section *"Configure PM&C"* from reference [10]. If the PMAC is **NOT** located on the same TVOE host as the failed NOAM, Execute the following sections/procedures 1. Section *"Installing TVOE on Rack Mount Server(s)"* from reference [10].
10 □	**HP-Class Blade Failure:** Configure Blade Server iLO, Update Firmware/BIOS Settings	If the failed server is **NOT** an HP C-Class Blade, **skip to step 13.** 1. Execute procedure *"Configure Blade Server iLO Password for Administrator Account"* from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing section *"Server Blades Installation Preparation"* from reference [10]

Procedure 2: Recovery Scenario 2

11 □	**HP-Class Blade Failure:** Backups Available	If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 13.** This step assumes that TVOE backups are available, if backups are **NOT** available, **skip this step**. 1. Install and configure TVOE on failed TVOE blade servers by executing section *"Install TVOE on Blade Servers"* 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.
12 □	**HP-Class Blade Failure:** Backups **NOT** Available	If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 13.** This step assumes that TVOE backups are **NOT** are available 1. Install and configure TVOE on failed TVOE blade servers by executing section *"Install TVOE on Blade Servers"* 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] **Note:** Although the title of the procedure is related to SOAMs only, execute this procedure for any failed NOAMs located on TVOE server blades.
13 □	**Create VMs**	Execute Appendix K: Create NOAM/SOAM Virtual Machines to create the NOAM and SOAM VMs on failed TVOE servers.
14 □	**IPM and Install DSR Application on Failed Guest/Servers**	1. Execute procedure *"IPM Blades and VMs"* for the failed SOAM VMs and MP blades from reference [8]. 2. Execute procedure *"Install the Application"* for the failed SOAM VMs and MP blades from reference [8].
15 □	**Install NetBackup Client (Optional)**	If NetBackup is used execute procedure *"Install NetBackup Client"* from reference [8]

16 □	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:  **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*
17 □	**NOAM VIP GUI:** Export the Initial Configuration	Navigate to **Main Menu -> Configuration -> Servers.**  Configuration Network Elements Network Services Servers Server Groups Resource Domains Places Place Associations From the GUI screen, select the failed NOAM server and then select **Export** to generate the initial configuration data for that server. 

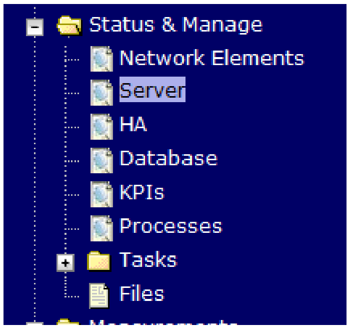
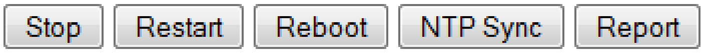
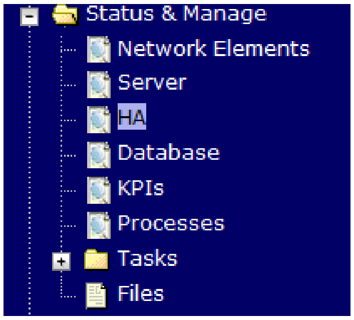
Procedure 2: Recovery Scenario 2

18 □	**NOAM VIP GUI:** Copy Configuration File to Failed NOAM Server	Obtain a terminal session to the NOAM VIP, login as the ***admusr*** user. Execute the following command to configure the failed NOAM server: **`$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<Faile_NOAM_Hostname>.sh admusr@<Failed_NOAM_control_IP_address>:/var/tmp/TKLCConfigData.sh`**
19 □	**Failed NOAM Server:** Verify the configuration was called and Reboot the Server	Establish an SSH session to the failed NOAM server, login as the ***admusr*** user. 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. Verify awpushcfg was called by checking the following file **`$ sudo cat /var/TKLC/appw/logs/Process/install.log`** Verify the following message is displayed: `[SUCCESS] script completed successfully!` Now Reboot the Server: **`$ sudo init 6`** Wait for the server to reboot

20
□
	Failed NOAM Server: Configure Networking for Dedicated NetBackup Interface (Optional)	**Note:** You will only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.
		Obtain a terminal window to the failed NOAM server, logging in as the ***admusr***.
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup`
		`--type=Ethernet --onboot=yes`
		`--address=<NO2_NetBackup_IP_Adress>`
		`--netmask=<NO2_NetBackup_NetMask>`
		`$ 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>`

Procedure 2: Recovery Scenario 2

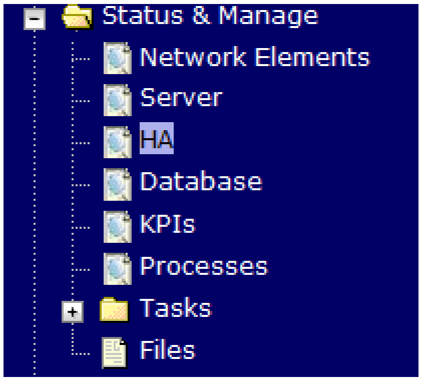
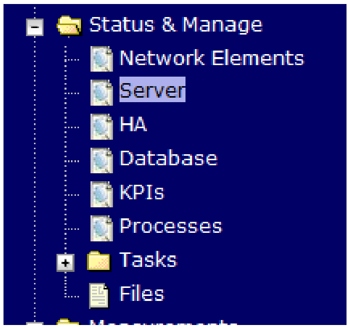
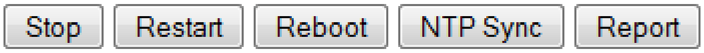
21
□
	Failed NOAM Server: Verify Server Health	Execute the following command on the 2nd NOAM server and make sure that no errors are returned:
		`$ sudo syscheck`
		`Running modules in class hardware...OK`
		`Running modules in class disk...OK`
		`Running modules in class net...OK`
		`Running modules in class system...OK`
		`Running modules in class proc...OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

22 □	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered standby NOAM server and click on **Restart**. 
23 □	**NOAM VIP GUI:** Set HA on Standby NOAM	Navigate to **Status & Manage -> HA**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click on **Edit** at the bottom of the screen Select the standby NOAM server, set it to **Active** Press **OK**

Procedure 2: Recovery Scenario 2

24 □	**NOAM VIP GUI:** Stop Replication to the C-Level Servers of this Site.	STOP ***!!!*** ***!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Warning !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!*** ***!!!*** Prior to continuing this procedure, replication to C Level servers at the SOAM site being recovered ***MUST*** be inhibited. **Failure to inhibit replication to the working c-level servers will result in their database being destroyed!** Execute **Appendix E**: Inhibit A and B Level Replication on C-Level Servers to inhibit replication to working C Level servers before continuing.
25 □	**Recover Active SOAM Server**	1. Execute procedure "Configure the SOAM Servers", steps 1-3, and 5-8 from reference [8]. **Note:** If you are using NetBackup, also execute step 10 2. If you are using NetBackup, execute procedure *"Install NetBackup Client"* from reference [8].

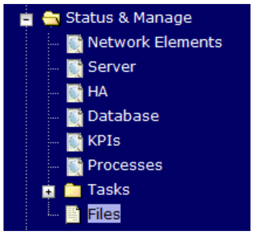
Procedure 2: Recovery Scenario 2

26 □	**NOAM VIP GUI:** Set HA on SOAM Server	Navigate to **Status & Manage -> HA**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click on **Edit** at the bottom of the screen Select the SOAM server, set it to **Active** Press **OK**
27 □	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered SOAM server and click on **Restart**. 

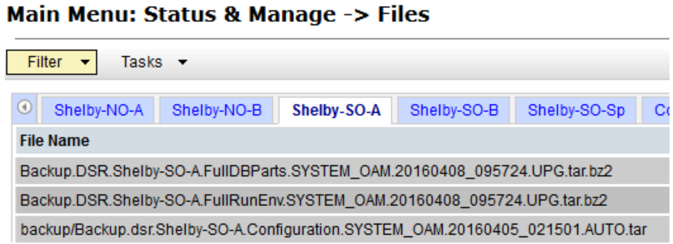
28 □

NOAM VIP GUI: Upload the backed up SOAM Database file

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

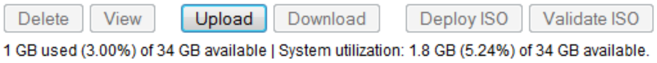


Select the Active SOAM server. The following screen will appear:


Main Menu: Status & Manage -> Files

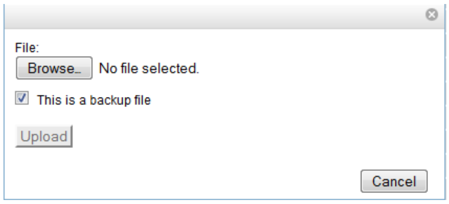
File Name
Backup.DSR.Shelby-SO-A.FullDBParts.SYSTEM_OAM.20160408_095724.UPG.tar.bz2
Backup.DSR.Shelby-SO-A.FullRunEnv.SYSTEM_OAM.20160408_095724.UPG.tar.bz2
backup/Backup.dsr.Shelby-SO-A.Configuration.SYSTEM_OAM.20160405_021501.AUTO.tar

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



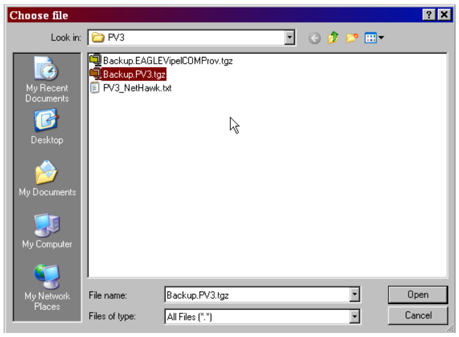
1 GB used (3.00%) of 34 GB available | System utilization: 1.8 GB (5.24%) of 34 GB available.

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


File:

Browse... No file selected.

☑ This is a backup file

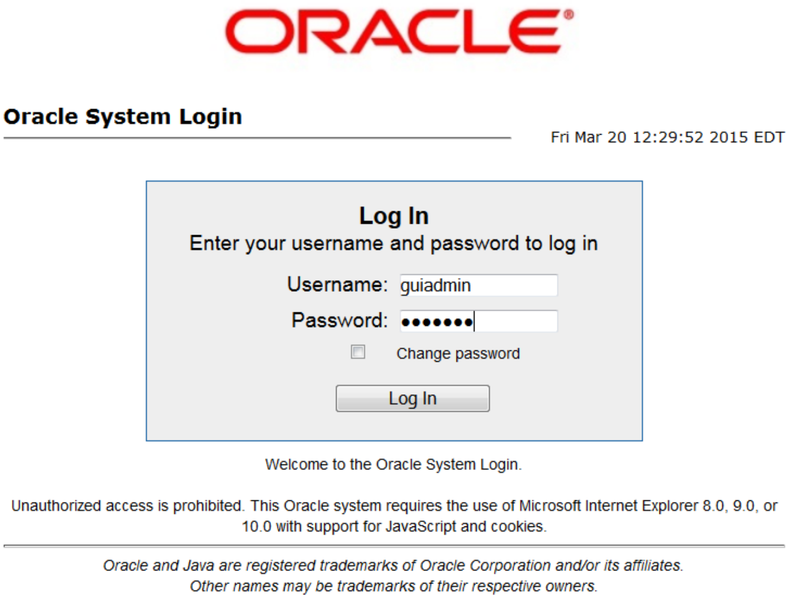


File name: Backup.PV3.tgz

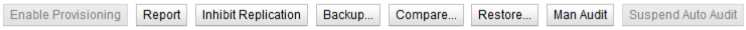
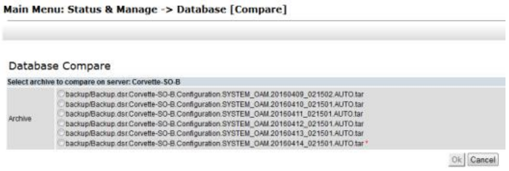
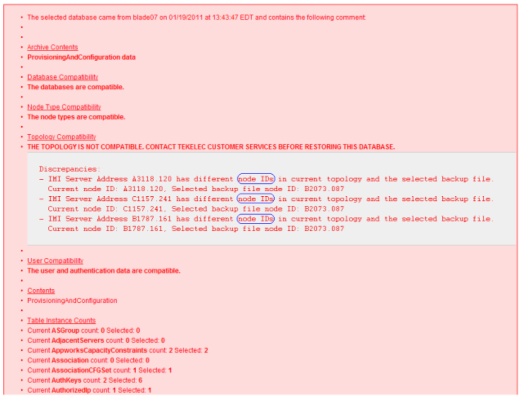
Files of type: All Files (*.*)

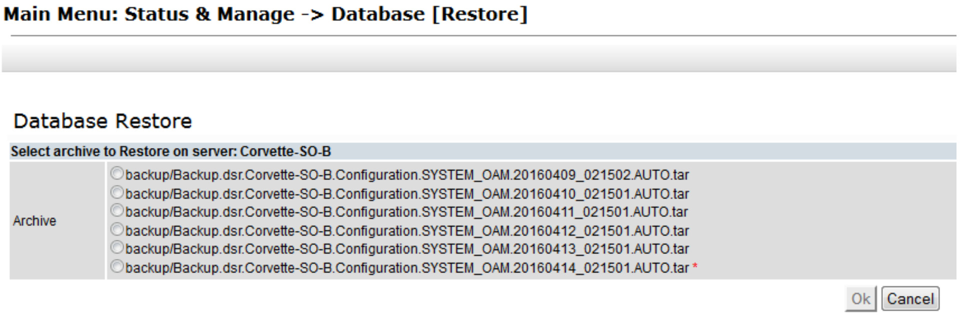
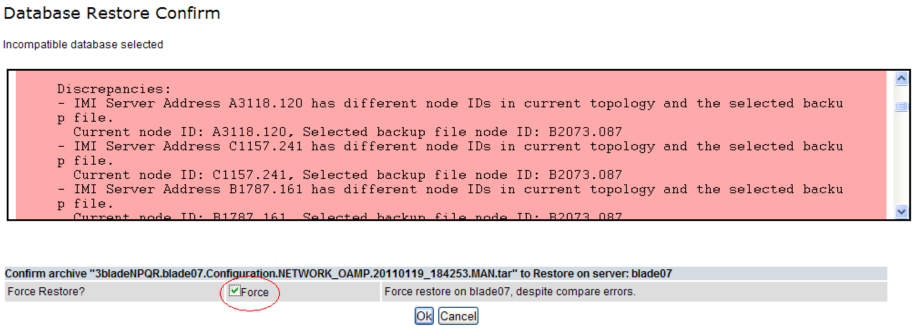
Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.

Procedure 2: Recovery Scenario 2

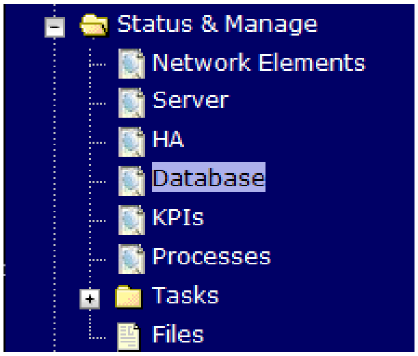
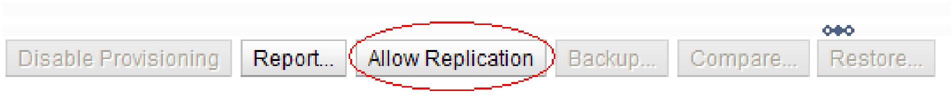
29 □	**Recovered SOAM GUI:** Login	Establish a GUI session on the recovered SOAM server. Open the web browser and enter a URL of: `http://<Recovered_SOAM_IP_Address>` Login as the ***guiadmin*** user:  **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.* *Other names may be trademarks of their respective owners.*

Procedure 2: Recovery Scenario 2

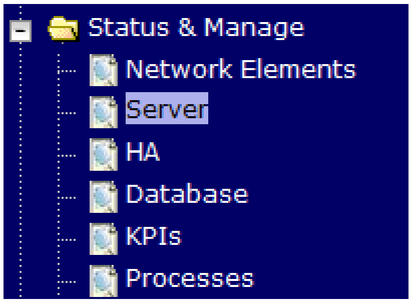
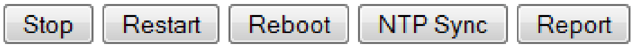
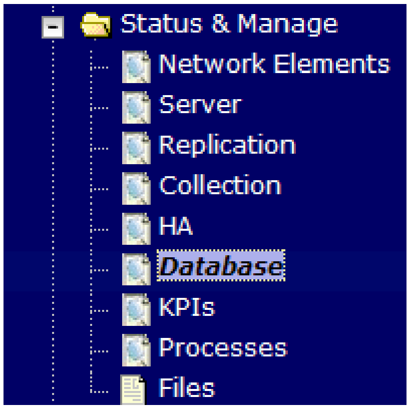
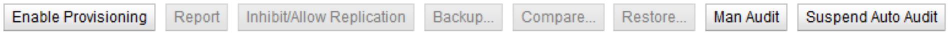
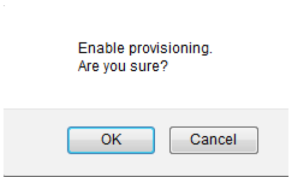
30 □	**Recovered SOAM GUI:** Verify the Archive Contents and Database Compatibility	Click on **Main Menu->Status & Manage->Database** Select the **Active SOAM** server and click on the **Compare**.  Enable Provisioning Report Inhibit Replication Backup... Compare... Restore... Man Audit Suspend Auto Audit 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.  Main Menu: Status & Manage -> Database [Compare] Database Compare Select archive to compare on server: Corvette-SO-B Archive ○ backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160409_021502.AUTO.tar ○ backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160410_021501.AUTO.tar ○ backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160411_021501.AUTO.tar ○ backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160412_021501.AUTO.tar ○ backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160413_021501.AUTO.tar ○ backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160414_021501.AUTO.tar * Ok Cancel **Verify** that the output window matches the screen below. **Note:** You will get a database mismatch regarding the NodeIDs of the blades. That is expected. If that is the only mismatch, proceed, otherwise stop and contact **Appendix L: My Oracle** Support (MOS)  • The selected database came from blade07 on 01/19/2011 at 13:43:47 EDT and contains the following comment: • • • Archive Contents • ProvisioningAndConfiguration data • • Database Compatibility • The databases are compatible. • • Node Type Compatibility • The node types are compatible. • • Topology Compatibility • THE TOPOLOGY IS NOT COMPATIBLE. CONTACT TEKELEC CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE. Discrepancies: - IMI Server Address A3118.120 has different node IDs in current topology and the selected backup file. Current node ID: A3118.120, Selected backup file node ID: B2073.087 - IMI Server Address C1157.241 has different node IDs in current topology and the selected backup file. Current node ID: C1157.241, Selected backup file node ID: B2073.087 - IMI Server Address B1787.161 has different node IDs in current topology and the selected backup file. Current node ID: B1787.161, Selected backup file node ID: B2073.087 • • User Compatibility • The user and authentication data are compatible. • • Contents • ProvisioningAndConfiguration • • Table Instance Counts • Current ASGroup count: 0 Selected: 0 • Current AdjacentServers count: 0 Selected: 0 • Current AppworksCapacityConstraints count: 2 Selected: 2 • Current Association count: 0 Selected: 0 • Current AssociationCFGSet count: 1 Selected: 1 • Current AuthKeys count: 2 Selected: 6 • Current AuthorizedIp count: 1 Selected: 1 **Note:** Archive Contents and Database Compatibilities must be the following: **Archive Contents:** Configuration data **Database Compatibility:** The databases are compatible. **Note:** The following is expected Output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. **Note:** We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility. If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.

31
□
	Recovered SOAM GUI: Restore the Database	Select the **Active SOAM** server, and click on **Restore** as shown below.
		
		The following screen will be displayed. Select the proper back up provisioning and configuration file.
		
		Main Menu: Status & Manage -> Database [Restore]
		Database Restore
		Select archive to Restore on server: Corvette-SO-B
		Archive
		○backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160409_021502.AUTO.tar
		○backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160410_021501.AUTO.tar
		○backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160411_021501.AUTO.tar
		○backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160412_021501.AUTO.tar
		○backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160413_021501.AUTO.tar
		○backup/Backup.dsr.Corvette-SO-B.Configuration.SYSTEM_OAM.20160414_021501.AUTO.tar *
		
		Click **OK** Button. The following confirmation screen will be displayed.
		
		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.
		
		Database Restore Confirm
		Incompatible database selected
		`Discrepancies:`
		`- IMI Server Address A3118.120 has different node IDs in current topology and the selected backu`
		`p file.`
		`  Current node ID: A3118.120, Selected backup file node ID: B2073.087`
		`- IMI Server Address C1157.241 has different node IDs in current topology and the selected backu`
		`p file.`
		`  Current node ID: C1157.241, Selected backup file node ID: B2073.087`
		`- IMI Server Address B1787.161 has different node IDs in current topology and the selected backu`
		`p file.`
		`  Current node ID: B1787.161, Selected backup file node ID: B2073.087`
		Confirm archive "3bladeNPQR.blade07.Configuration.NETWORK_OAMP.20110119_184253.MAN.tar" to Restore on server: blade07
		Force Restore? ☑Force Force restore on blade07, despite compare errors.
		
		Note: After the restore has started, the user will be logged out of XMI SOAM GUI since the restored Topology is old data.

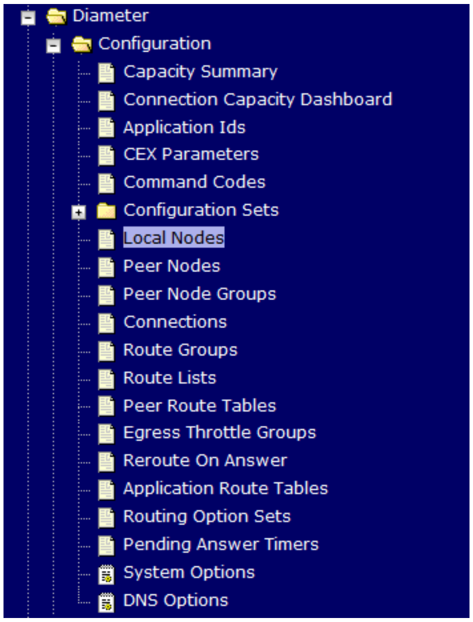
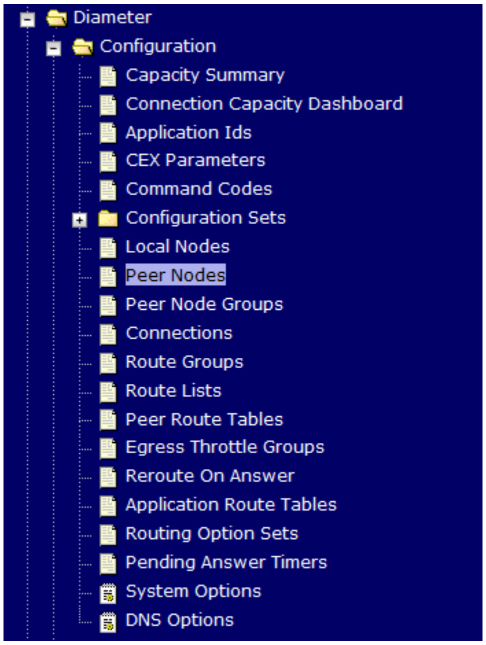
32 □	**Recovered SOAM GUI**: Monitor and Confirm database restoral	Wait for **5-10 minutes** for the System to stabilize with the new topology: Monitor the Info tab for **"Success"**. This will indicate that the restore is complete and the system is stabilized. **Note:** Do not pay attention to alarms until all the servers in the system are completely restored. **Note:** The Configuration and Maintenance information will be in the same state it was backed up during initial backup.

33 □	**NOAM VIP GUI:** Recover the Remaining SOAM Servers	Recover the **remaining** SOAM servers (**standby, spare**) by repeating the **following steps** for each SOAM server: 1. Execute procedure "Configure the SOAM Servers", steps 1-3, and 5-8 from reference [8]. **Note:** If you are using NetBackup, also execute step 10 2. If you are using NetBackup, execute procedure *"Install NetBackup Client"* from reference [8].
34 □	**NOAM VIP GUI:** Start replication on the recovered SOAMs	Un-Inhibit *(Start)* Replication to the remaining recovered SOAM servers Navigate to **Status & Manage -> Database**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click on the Allow Replication button as shown below on the remaining recovered SOAM servers. Verify that the replication on all servers is allowed. This can be done by clicking on each server and checking that the button below shows "Inhibit Replication", and **NOT** "Allow Replication".  Disable Provisioning Report... Allow Replication Backup... Compare... Restore...

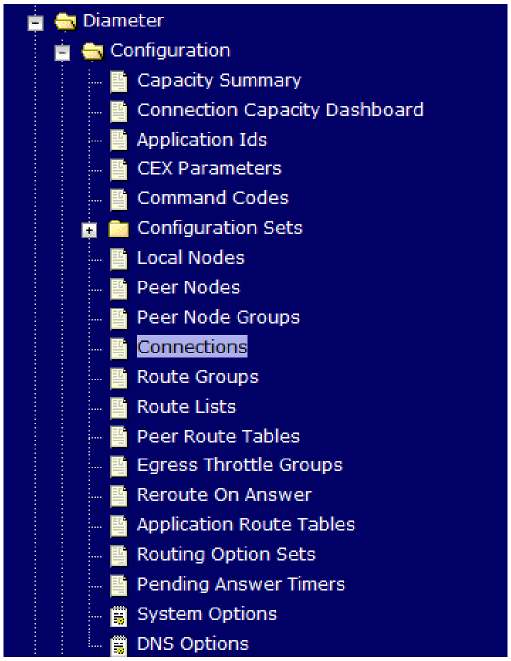
Procedure 2: Recovery Scenario 2

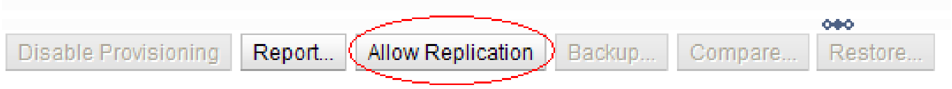
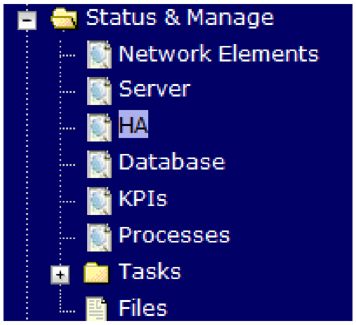
35 □	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Status & Manage Network Elements Server HA Database KPIs Processes Select the remaining recovered SOAM servers and click on **Restart**. 
36 □	**SOAM GUI:** Enable Provisioning	Click on **Main Menu->Status & Manage->Database**  Status & Manage Network Elements Server Replication Collection HA Database KPIs Processes Files Enable Provisioning by clicking on **Enable Provisioning** button at the bottom of the screen as shown below.  Enable Provisioning Report Inhibit/Allow Replication Backup... Compare... Restore... Man Audit Suspend Auto Audit A confirmation window will appear, press **OK** to enable Provisioning.  Enable provisioning. Are you sure?

Procedure 2: Recovery Scenario 2

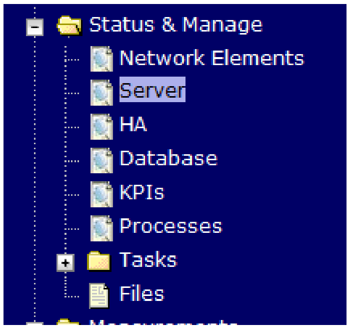
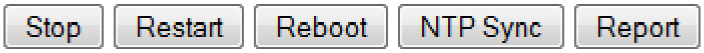
37 □	**SOAM VIP GUI:** Verify the Local Node Info	Navigate to **Main Menu->Diameter->Configuration->Local Node**  Diameter Configuration Capacity Summary Connection Capacity Dashboard Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes Peer Node Groups Connections Route Groups Route Lists Peer Route Tables Egress Throttle Groups Reroute On Answer Application Route Tables Routing Option Sets Pending Answer Timers System Options DNS Options Verify that all the local nodes are shown.
38 □	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Diameter Configuration Capacity Summary Connection Capacity Dashboard Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes Peer Node Groups Connections Route Groups Route Lists Peer Route Tables Egress Throttle Groups Reroute On Answer Application Route Tables Routing Option Sets Pending Answer Timers System Options DNS Options Verify that all the peer nodes are shown.

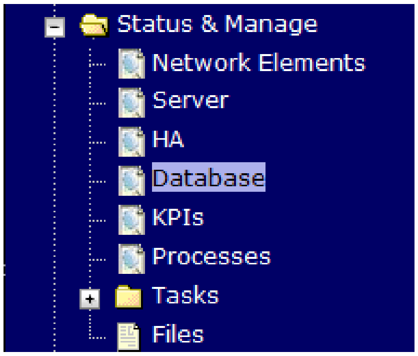
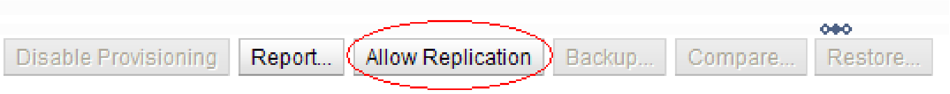
Procedure 2: Recovery Scenario 2

39 □	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections**  Diameter Configuration Capacity Summary Connection Capacity Dashboard Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes Peer Node Groups Connections Route Groups Route Lists Peer Route Tables Egress Throttle Groups Reroute On Answer Application Route Tables Routing Option Sets Pending Answer Timers System Options DNS Options Verify that all the connections are shown.

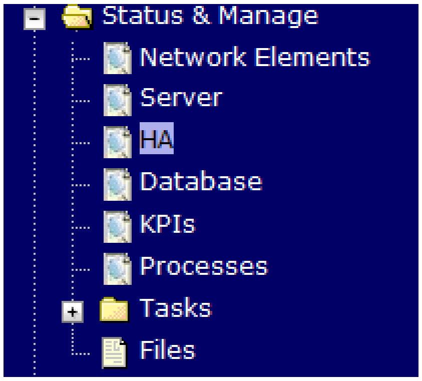
40 □	**NOAM VIP GUI:** Start Replication on working C-Level Servers	Un-Inhibit *(Start)* Replication to the **working** C-Level Servers which belong to the same site as of the failed SOAM servers. Execute **Appendix F**: Un-Inhibit A and B Level Replication on C-Level Servers If the *"Repl Status"* is set to "Inhibited", click on the **Allow Replication** button as shown below using the following order, otherwise if none of the servers are inhibited, skip this step and continue with the next step: • Active NOAM Server • Standby NOAM Server • Active SOAM Server • Standby SOAM Server • Spare SOAM Server *(if applicable)* • Active DR NOAM Server • Standby DR NOAM Server • MP/IPFE Servers *(if MPs are configured as Active/Standby, start with the Active MP, otherwise the order of the MPs does not matter)* • SBRS *(if SBR servers are configured, start with the active SBR, then standby, then spare)* Verify that the replication on all the working servers is allowed. This can be done by clicking on each server and checking that the button below shows "Inhibit Replication", and **NOT** "Allow Replication".  Disable Provisioning Report... Allow Replication Backup... Compare... Restore...
41 □	**NOAM VIP GUI:** Set HA on SOAM Servers	Navigate to **Status & Manage -> HA**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click on **Edit** at the bottom of the screen For each SOAM server whose Max Allowed HA Role is set to Standby, set it to **Active** Press **OK**

Procedure 2: Recovery Scenario 2

42 □	**(PCA Only) Activate PCA Feature**	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. **Note:** If not all SOAM sites are ready at this point, then you should repeat activation for each *new* SOAM site that comes online.
43 □	**NOAM VIP GUI:** Recover the C-Level Server (DA-MP, SBRs, IPFE, SS7-MP)	Execute procedure *“Configure MP Blade Servers”*, Steps 1, 7, 11-14, and 17 from reference [8]. **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. Repeat this step for any remaining failed MP servers.
44 □	**NOAM VIP GUI:** Restart DSR Application on recovered C-Level Servers.	Navigate to **Main Menu->Status & Manage->Server**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered C-Level servers and click on **Restart**. 

45 □	**NOAM VIP GUI:** Start replication on ALL C-Level Servers	Un-Inhibit *(Start)* Replication to the **ALL** C-Level Servers Navigate to **Status & Manage -> Database**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files If the *"Repl Status"* is set to "Inhibited", click on the Allow Replication button as shown below using the following order: • Active NOAMP Server • Standby NOAMP Server • Active SOAM Server • Standby SOAM Server • Spare SOAM Server *(if applicable)* • Active DR NOAM Server • Standby DR NOAM Server • MP/IPFE Servers *(if MPs are configured as Active/Standby, start with the Active MP, otherwise the order of the MPs does not matter)* Verify that the replication on all servers is allowed. This can be done by clicking on each server and checking that the button below shows "Inhibit Replication", and **NOT** "Allow Replication".  Disable Provisioning Report... Allow Replication Backup... Compare... Restore...

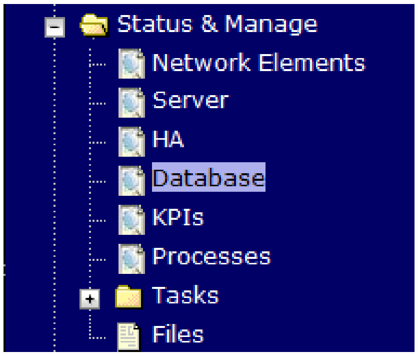
Procedure 2: Recovery Scenario 2

46 □	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click on **Edit** at the bottom of the screen For each server whose Max Allowed HA Role is set to Standby, set it to **Active** Press **OK**
47 □	**ACTIVE NOAM:** Perform key exchange between the active-NOAM and recovered servers.	Establish an SSH session to the Active NOAM, login as ***admusr.*** Execute the following command to perform a keyexchange from the active NOAM to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>`
48 □	**ACTIVE NOAM:** Activate Optional Features	Establish an SSH session to the active NOAM, login as ***admusr.*** Refer to **section** 1.5 Optional Features to activate any features that were previously activated. **Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: *`iload#31000{S/W Fault}`*

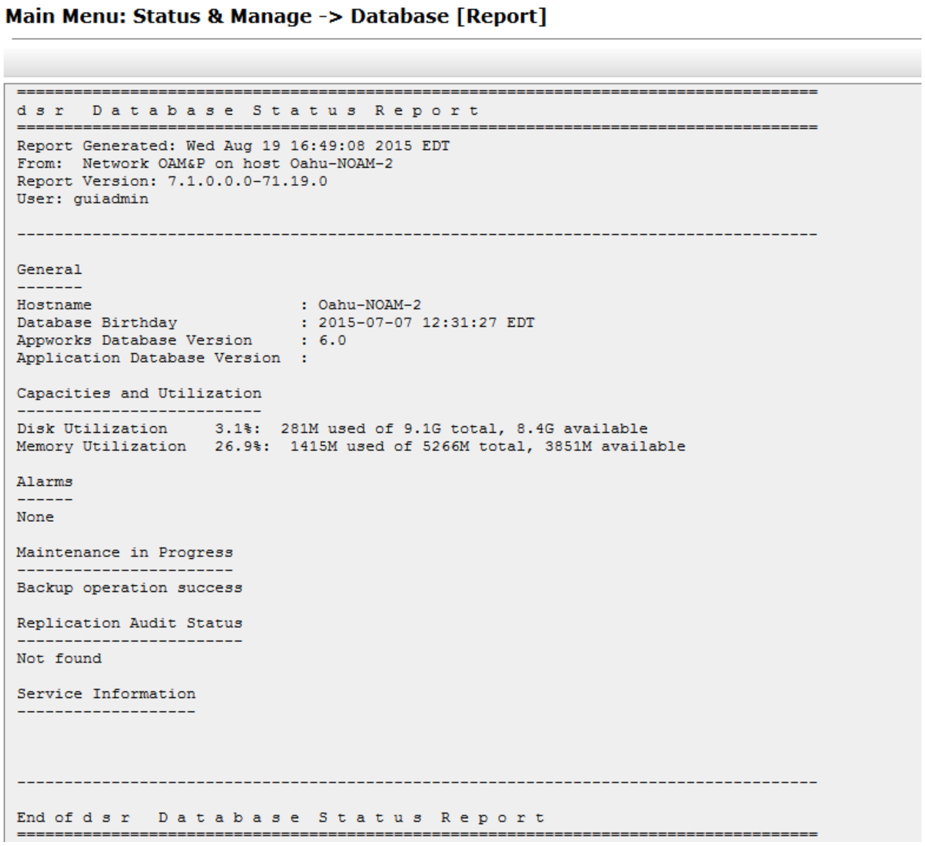
49 □

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]

```
=====================================================================================
d s r   D a t a b a s e   S t a t u s   R e p o r t
=====================================================================================
Report Generated: Wed Aug 19 16:49:08 2015 EDT
From:  Network OAM&P on host Oahu-NOAM-2
Report Version: 7.1.0.0.0-71.19.0
User: guiadmin

-------------------------------------------------------------------------------------


General
-------
Hostname                      : Oahu-NOAM-2
Database Birthday             : 2015-07-07 12:31:27 EDT
Appworks Database Version     : 6.0
Application Database Version  :

Capacities and Utilization
--------------------------
Disk Utilization     3.1%:  281M used of 9.1G total, 8.4G available
Memory Utilization   26.9%:  1415M used of 5266M total, 3851M available

Alarms
------
None

Maintenance in Progress
-----------------------
Backup operation success

Replication Audit Status
------------------------
Not found

Service Information
-------------------



-------------------------------------------------------------------------------------


End of d s r   D a t a b a s e   S t a t u s   R e p o r t
=====================================================================================
```

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

Procedure 2: Recovery Scenario 2

50

□

ACTIVE NOAM: Verify Replication Between Servers.

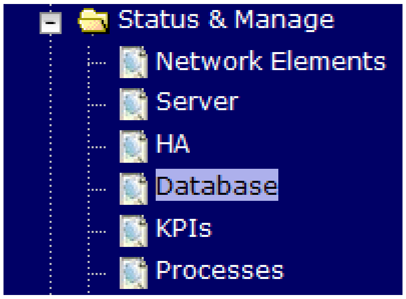
Login to the Active NOAM via SSH terminal as ***admusr***user.
Execute the following command:

```
$ sudo irepstat –m
```

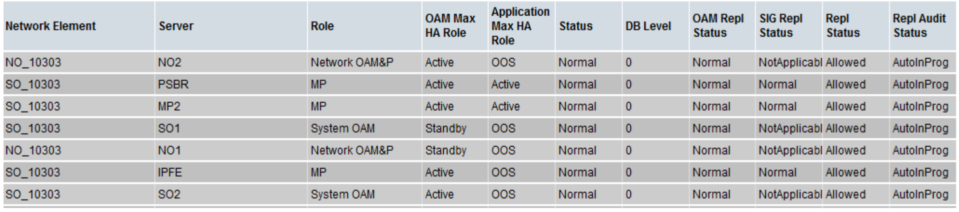
Output like below shall be generated:

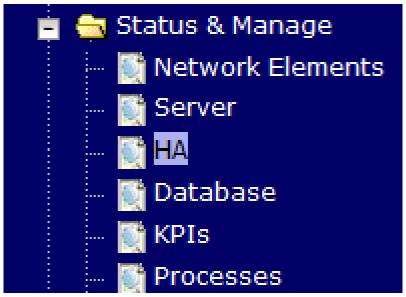
```
-- Policy 0 ActStb [DbReplication] -----------------------------------
----------
Oahu-DAMP-1 -- Active
  BC From Oahu-SOAM-2  Active      0   0.50 ^0.15%cpu 25B/s  A=me
  CC To   Oahu-DAMP-2  Active      0   0.10  0.14%cpu 25B/s  A=me
Oahu-DAMP-2 -- Stby
  BC From Oahu-SOAM-2  Active      0   0.50 ^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
```

<table>
<tr>
<td>51
□</td>
<td><b>NOAM VIP GUI:</b> Verify the Database states</td>
<td>
Click on <b>Main Menu->Status and Manager->Database</b>

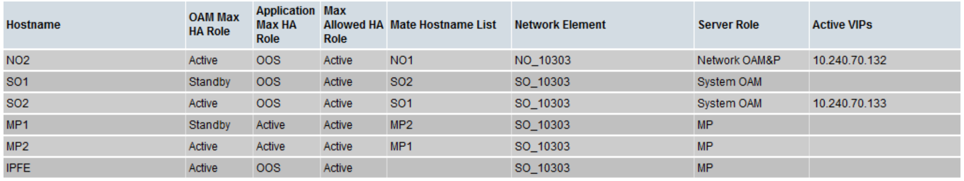


Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below:

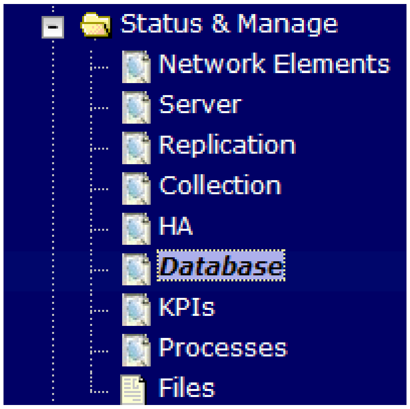
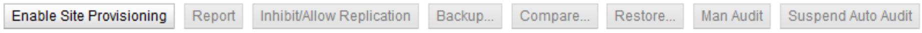
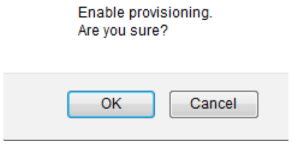
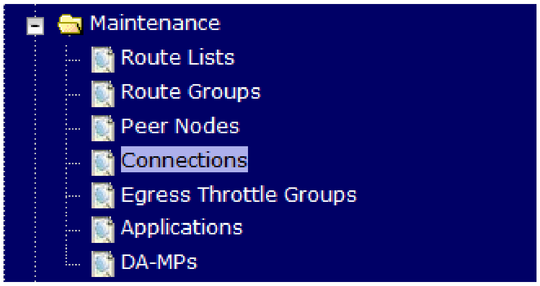
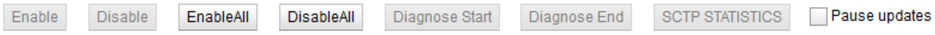

<table>
<tr><th>Network Element</th><th>Server</th><th>Role</th><th>OAM Max HA Role</th><th>Application Max HA Role</th><th>Status</th><th>DB Level</th><th>OAM Repl Status</th><th>SIG Repl Status</th><th>Repl Status</th><th>Repl Audit Status</th></tr>
<tr><td>NO_10303</td><td>NO2</td><td>Network OAM&P</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>IPFE</td><td>MP</td><td>Active</td><td>OOS</td><td>Normal</td><td>0</td><td>Normal</td><td>Normal</td><td>Allowed</td><td>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>
</table>
</td>
</tr>
<tr>
<td>52
□</td>
<td><b>NOAM VIP GUI:</b> Verify the HA Status</td>
<td>
Click on <b>Main Menu->Status and Manage-&gt;HA</b>

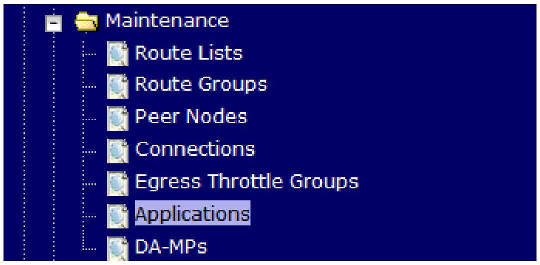
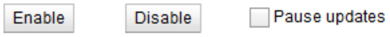
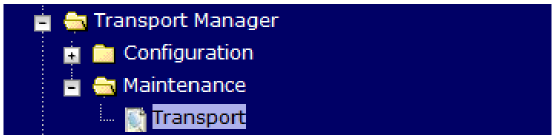
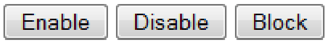
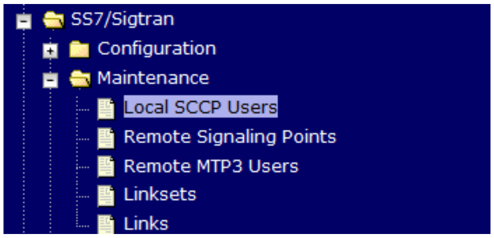
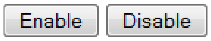


Select the row for all of the servers
Verify that the “HA Role” is either “Active” or “Standby”.

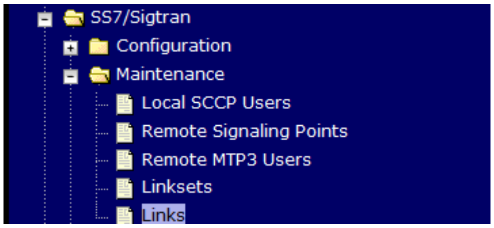
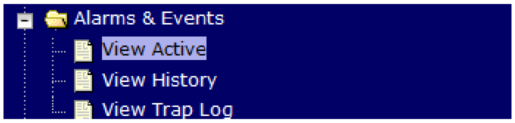
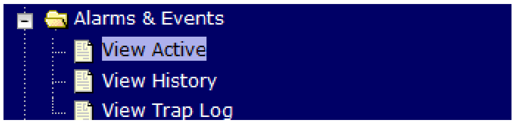

<table>
<tr><th>Hostname</th><th>OAM Max HA Role</th><th>Application Max HA Role</th><th>Max Allowed HA Role</th><th>Mate Hostname List</th><th>Network Element</th><th>Server Role</th><th>Active VIPs</th></tr>
<tr><td>NO2</td><td>Active</td><td>OOS</td><td>Active</td><td>NO1</td><td>NO_10303</td><td>Network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

Procedure 2: Recovery Scenario 2

53 □	**SOAM GUI:** Enable Site Provisioning	Click on **Main Menu->Status & Manage->Database**  Status & Manage Network Elements Server Replication Collection HA Database KPIs Processes Files Enable Site Provisioning by clicking on **Enable Site Provisioning** button at the bottom of the screen as shown below.  Enable Site Provisioning Report Inhibit/Allow Replication Backup... Compare... Restore... Man Audit Suspend Auto Audit A confirmation window will appear, press **OK** to enable Provisioning.  Enable provisioning. Are you sure?
54 □	**MP Servers:** Disable SCTP Auth Flag	For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [14] Execute this procedure on all Failed MP Servers.
55 □	**SOAM VIP GUI:** Enable Connections if needed	Navigate to **Main Menu->Diameter->Maintenance->Connections**  Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups Applications DA-MPs Select each connection and click on the **Enable** button. Alternatively you can enable all the connections by selecting the **EnableAll** button.  Enable Disable EnableAll DisableAll Diagnose Start Diagnose End SCTP STATISTICS Pause updates Verify that the Operational State is Available.

56 □	**SOAM VIP GUI:** Enable Optional Features	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups Applications DA-MPs Select the optional feature application configured in **step 29**. Click the **Enable** button. 
57 □	**SOAM VIP GUI:** Re-enable Transports if Needed	Navigate to **Main Menu->Transport Manager -> Maintenance -> Transport**  Transport Manager Configuration Maintenance Transport Select each transport and click on the **Enable** button  Verify that the Operational Status for each transport is Up.
58 □	**SOAM VIP GUI:** Re-enable MAPIWF application if needed	Navigate to **Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users**  SS7/Sigtran Configuration Maintenance Local SCCP Users Remote Signaling Points Remote MTP3 Users Linksets Links Click on the **Enable** button corresponding to MAPIWF Application Name.  Verify that the SSN Status is Enabled.

Procedure 2: Recovery Scenario 2

59 □	**SOAM VIP GUI:** Re-enable links if needed	Navigate to **Main Menu->SS7/Sigtran->Maintenance->Links**  SS7/Sigtran Configuration Maintenance Local SCCP Users Remote Signaling Points Remote MTP3 Users Linksets Links Click on **Enable** button for each link. Verify that the Operational Status for each link is Up.
60 □	**SOAM VIP GUI:** Examine All Alarms	Navigate to **Main Menu->Alarms & Events->View Active**  Alarms & Events View Active View History View Trap Log Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix L: My Oracle** Support (MOS).
61 □	**NOAM VIP GUI:** Examine All Alarms	Login to the NOAM VIP if not already logged in. Navigate to **Main Menu->Alarms & Events->View Active**  Alarms & Events View Active View History View Trap Log Examine all active alarms and refer to the on-line help on how to address them.

<table>
<tr>
<td>62
□</td>
<td><b>NOAM VIP:</b> Verify all servers in Topology are accessible (RADIUS Only)</td>
<td>

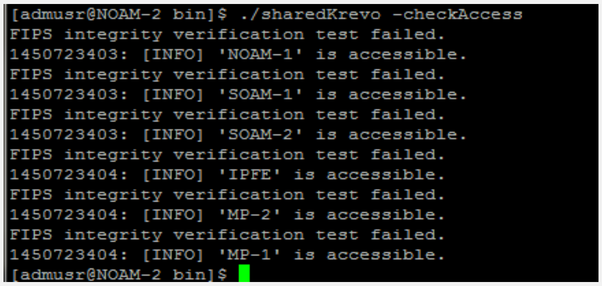
If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)

Establish an SSH session to the NOAM VIP. Login as ***admusr.***

Execute following commands to check if all the servers in the Topology are accessible :

```
$ cd /usr/TKLC/dpi/bin/
$ ./sharedKrevo -checkAccess
```

Example Output:



```
[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]$
```

</td>
</tr>
</table>

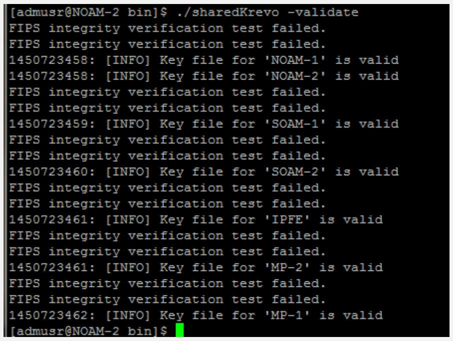
Procedure 2: Recovery Scenario 2

<table>
<tr>
<td>63
□</td>
<td><b>NOAM VIP:</b> Copy key file to all the servers in Topology (RADIUS Only)</td>
<td>

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 :

```
$ cd /usr/TKLC/dpi/bin/
$ ./sharedKrevo -validate
```

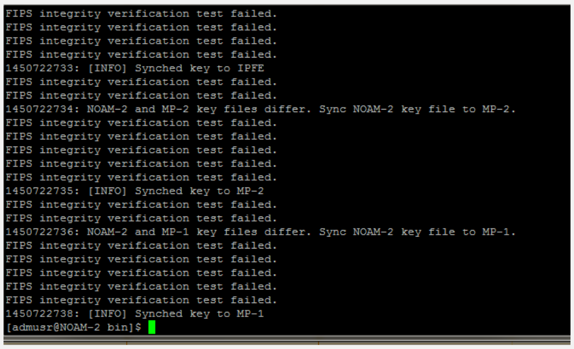


```
[admusr@NOAM-2 bin]$ ./sharedKrevo -validate
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723458: [INFO] Key file for 'NOAM-1' is valid
1450723458: [INFO] Key file for 'NOAM-2' is valid
FIPS integrity verification test failed.
FIPS integrity verification test 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
[admusr@NOAM-2 bin]$
```

If output of above command shows that the existing key file is not valid, contact **Appendix L: My Oracle** Support (MOS)

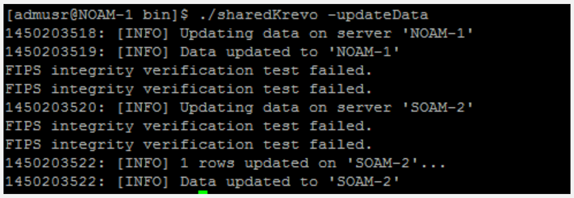
Execute following command to copy the key file to all the servers in the Topology:

```
$ ./sharedKrevo -synchronize
```



```
FIPS integrity verification test failed.
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.
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.
FIPS integrity verification test failed.
1450722738: [INFO] Synched key to MP-1
[admusr@NOAM-2 bin]$
```

```
$ ./sharedKrevo -updateData
```



```
[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'
```

Note: If any errors are present, stop and contact Appendix L: My Oracle Support (MOS)

</td>
</tr>
</table>

Procedure 2: Recovery Scenario 2

64 □	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**: DSR Database Backup to back up the Configuration databases:
65 □	**Recover IDIH**	If IDIH were affected, refer to **Section 11** 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 #	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). 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 □	**Workarounds**	Refer to **Appendix G**: Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
2 □	**Gather Required Materials**	Gather the documents and required materials listed in **Section 3.1** Required Materials
3 □	**Replace Failed Equipment**	HW vendor to replace the failed equipment
4 □	**RMS NOAM Failure:** Configure BIOS Settings and Update Firmware	If the failed server is **NOT** a rack mount server, **skip to step 7.** 1. Configure and verify the BIOS settings by executing procedure *"Configure the RMS Server BIOS Settings"* from reference [10] 2. Verify and/or upgrade server firmware by executing procedure *"Upgrade Management Server Firmware"* from reference[10] **Note:** Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.
5 □	**RMS NOAM Failure:** Backups Available	If the failed server is **NOT** a rack mount server, **skip to step 7.** This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, **skip this step**. 1. Restore the TVOE backup by executing Appendix H: Restore TVOE Configuration from Backup Media If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing 2. Appendix I: Restore PMAC from Backup

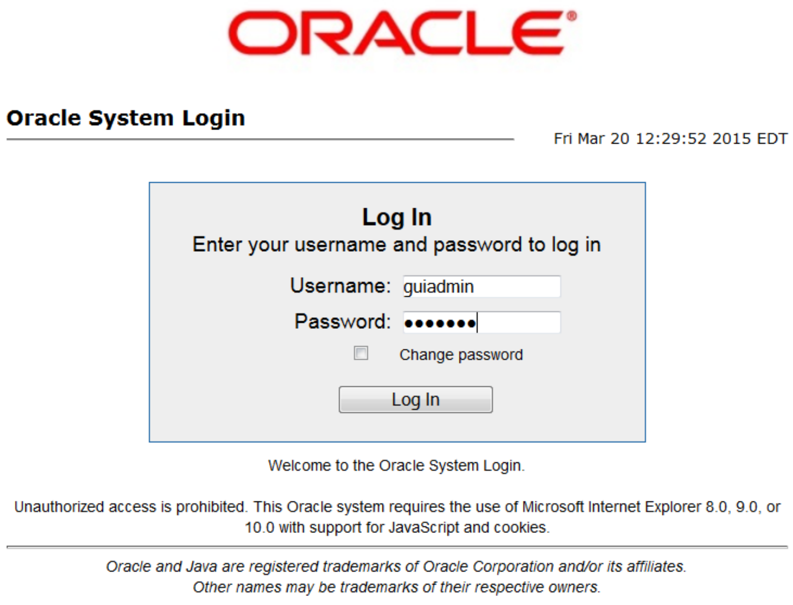
Procedure 3: Recovery Scenario 3

6 □	**Recover Failed Aggregation/ Enclosure Switches, and OAs**	Recover failed OAs, aggregation and enclosure switches if needed. Backups Available: 1. Refer to Appendix B: Recovering/Replacing Failed 3rd Party Components (Switches, OAs)to recover failed OAs, aggregation, and enclosure switches Backups **NOT** Available: 1. Execute section *“HP C-7000 Enclosure Configuration”* 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.
7 □	**RMS NOAM Failure:** Backups **NOT** Available	If the failed server is **NOT** a rack mount server, **skip to step 7.** This step assumes that TVOE and PMAC backups **NOT** are available, if the TVOE and PMAC have already been restored, **skip this step.** If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. Section *“Configure and IPM Management Server”* from reference [10]. 2. Section *“Install PM&C”* from reference [10]. 3. Section *“Configure PM&C”* from reference [10]. If the PMAC is **NOT** located on the same TVOE host as the failed NOAM, Execute the following sections/procedures 1. Section *“Installing TVOE on Rack Mount Server(s)”* from reference [10].
8 □	**HP-Class Blade Failure:** Configure Blade Server iLO, Update Firmware/BIOS Settings	If the failed server is **NOT** an HP C-Class Blade, **skip to step 11.** 1. Execute procedure *“Configure Blade Server iLO Password for Administrator Account”* from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing section *“Server Blades Installation Preparation”* from reference [10]

Procedure 3: Recovery Scenario 3

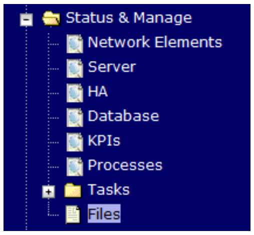
9 □	**HP-Class Blade Failure:** Backups Available	If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 11.** This step assumes that TVOE backups are available, if backups are **NOT** available, **skip this step**. 1. Install and configure TVOE on failed TVOE blade servers by executing section *"Install TVOE on Blade Servers"* 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.
10 □	**HP-Class Blade Failure:** Backups **NOT** Available	If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 11.** This step assumes that TVOE backups are **NOT** are available 1. Install and configure TVOE on failed TVOE blade servers by executing section *"Install TVOE on Blade Servers"* from reference [10].
11 □	**Execute Fast Deployment File for NOAMs**	The backup fdconfig file used during the initial DSR 7.2 installation, this file will be available on the PMAC if a database backup was restored on the PMAC. If a backup fast deployment xml is NOT available, execute procedure *"Configure NOAM Servers"* from reference [8]. If a backup fast deployment xml is already present on the PMAC, execute the following procedure: 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: **`$ cd /usr/TKLC/smac/etc`** **`$ screen`** **`$ sudo fdconfig config --file=<Created_FD_File>.xml`**
12 □	**Obtain Latest Database Backup and Network Configuration Data.**	Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. From required materials list in **Section 3.1** `Required Materials`; use site survey documents and Network Element report (if available), to determine network configuration data.

Procedure 3: Recovery Scenario 3

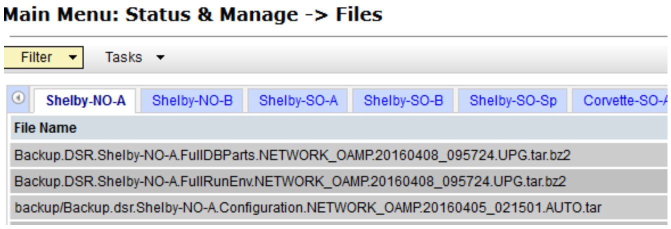
13 □	**Execute DSR Installation Procedure for the First NOAM**	1. Configure the first NOAM server by executing procedure *“Configure the First NOAM NE and Server”* from reference [8]. 2. Configure the NOAM server group by executing procedure *“Configure the NOAM Server Group”* from reference [8]. **Note:** Use the backup copy of network configuration data and site surveys (Step 2)
14 □	**NOAM GUI:** Login	Login to the NOAM GUI as the ***guiadmin*** user:  ORACLE **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*

15 □ **NOAM GUI:** Upload the Backed up Database File

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



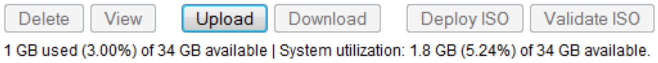
Select the Active NOAM server. The following screen will appear:



Main Menu: Status & Manage -> Files

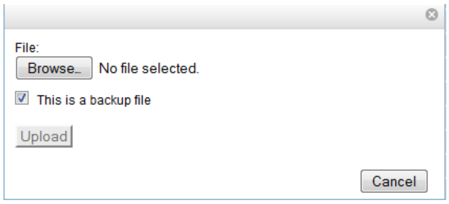
File Name
Backup.DSR.Shelby-NO-A.FullDBParts.NETWORK_OAMP.20160408_095724.UPG.tar.bz2
Backup.DSR.Shelby-NO-A.FullRunEnv.NETWORK_OAMP.20160408_095724.UPG.tar.bz2
backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160405_021501.AUTO.tar

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



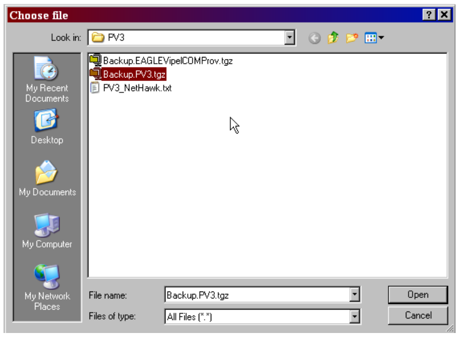
1 GB used (3.00%) of 34 GB available | System utilization: 1.8 GB (5.24%) of 34 GB available.

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



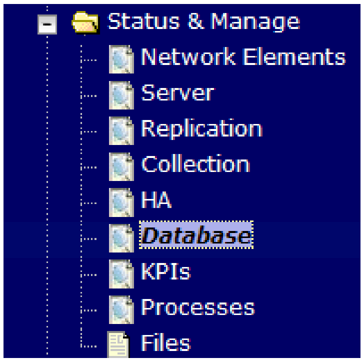
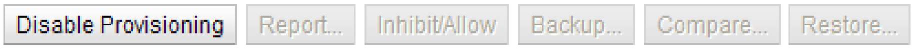
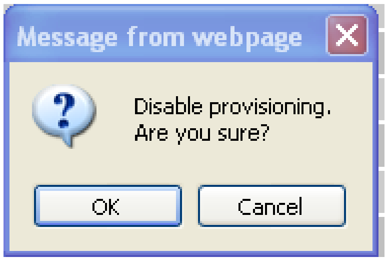
File:
Browse... No file selected.

☑ This is a backup file



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

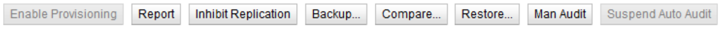
16 □	**NOAM GUI:** Disable Provisioning	Click on **Main Menu->Status & Manage->Database**  Status & Manage Network Elements Server Replication Collection HA Database KPIs Processes Files Disable Provisioning by clicking on **Disable Provisioning** button at the bottom of the screen as shown below.  Disable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

17

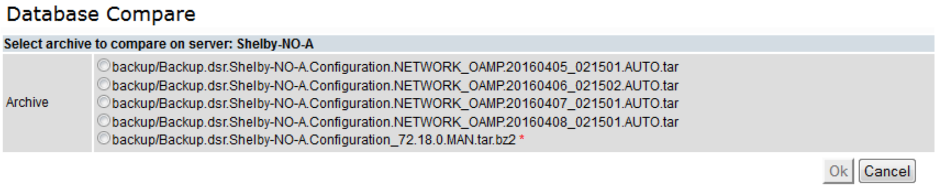
□

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.



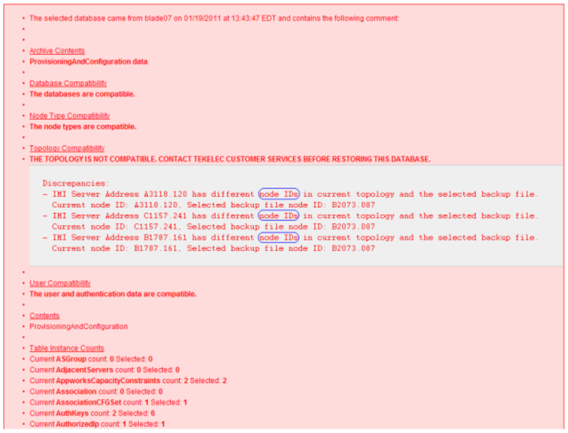
Database Compare

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

Archive
○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160405_021501.AUTO.tar
○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160406_021502.AUTO.tar
○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160407_021501.AUTO.tar
○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160408_021501.AUTO.tar
○ backup/Backup.dsr.Shelby-NO-A.Configuration_72.18.0.MAN.tar.bz2 *

Verify that the output window matches the screen below.

Note: You will get a Topology Compatability warnings. That is expected. If that is the only mismatch, proceed, otherwise stop and contact **Appendix L: My Oracle** Support (MOS)



- The selected database came from blade07 on 01/19/2011 at 13:43:47 EDT and contains the following comment:
-
-
- Archive Contents
- ProvisioningAndConfiguration data
-
- Database Compatibility
- The databases are compatible.
-
- Node Type Compatibility
- The node types are compatible.
-
- Topology Compatibility
- THE TOPOLOGY IS NOT COMPATIBLE. CONTACT TEKELEC CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE.

```
Discrepancies:
- IMI Server Address A3118.120 has different node IDs in current topology and the selected backup file.
  Current node ID: A3118.120, Selected backup file node ID: B2073.087
- IMI Server Address C1157.241 has different node IDs in current topology and the selected backup file.
  Current node ID: C1157.241, Selected backup file node ID: B2073.087
- IMI Server Address B1787.161 has different node IDs in current topology and the selected backup file.
  Current node ID: B1787.161, Selected backup file node ID: B2073.087
```

-
- User Compatibility
- The user and authentication data are compatible.
-
- Contents
- ProvisioningAndConfiguration
-
- Table Instance Counts
- Current **ASGroup** count: **0** Selected: **0**
- Current **AdjacentServers** count: **0** Selected: **0**
- Current **AppworksCapacityConstraints** count: **2** Selected: **2**
- Current **Association** count: **0** Selected: **0**
- Current **AssociationCFGSet** count: **1** Selected: **1**
- Current **AuthKeys** count: **2** Selected: **6**
- Current **AuthorizedIp** count: **1** Selected: **1**

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

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

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

Topology Compatibility
THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.

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

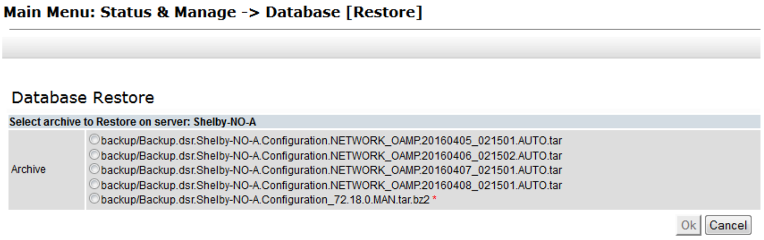
If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.

18 □

ACTIVE NOAM: Restore the Database

Select the **Active NOAM** server, and click on **Restore** as shown below.

The following screen will be displayed. Select the proper back up provisioning and configuration file.



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

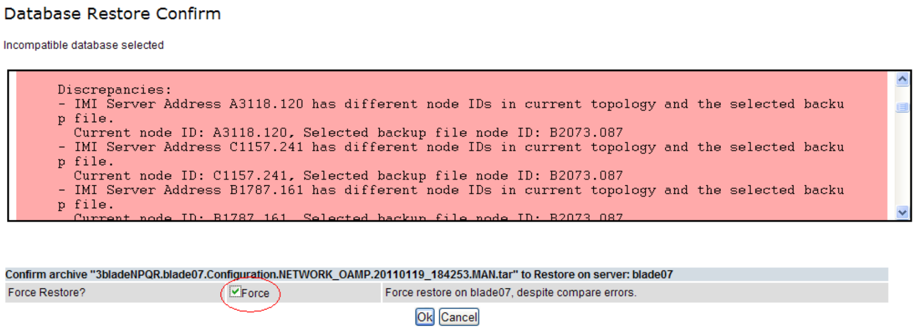
Database Restore

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

Archive	○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160405_021501.AUTO.tar ○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160406_021502.AUTO.tar ○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160407_021501.AUTO.tar ○ backup/Backup.dsr.Shelby-NO-A.Configuration.NETWORK_OAMP.20160408_021501.AUTO.tar ○ backup/Backup.dsr.Shelby-NO-A.Configuration_72.18.0.MAN.tar.bz2 *

Click **OK** Button. The following confirmation screen will be displayed.

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.



Database Restore Confirm

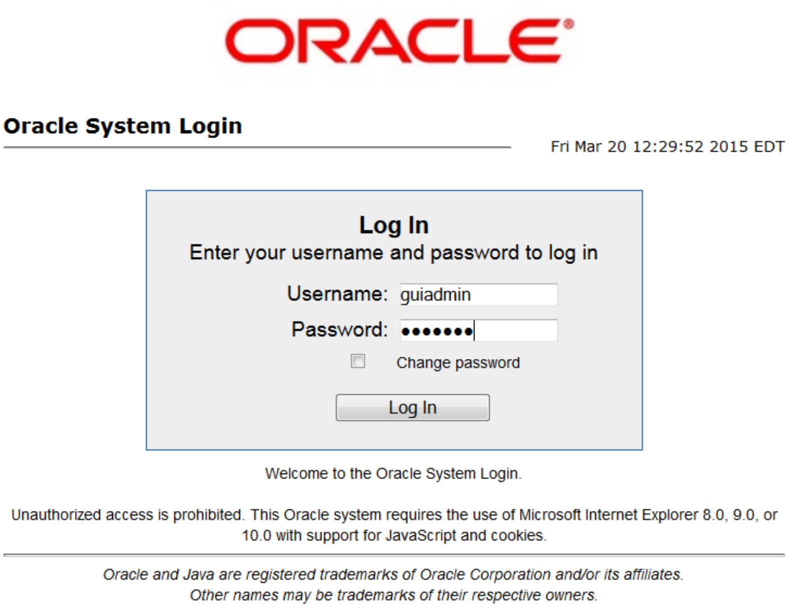
Incompatible database selected

```
Discrepancies:
- IMI Server Address A3118.120 has different node IDs in current topology and the selected backu
p file.
  Current node ID: A3118.120, Selected backup file node ID: B2073.087
- IMI Server Address C1157.241 has different node IDs in current topology and the selected backu
p file.
  Current node ID: C1157.241, Selected backup file node ID: B2073.087
- IMI Server Address B1787.161 has different node IDs in current topology and the selected backu
p file.
  Current node ID: B1787.161, Selected backup file node ID: B2073.087
```

Confirm archive "3bladeNPQR.blade07.Configuration.NETWORK_OAMP.20110119_184253.MAN.tar" to Restore on server: blade07

Force Restore?	☑ Force	Force restore on blade07, despite compare errors.

Note: After the restore has started, the user will be logged out of XMI NO GUI since the restored Topology is old data.

19 □	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:  **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ●●●●●●● □ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*
20 □	**NOAM VIP GUI:** Monitor and Confirm database restoral	Wait for **5-10 minutes** for the System to stabilize with the new topology: Monitor the Info tab for **"Success"**. This will indicate that the restore is complete and the system is stabilized. Following alarms **must** be ignored for NOAM and MP Servers until all the Servers are configured: Alarms with Type Column as **"REPL"** , **"COLL", "HA"** (with mate NOAM), **"DB"** (about Provisioning Manually Disabled) **Note:** Do not pay attention to alarms until all the servers in the system are completely restored. **Note:** The Configuration and Maintenance information will be in the same state it was backed up during initial backup.
21 □	**ACTIVE NOAM:** Login	Login to the recovered Active NOAM via SSH terminal as ***admusr*** user.

Procedure 3: Recovery Scenario 3

<table>
<tr><td>22
□</td><td><b>NOAM VIP GUI:</b> Recover Standby NOAM</td><td>

Install the second NOAM server by executing procedure *“Configure the Second NOAM Server”,* steps 3-5, 7 from reference [8].

Note: Execute step 6 if NetBackup is used.

</td></tr>
<tr><td>23
□</td><td><b>Active NOAM:</b> Correct the RecognizedAuthority table</td><td>

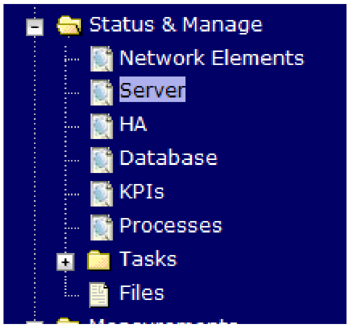
Establish an SSH session to the active NOAM, login as ***admusr***.

Execute the following command:

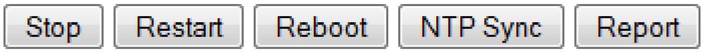
```
$ sudo top.setPrimary
- Using my cluster: A1789
- New Primary Timestamp: 11/09/15 20:21:43.418
- Updating A1789.022: <DSR_NOAM_B_hostname>
- Updating A1789.144: <DSR_NOAM_A_hostname>
```

</td></tr>
<tr><td>24
□</td><td><b>NOAM VIP GUI:</b> Restart DSR application</td><td>

Navigate to **Main Menu->Status & Manage->Server**,

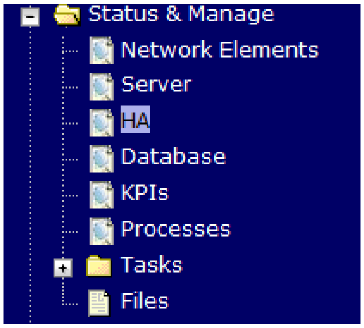


Select the recovered NOAM server and click on **Restart**.



</td></tr>
<tr><td>25
□</td><td><b>NOAM VIP GUI:</b> Set recovered NOAM Server to Active</td><td>

Navigate to **Status & Manage -> HA**



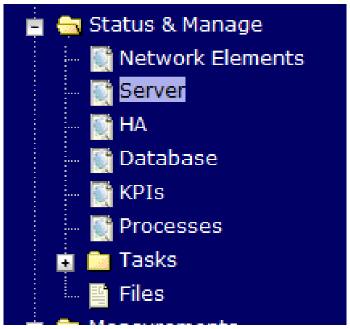
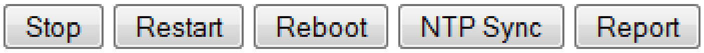
Click on **Edit** at the bottom of the screen

For the recovered standby NOAM that is set to forced standby, set it to **Active**

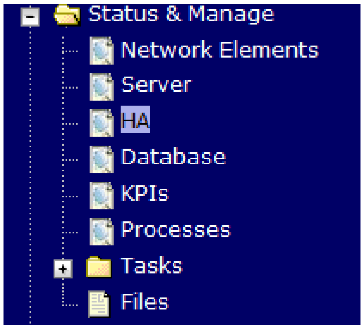
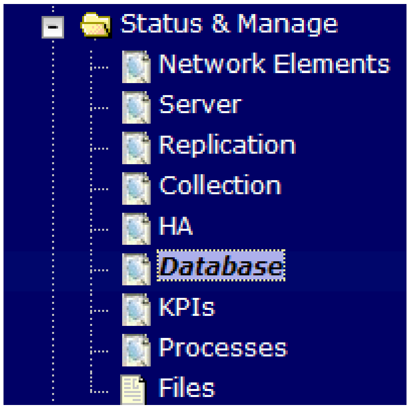
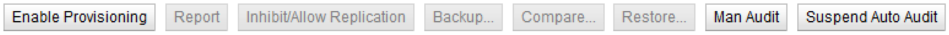
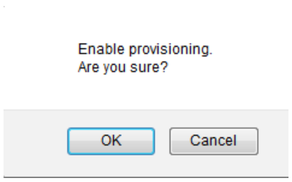
Press **OK**

</td></tr>
</table>

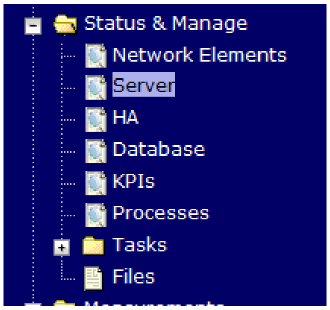
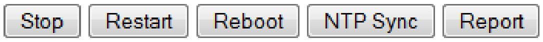
Procedure 3: Recovery Scenario 3

26 □	**Install NetBackup Client (Optional)**	If NetBackup is used execute procedure *"Install NetBackup Client"* from reference [8]
27 □	**NOAM VIP GUI:** Recover Failed SOAM Servers	Recover failed SOAM servers (**standby, spare**) by repeating the **following steps** for each SOAM server: 1. Execute procedure "Configure the SOAM Servers", steps 1-3, and 5-8 from reference [8]. **Note:** If you are using NetBackup, also execute step 10 2. If you are using NetBackup, execute procedure *"Install NetBackup Client"* from reference [8].
28 □	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered SOAM server and click on **Restart**. 
29 □	**(PCA Only) Activate PCA Feature**	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. **Note:** If not all SOAM sites are ready at this point, then you should repeat activation for each *new* SOAM site that comes online.
30 □	**NOAM VIP GUI:** Recover the C-Level Server (DA-MP, SBRs, IPFE, SS7-MP)	Execute procedure *"Configure MP Blade Servers"*, Steps 1, 7, 11-14, and 17 from reference [8]. **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. Repeat this step for any remaining failed MP servers.

Procedure 3: Recovery Scenario 3

31 □	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click on **Edit** at the bottom of the screen For each server whose Max Allowed HA Role is set to Standby, set it to **Active** Press **OK**
32 □	**NOAM VIP GUI:** Enable Provisioning	Click on **Main Menu->Status & Manage->Database**  Status & Manage Network Elements Server Replication Collection HA Database KPIs Processes Files Enable Provisioning by clicking on **Enable Provisioning** button at the bottom of the screen as shown below.  Enable Provisioning Report Inhibit/Allow Replication Backup... Compare... Restore... Man Audit Suspend Auto Audit A confirmation window will appear, press **OK** to enable Provisioning.  Enable provisioning. Are you sure?

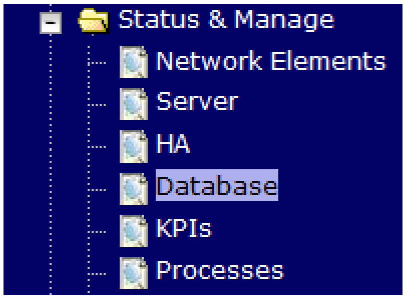
Procedure 3: Recovery Scenario 3

33 □	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select each recovered server and click on **Restart**. 
34 □	**ACTIVE NOAM:** Perform key exchange between the active-NOAM and recovered servers.	Establish an SSH session to the Active NOAM, login as ***admusr.*** Execute the following command to perform a keyexchange from the active NOAM to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>` **Note:** If an export server is configured, perform this step.
35 □	**ACTIVE NOAM:** Activate Optional Features	Establish an SSH session to the active NOAM, login as ***admusr.*** Refer to **section** **1.5** Optional Features to activate any features that were previously activated. **Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: *`iload#31000{S/W Fault}`*

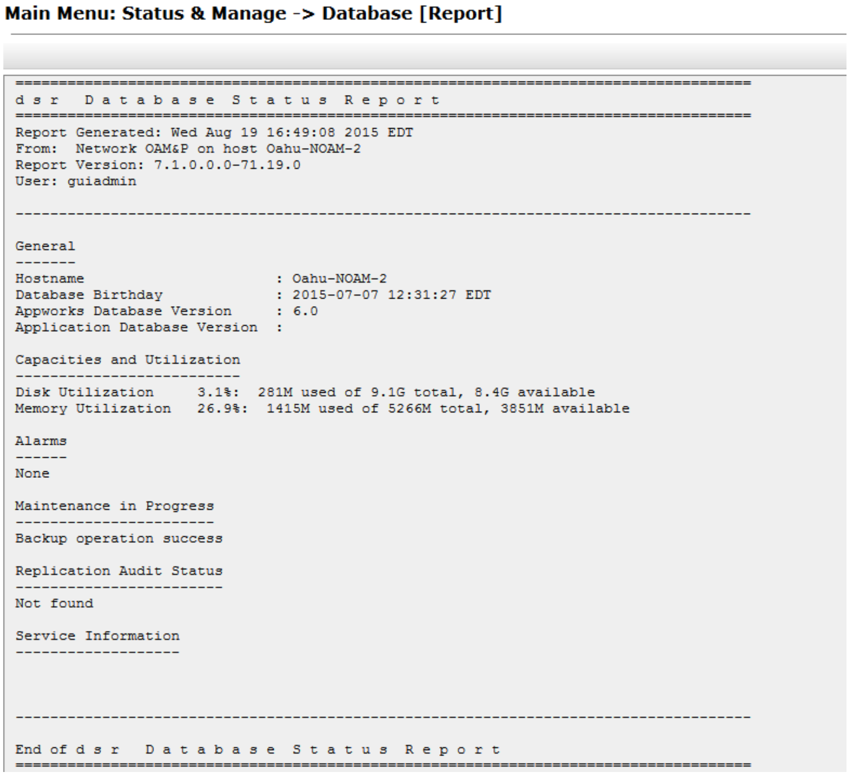
Procedure 3: Recovery Scenario 3

<table>
<tr>
<td>36
□</td>
<td><b>NOAM VIP GUI:</b> Fetch and Store the database Report for the Newly Restored Data and Save it</td>
<td>

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



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



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

```
=====================================================================================
d s r   D a t a b a s e   S t a t u s   R e p o r t
=====================================================================================
Report Generated: Wed Aug 19 16:49:08 2015 EDT
From:  Network OAM&P on host Oahu-NOAM-2
Report Version: 7.1.0.0.0-71.19.0
User: guiadmin

-------------------------------------------------------------------------------------


General
-------
Hostname                      : Oahu-NOAM-2
Database Birthday             : 2015-07-07 12:31:27 EDT
Appworks Database Version     : 6.0
Application Database Version  :

Capacities and Utilization
--------------------------
Disk Utilization     3.1%:  281M used of 9.1G total, 8.4G available
Memory Utilization   26.9%:  1415M used of 5266M total, 3851M available

Alarms
------
None

Maintenance in Progress
-----------------------
Backup operation success

Replication Audit Status
------------------------
Not found

Service Information
-------------------



-------------------------------------------------------------------------------------

End of d s r   D a t a b a s e   S t a t u s   R e p o r t
=====================================================================================
```

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

</td>
</tr>
</table>

Procedure 3: Recovery Scenario 3

37 □

ACTIVE NOAM: Verify Replication Between Servers.

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

```
$ sudo irepstat –m
```

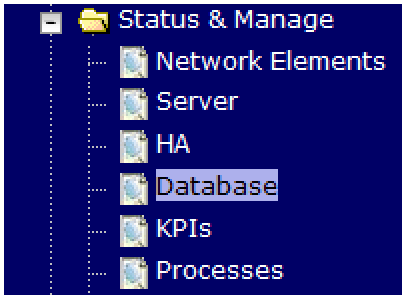
Output like below shall be generated:

```
-- Policy 0 ActStb [DbReplication] ----------------------------------
----------------------------------------------------------------------
-------------------------------------
RDU06-MP1 -- Stby
  BC From RDU06-SO1 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-SO1 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-NO1 -- Active
  AB To   RDU06-SO1 Active      0   0.50 1%R 0.03%cpu 21B/s
RDU06-SO1 -- Active
  AB From RDU06-NO1 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
```

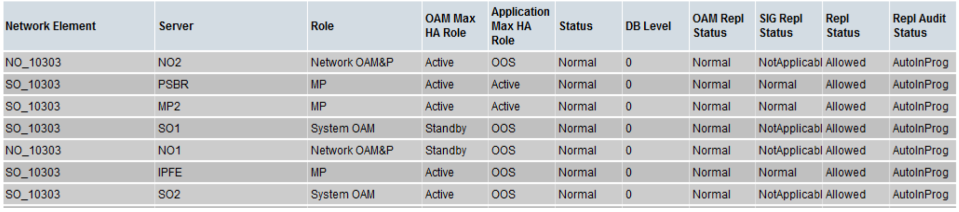
38 □

NOAM VIP GUI: Verify the Database states

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



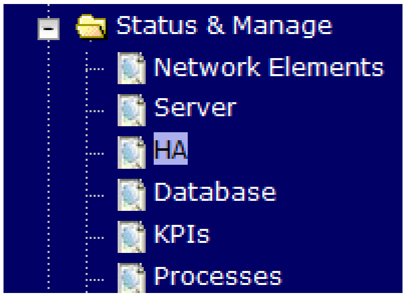
Verify that the "OAM Max HA Role" is either "Active" or "Standby" for NOAM and SOAM and "Application Max HA Role" for MPs is "Active", and that the status is "Normal" as shown below:



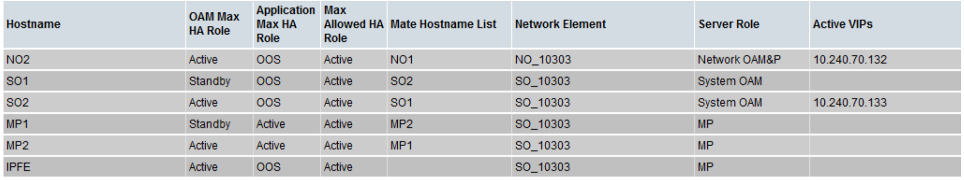
Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
NO_10303	NO2	Network OAM&P	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg
SO_10303	PSBR	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg
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

39 □ **NOAM VIP GUI:** Verify the HA Status

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



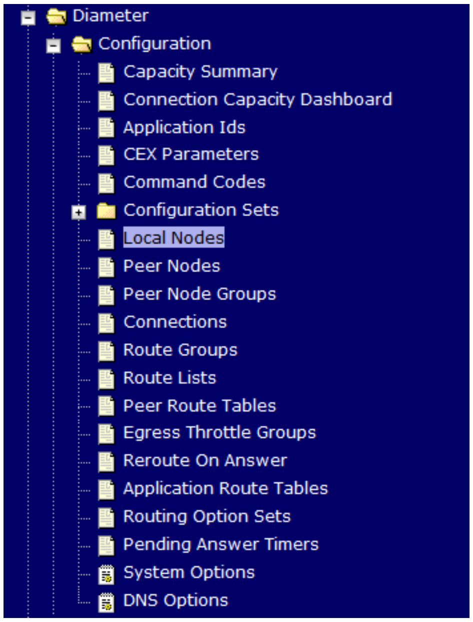
Select the row for all of the servers
Verify that the “HA Role” is either “Active” or “Standby”.



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

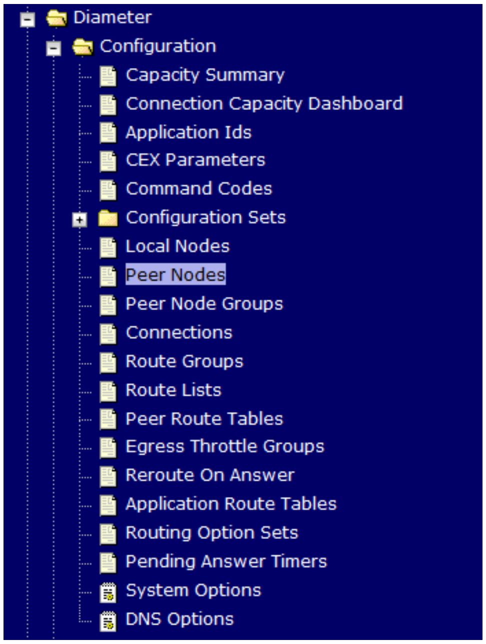
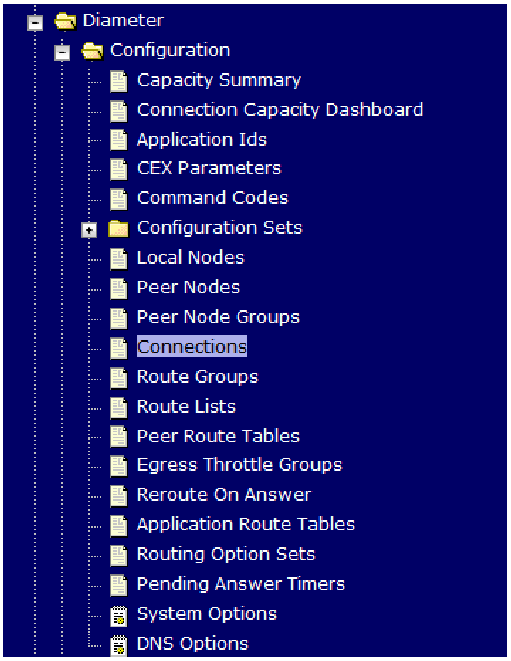
40 □ **SOAM VIP GUI:** Verify the Local Node Info

Navigate to **Main Menu->Diameter->Configuration->Local Node**

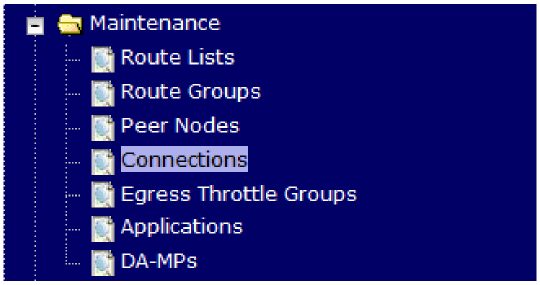
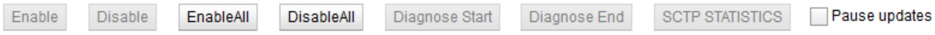
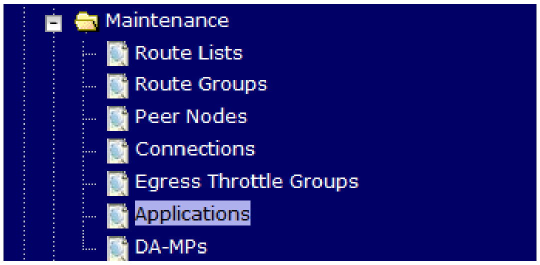
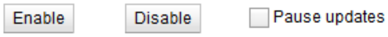
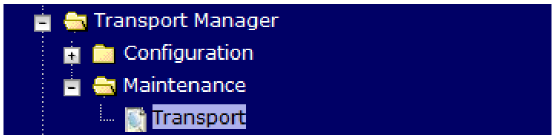
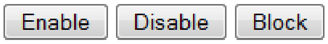


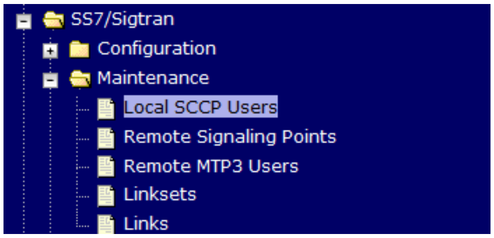
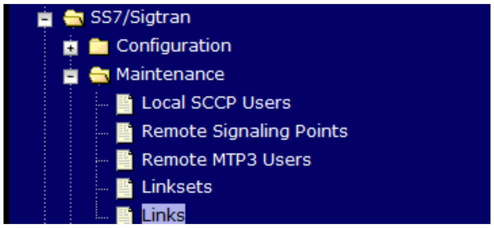
Verify that all the local nodes are shown.

Procedure 3: Recovery Scenario 3

41 □	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Diameter Configuration Capacity Summary Connection Capacity Dashboard Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes Peer Node Groups Connections Route Groups Route Lists Peer Route Tables Egress Throttle Groups Reroute On Answer Application Route Tables Routing Option Sets Pending Answer Timers System Options DNS Options Verify that all the peer nodes are shown.
42 □	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections**  Diameter Configuration Capacity Summary Connection Capacity Dashboard Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes Peer Node Groups Connections Route Groups Route Lists Peer Route Tables Egress Throttle Groups Reroute On Answer Application Route Tables Routing Option Sets Pending Answer Timers System Options DNS Options Verify that all the connections are shown.

Procedure 3: Recovery Scenario 3

43 □	**SOAM VIP GUI:** Enable Connections if needed	Navigate to **Main Menu->Diameter->Maintenance->Connections**  Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups Applications DA-MPs Select each connection and click on the **Enable** button. Alternatively you can enable all the connections by selecting the **EnableAll** button.  Enable Disable EnableAll DisableAll Diagnose Start Diagnose End SCTP STATISTICS □ Pause updates Verify that the Operational State is Available.
44 □	**SOAM VIP GUI:** Enable Optional Features	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups Applications DA-MPs Select the optional feature application configured in **step 31**. Click the **Enable** button. 
45 □	**SOAM VIP GUI:** Re-enable Transports if Needed	Navigate to **Main Menu->Transport Manager -> Maintenance -> Transport**  Transport Manager Configuration Maintenance Transport Select each transport and click on the Enable button  Verify that the Operational Status for each transport is Up.

46 □	**SOAM VIP GUI:** Re-enable MAPIWF application if needed	Navigate to **Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users**  SS7/Sigtran Configuration Maintenance Local SCCP Users Remote Signaling Points Remote MTP3 Users Linksets Links Click on the **Enable** button corresponding to MAPIWF Application Name. Verify that the SSN Status is Enabled.
47 □	**SOAM VIP GUI:** Re-enable links if needed	Navigate to **Main Menu->SS7/Sigtran->Maintenance->Links**  SS7/Sigtran Configuration Maintenance Local SCCP Users Remote Signaling Points Remote MTP3 Users Linksets Links Click on **Enable** button for each link. Verify that the Operational Status for each link is Up.

Procedure 3: Recovery Scenario 3

<table>
<tr>
<td>48
□</td>
<td><b>NOAM VIP:</b> Verify all servers in Topology are accessible (RADIUS Only)</td>
<td>

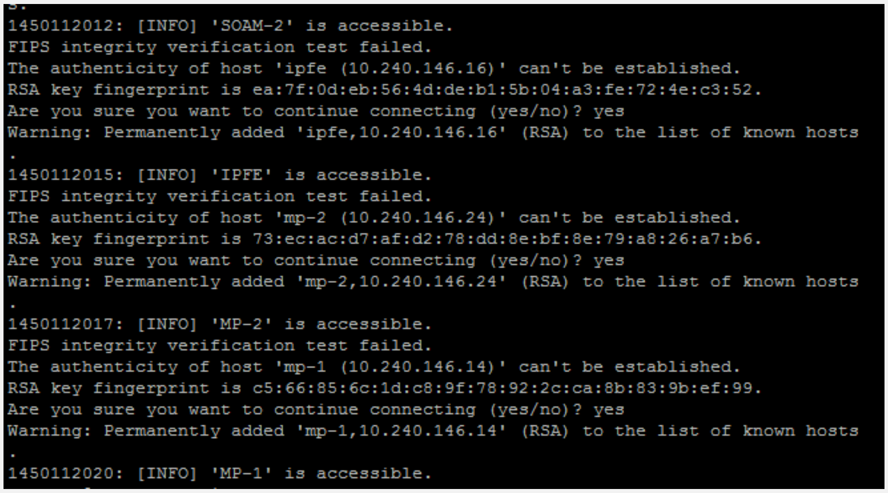
If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)

Establish an SSH session to the NOAM VIP. Login as ***admusr.***

Execute following commands to check if all the servers in the Topology are accessible :

```
$ /usr/TKLC/dpi/bin/sharedKrevo –checkAccess
```

Output Example:



```
1450112012: [INFO] 'SOAM-2' is accessible.
FIPS integrity verification test failed.
The authenticity of host 'ipfe (10.240.146.16)' can't be established.
RSA key fingerprint is ea:7f:0d:eb:56:4d:de:b1:5b:04:a3:fe:72:4e:c3:52.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ipfe,10.240.146.16' (RSA) to the list of known hosts
.
1450112015: [INFO] 'IPFE' is accessible.
FIPS integrity verification test failed.
The authenticity of host 'mp-2 (10.240.146.24)' can't be established.
RSA key fingerprint is 73:ec:ac:d7:af:d2:78:dd:8e:bf:8e:79:a8:26:a7:b6.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mp-2,10.240.146.24' (RSA) to the list of known hosts
.
1450112017: [INFO] 'MP-2' is accessible.
FIPS integrity verification test failed.
The authenticity of host 'mp-1 (10.240.146.14)' can't be established.
RSA key fingerprint is c5:66:85:6c:1d:c8:9f:78:92:2c:ca:8b:83:9b:ef:99.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mp-1,10.240.146.14' (RSA) to the list of known hosts
.
1450112020: [INFO] 'MP-1' is accessible.
```

Note: If any of the servers are not accessible, stop and contact Appendix L: My Oracle Support (MOS)

</td>
</tr>
</table>

Procedure 3: Recovery Scenario 3

49 □	**SOAM 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)** 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***. Execute following commands to check if existing Key file on Active SOAM server is valid : **`$ cd /usr/TKLC/dpi/bin/`** **`$ ./sharedKrevo –validate`** Expected Output: **`/usr/TKLC/dpi/`** **Note:** If output of above command shows that existing key file is not valid, contact Appendix L: My Oracle Support (MOS) Establish an SSH session to the active SOAM, login as ***admusr***. Execute following command to copy the key file to Active NOAM : **`$ cd /usr/TKLC/dpi/bin/`** **`$ ./sharedKrevo –copyKey –destServer <Active NOAM server name>`**

Procedure 3: Recovery Scenario 3

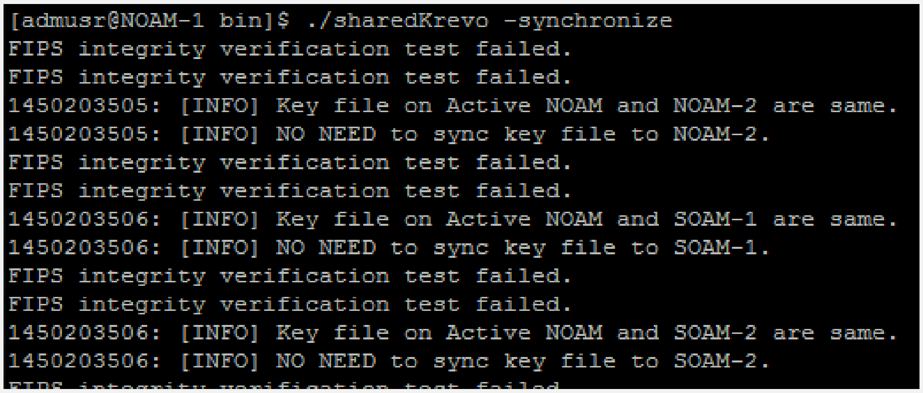
50 □

NOAM VIP:
Copy key file to all the servers in Topology (RADIUS Only)

Establish an SSH session to any of the Active NOAM. Login as admusr.

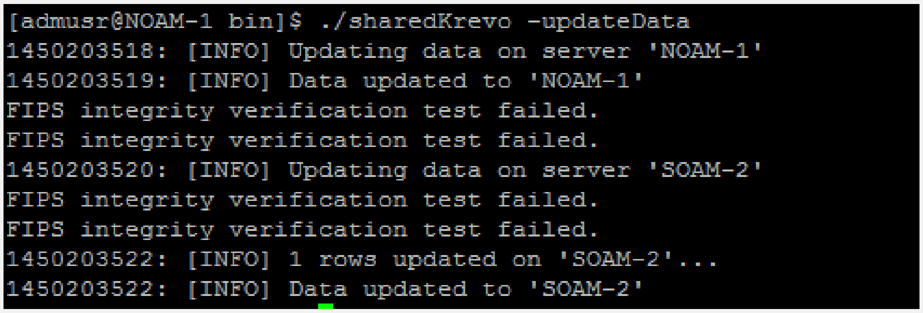
Execute following command to copy the key file to all the servers in the Topology :

```
$ ./sharedKrevo -synchronize
```



```
[admusr@NOAM-1 bin]$ ./sharedKrevo -synchronize
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450203505: [INFO] Key file on Active NOAM and NOAM-2 are same.
1450203505: [INFO] NO NEED to sync key file to NOAM-2.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450203506: [INFO] Key file on Active NOAM and SOAM-1 are same.
1450203506: [INFO] NO NEED to sync key file to SOAM-1.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450203506: [INFO] Key file on Active NOAM and SOAM-2 are same.
1450203506: [INFO] NO NEED to sync key file to SOAM-2.
FIPS integrity verification test failed.
```

```
$ ./sharedKrevo -updateData
```

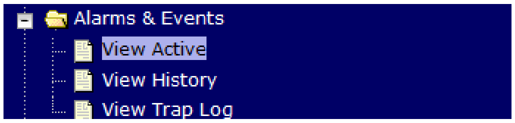


```
[admusr@NOAM-1 bin]$ ./sharedKrevo -updateData
1450203518: [INFO] Updating data on server 'NOAM-1'
1450203519: [INFO] Data updated to 'NOAM-1'
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450203520: [INFO] Updating data on server 'SOAM-2'
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450203522: [INFO] 1 rows updated on 'SOAM-2'...
1450203522: [INFO] Data updated to 'SOAM-2'
```

51 □

SOAM VIP GUI:
Examine All Alarms

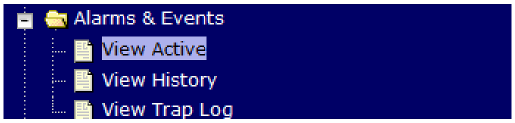
Navigate to **Main Menu->Alarms & Events->View Active**



Examine all active alarms and refer to the on-line help on how to address them.

If needed contact **Appendix L: My Oracle** Support (MOS).

Procedure 3: Recovery Scenario 3

52 □	**NOAM VIP GUI:** Examine All Alarms	Login to the NOAM VIP if not already logged in. Navigate to **Main Menu->Alarms & Events->View Active**  Alarms & Events View Active View History View Trap Log Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix L: My Oracle** Support (MOS).
53 □	**Restore GUI Usernames and Passwords**	If applicable, Execute steps in **Section 0** to recover the user and group information restored.
54 □	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**: DSR Database Backup to back up the Configuration databases:
55 □	**Recover IDIH**	If IDIH were affected, refer to **Section 11** to perform disaster recovery on IDIH.

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

For a partial outage with an NOAM server and an SOAM server intact and available, only base recovery of hardware and software is needed. The intact NO and SOAM servers are capable of restoring the database via replication to all servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures' detailed steps are in Procedure 4. The major activities are summarized as follows:

Recover Standby NOAM server by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.

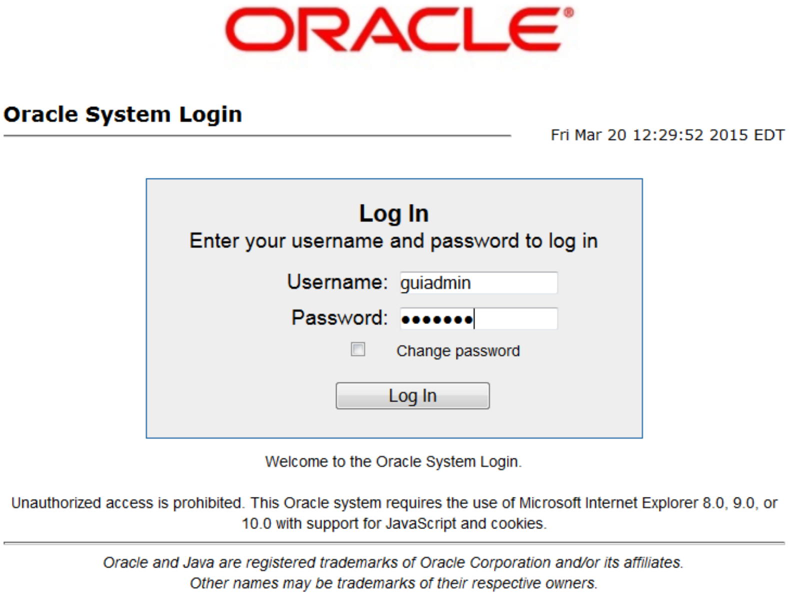
The database is intact at the active NOAM server and does not require restoration at the standby NOAM server.

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

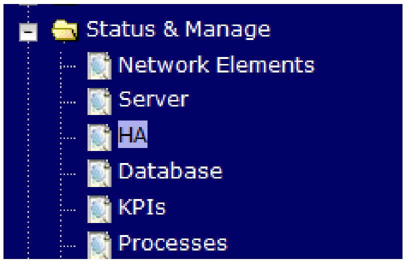
The database in intact at the active NOAM server and does not require restoration at the SO and MP servers.

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

Procedure 4: Recovery Scenario 4

STEP #		
S **T** **E** **P** **#**	This procedure performs recovery if at least 1 NOAM server is intact and available and 1 SOAM server is intact and available. 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 □	**Workarounds**	Refer to **Appendix G**: Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
2 □	**Gather Required Materials**	Gather the documents and required materials listed in **Section 3.1** Required Materials
3 □	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:  ORACLE **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*

Procedure 4: Recovery Scenario 4

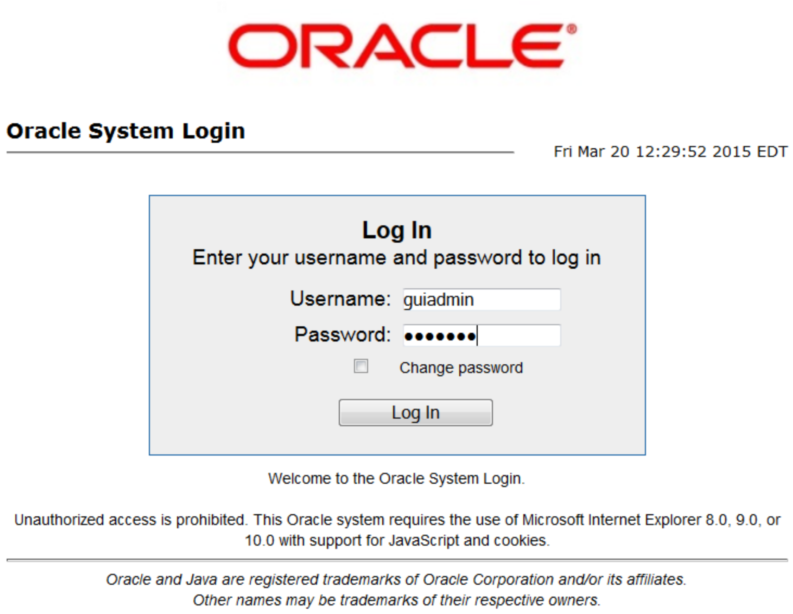
4 □	**Active NOAM:** Set Failed Servers to Standby	Navigate to **Main Menu -> Status & Manage -> HA**  Status & Manage Network Elements Server HA Database KPIs Processes Select **Edit** Set the Max Allowed HA Role drop down box to **Standby** for the failed servers. Select **Ok**
5 □	**RMS NOAM Failure:** Configure BIOS Settings and Update Firmware	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** 1. Configure and verify the BIOS settings by executing procedure *“Configure the RMS Server BIOS Settings”* from reference [10] 2. Verify and/or upgrade server firmware by executing procedure *“Upgrade Management Server Firmware”* from reference[10] **Note:** Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.
6 □	**RMS NOAM Failure:** Backups Available	If the failed server is **NOT** a rack mount server, **skip to step 9.** This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, **skip this step**. 1. Restore the TVOE backup by executing Appendix H: Restore TVOE Configuration from Backup Media If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing 2. Appendix I: Restore PMAC from Backup

Procedure 4: Recovery Scenario 4

7 □	**Recover Failed Aggregation/ Enclosure Switches, and OAs**	Recover failed OAs, aggregation and enclosure switches if needed. Backups Available: 1. Refer to Appendix B: Recovering/Replacing Failed 3rd Party Components (Switches, OAs)to recover failed OAs, aggregation, and enclosure switches Backups **NOT** Available: 1. Execute section *"HP C-7000 Enclosure Configuration"* 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.
8 □	**RMS NOAM Failure:** Backups **NOT** Available	If the failed server is **NOT** a rack mount server, **skip to step 9.** This step assumes that TVOE and PMAC backups **NOT** are available, if the TVOE and PMAC have already been restored, **skip this step.** If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. Section *"Configure and IPM Management Server"* from reference [10]. 2. Section *"Install PM&C"* from reference [10]. 3. Section *"Configure PM&C"* from reference [10]. If the PMAC is **NOT** located on the same TVOE host as the failed NOAM, Execute the following sections/procedures Section *"Installing TVOE on Rack Mount Server(s)"* from reference [10].
9 □	**HP-Class Blade Failure:** Configure Blade Server iLO, Update Firmware/BIOS Settings	If the failed server is **NOT** an HP C-Class Blade, **skip to step 13.** 1. Execute procedure *"Configure Blade Server iLO Password for Administrator Account"* from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing section *"Server Blades Installation Preparation"* from reference [10]

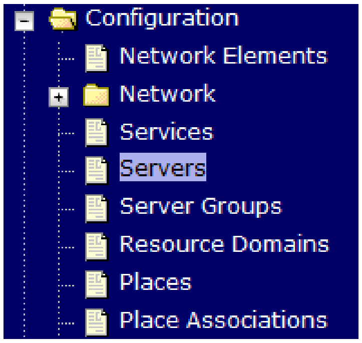
Procedure 4: Recovery Scenario 4

10 □	**HP-Class Blade Failure:** Backups Available	If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 13.** This step assumes that TVOE backups are available, if backups are **NOT** available, **skip this step**. 1. Install and configure TVOE on failed TVOE blade servers by executing section *"Install TVOE on Blade Servers"* 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.
11 □	**HP-Class Blade Failure:** Backups **NOT** Available	If the failed server is **NOT** an OAM HP C-Class Blade, **skip to step 13.** This step assumes that TVOE backups are **NOT** are available 1. Install and configure TVOE on failed TVOE blade servers by executing section *"Install TVOE on Blade Servers"* 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] **Note:** Although the title of the procedure is related to SOAMs only, execute this procedure for any failed NOAMs located on TVOE server blades.
12 □	**Create VMs**	Execute Appendix K: Create NOAM/SOAM Virtual Machines to create the NOAM and SOAM VMs on failed TVOE server blades.
13 □	**IPM and Install DSR Application on Failed Guest/Servers**	1. Execute procedure *"IPM Blades and VMs"* for the failed SOAM VMs and MP blades from reference [8]. 2. Execute procedure *"Install the Application"* for the failed SOAM VMs and MP blades from reference [8].
14 □	**Install NetBackup Client (Optional)**	If NetBackup is used execute procedure *"Install NetBackup Client"* from reference [8]

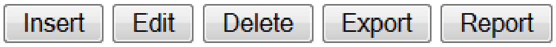
15 □	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:  ORACLE **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*
16 □	**Exchange SSH keys between PMAC and Failed NOAM Server**	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.** Note the IP address for the failed NOAM server VM. Login to the PMAC terminal as the ***admusr.*** From a terminal window connection on the PMAC as the ***admusr*** user, exchange SSH keys for ***admusr*** between the PMAC and the failed NOAM server VM control network IP address. When prompted for the password, enter the password for the ***admusr*** user of the NOAM server. `$ keyexchange admusr@<NO2_Control_IP Address>` **Note:** if Key exchange fails, edit /home/admusr/.ssh/known_hosts and remove blank lines, and retry the keyexchange commands.

Procedure 4: Recovery Scenario 4

<table>
<tr>
<td>17
□</td>
<td><b>NOAM VIP GUI:</b> Export the Initial Configuration</td>
<td>
Navigate to <b>Main Menu -> Configuration -> Servers.</b>



From the GUI screen, select the failed NOAM server and then select <b>Export</b> to generate the initial configuration data for that server.



</td>
</tr>
<tr>
<td>18
□</td>
<td><b>NOAM VIP:</b> Copy Configuration File to Failed NOAM Server</td>
<td>
Obtain a terminal session to the NOAM VIP, login as the <b><i>admusr</i></b>.

Use the <b>awpushcfg</b> utility to copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the active NOAM to the failed NOAM server, using the Control network IP address for the failed NOAM VM.

The configuration file will have a filename like “TKLCConfigData.<<b><i>hostname</i></b>>.sh”.

```
$ sudo awpushcfg
```

The awpushcfg utility is interactive, so the user will be prompted for the following:

- IP address of the local PMAC server: Use the local control network address from the PMAC.
- Username: Use <b>admusr</b>
- 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 <b>Step 17</b>
</td>
</tr>
</table>

Procedure 4: Recovery Scenario 4

<table>
<tr>
<td>19
□</td>
<td><b>Failed NOAM Server:</b> Verify awpushcfg was called and Reboot the Server</td>
<td>

Establish an SSH session to the failed NOAM server, login as the ***admusr*** user.

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.

Verify awpushcfg was called by checking the following file

```
$ sudo cat /var/TKLC/appw/logs/Process/install.log
```

Verify the following message is displayed:

```
[SUCCESS] script completed successfully!
```

Now Reboot the Server:

```
$ sudo init 6
```

```
Wait for the server to reboot
```

</td>
</tr>
<tr>
<td>20
□</td>
<td><b>Failed NOAM Server:</b> Configure Networking for Dedicated NetBackup Interface (Optional)</td>
<td>

Note: You will only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.

Obtain a terminal window to the failed NOAM server, logging in as the ***admusr***.

```
$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup
--type=Ethernet --onboot=yes
--address=<NO2_NetBackup_IP_Adress>
--netmask=<NO2_NetBackup_NetMask>
```

```
$ 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>
```

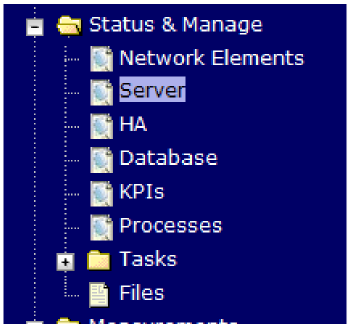
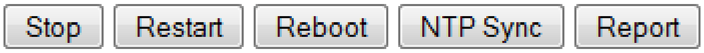
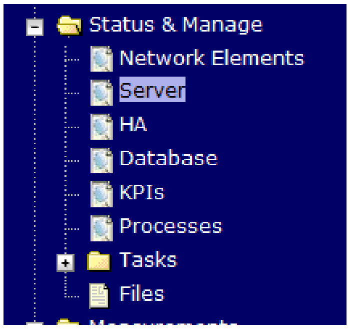
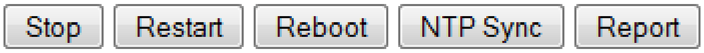
</td>
</tr>
<tr>
<td>21
□</td>
<td><b>Failed NOAM Server:</b> Verify Server Health</td>
<td>

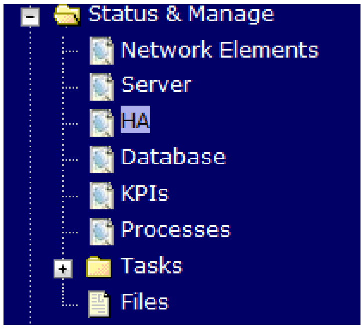
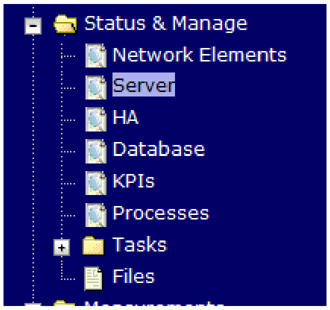
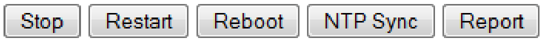
Execute the following command on the 2nd NOAM server and make sure that no errors are returned:

```
$ 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
```

</td>
</tr>
</table>

Procedure 4: Recovery Scenario 4

22 □	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered NOAM server and click on **Restart**. 
23 □	**NOAM VIP GUI:** Recover Failed SOAM Servers	Recover failed SOAM servers (**standby, spare**) by repeating the **following steps** for each SOAM server: 1. Execute procedure “Configure the SOAM Servers”, steps 1-3, and 5-8 from reference [8]. **Note:** If you are using NetBackup, also execute step 10 2. If you are using NetBackup, execute procedure *“Install NetBackup Client”* from reference [8].
24 □	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered SOAM server and click on **Restart**. 

25 □	**(PCA Only) Activate PCA Feature**	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. **Note:** If not all SOAM sites are ready at this point, then you should repeat activation for each *new* SOAM site that comes online.
26 □	**NOAM VIP GUI:** Recover the C-Level Server (DA-MP, SBRs, IPFE, SS7-MP)	Execute procedure *“Configure MP Blade Servers”*, Steps 1, 7, 11-14, and 17 from reference [8]. **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. Repeat this step for any remaining failed MP servers.
27 □	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click on **Edit** at the bottom of the screen For each server whose Max Allowed HA Role is set to Standby, set it to **Active** Press **OK**
28 □	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select each recovered server and click on **Restart**. 

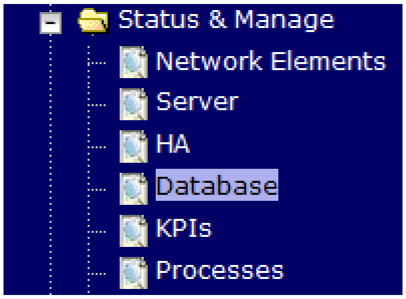
Procedure 4: Recovery Scenario 4

29 □	**ACTIVE NOAM:** Login	Login to the recovered Active NOAM via SSH terminal as ***admusr*** user.
30 □	**ACTIVE NOAM:** Perform key exchange between the active-NOAM and recovered servers.	Establish an SSH session to the Active NOAM, login as ***admusr.*** Execute the following command to perform a keyexchange from the active NOAM to each recovered server: **`$ keyexchange admusr@<Recovered Server Hostname>`**
31 □	**ACTIVE NOAM:** Activate Optional Features	Establish an SSH session to the active NOAM, login as ***admusr.*** Refer to **section** 1.5 Optional Featuresto activate any features that were previously activated. **Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: *`iload#31000{S/W Fault}`*

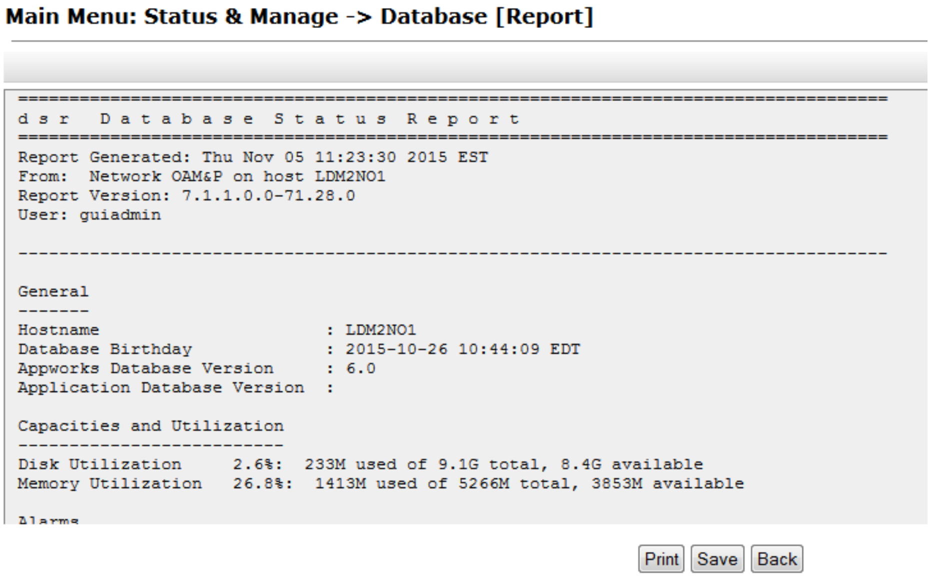
Procedure 4: Recovery Scenario 4

<table>
<tr>
<td>32
□</td>
<td><b>NOAM VIP GUI:</b> Fetch and Store the database Report for the Newly Restored Data and Save it</td>
<td>

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 LDM2NO1
Report Version: 7.1.1.0.0-71.28.0
User: guiadmin

-------------------------------------------------------------------------------------

General
-------
Hostname                      : LDM2NO1
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
```

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

</td>
</tr>
</table>

Procedure 4: Recovery Scenario 4

33 □ **ACTIVE NOAM:** Verify Replication Between Servers.

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

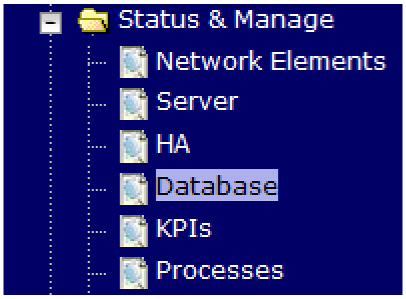
```
$ sudo irepstat –m
```

Output like below shall be generated:

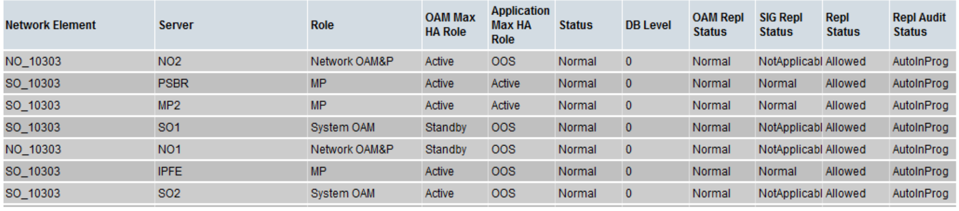
```
-- Policy 0 ActStb [DbReplication] ----------------------------------
----------------------------------------------------------------------
-------------------------------------
RDU06-MP1 -- Stby
  BC From RDU06-SO1 Active      0   0.50 ^0.17%cpu 42B/s  A=none
  CC From RDU06-MP2 Active      0   0.10 ^0.17 0.88%cpu 32B/s  A=none
RDU06-MP2 -- Active
  BC From RDU06-SO1 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-NO1 -- Active
  AB To   RDU06-SO1 Active      0   0.50 1%R 0.03%cpu 21B/s
RDU06-SO1 -- Active
  AB From RDU06-NO1 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
```

34 □ **NOAM VIP GUI:** Verify the Database states

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

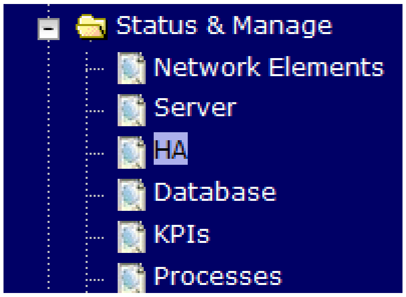


Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below:

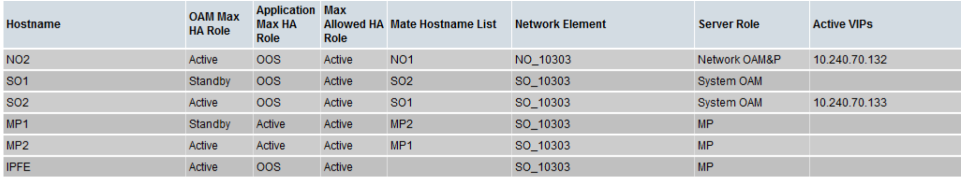


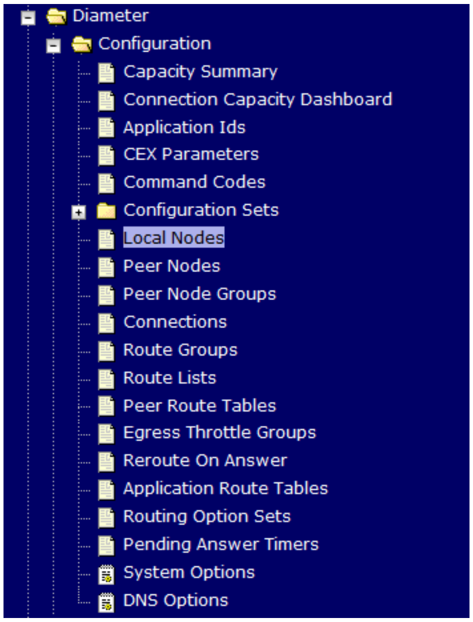
Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
NO_10303	NO2	Network OAM&P	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg
SO_10303	PSBR	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg
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

<table>
<tr>
<td>35
□</td>
<td><b>NOAM VIP GUI:</b> Verify the HA Status</td>
<td>
Click on <b>Main Menu->Status and Manage-&gt;HA</b>



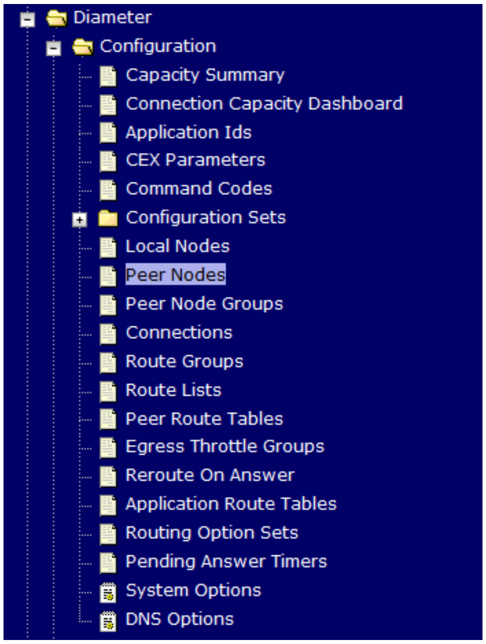
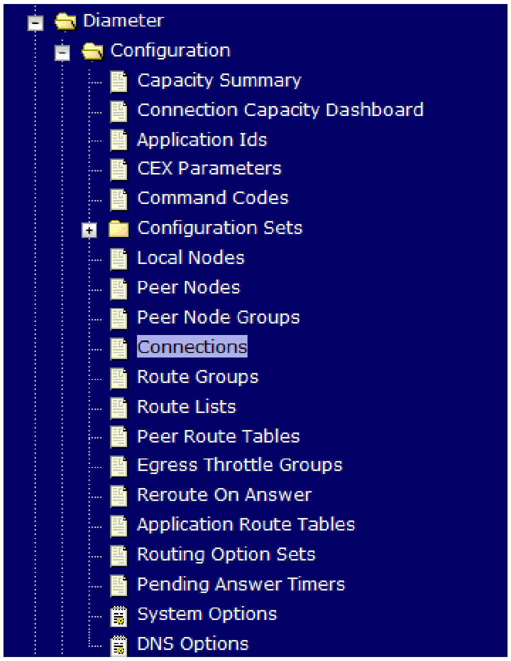
Select the row for all of the servers
Verify that the “HA Role” is either “Active” or “Standby”.

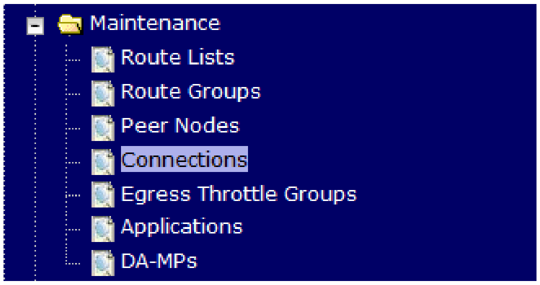
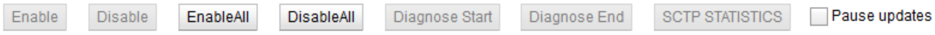
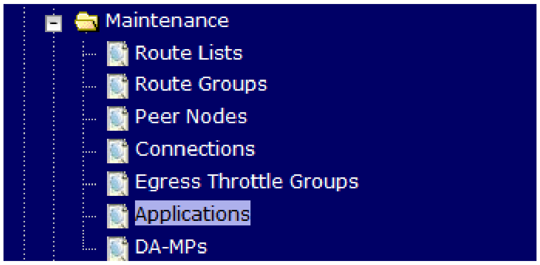
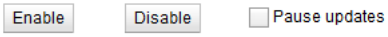

<table>
<tr><th>Hostname</th><th>OAM Max HA Role</th><th>Application Max HA Role</th><th>Max Allowed HA Role</th><th>Mate Hostname List</th><th>Network Element</th><th>Server Role</th><th>Active VIPs</th></tr>
<tr><td>NO2</td><td>Active</td><td>OOS</td><td>Active</td><td>NO1</td><td>NO_10303</td><td>Network OAM&P</td><td>10.240.70.132</td></tr>
<tr><td>SO1</td><td>Standby</td><td>OOS</td><td>Active</td><td>SO2</td><td>SO_10303</td><td>System OAM</td><td></td></tr>
<tr><td>SO2</td><td>Active</td><td>OOS</td><td>Active</td><td>SO1</td><td>SO_10303</td><td>System OAM</td><td>10.240.70.133</td></tr>
<tr><td>MP1</td><td>Standby</td><td>Active</td><td>Active</td><td>MP2</td><td>SO_10303</td><td>MP</td><td></td></tr>
<tr><td>MP2</td><td>Active</td><td>Active</td><td>Active</td><td>MP1</td><td>SO_10303</td><td>MP</td><td></td></tr>
<tr><td>IPFE</td><td>Active</td><td>OOS</td><td>Active</td><td></td><td>SO_10303</td><td>MP</td><td></td></tr>
</table>
</td>
</tr>
<tr>
<td>36
□</td>
<td><b>SOAM VIP GUI:</b> Verify the Local Node Info</td>
<td>
Navigate to <b>Main Menu->Diameter->Configuration->Local Node</b>



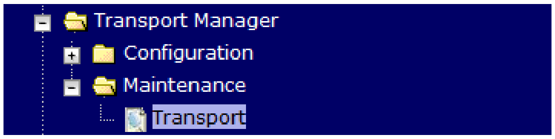
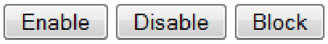
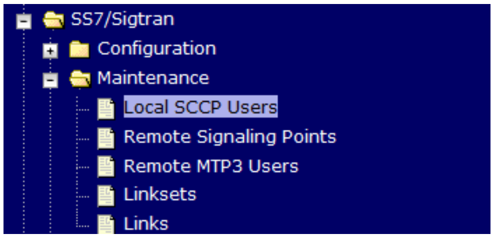
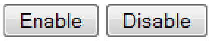
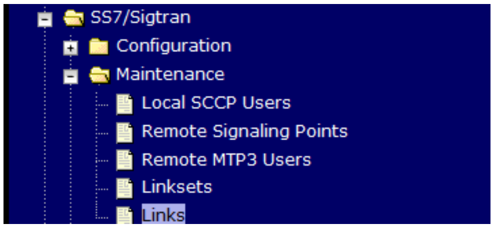
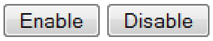
Verify that all the local nodes are shown.
</td>
</tr>
</table>

Procedure 4: Recovery Scenario 4

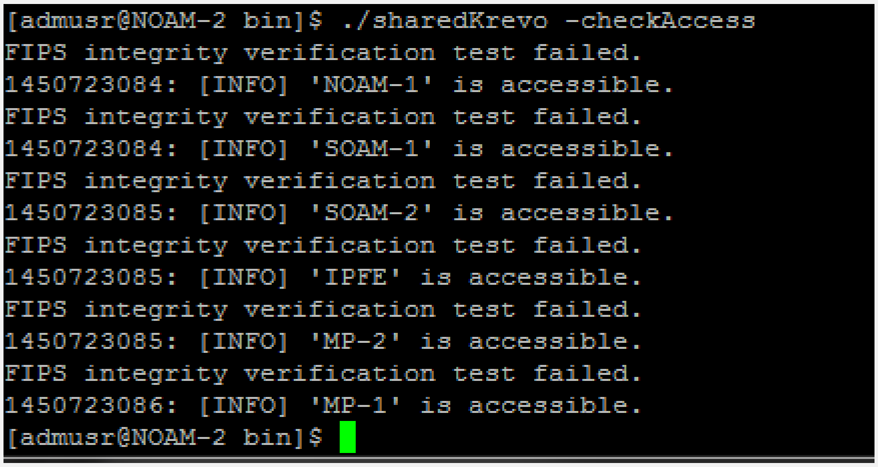
37 □	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Diameter Configuration Capacity Summary Connection Capacity Dashboard Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes Peer Node Groups Connections Route Groups Route Lists Peer Route Tables Egress Throttle Groups Reroute On Answer Application Route Tables Routing Option Sets Pending Answer Timers System Options DNS Options Verify that all the peer nodes are shown.
38 □	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections**  Diameter Configuration Capacity Summary Connection Capacity Dashboard Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes Peer Node Groups Connections Route Groups Route Lists Peer Route Tables Egress Throttle Groups Reroute On Answer Application Route Tables Routing Option Sets Pending Answer Timers System Options DNS Options Verify that all the connections are shown.

39 □	**MP Servers:** Disable SCTP Auth Flag	For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [14] Execute this procedure on all Failed MP Servers.
40 □	**SOAM VIP GUI:** Enable Connections if needed	Navigate to **Main Menu->Diameter->Maintenance->Connections**  Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups Applications DA-MPs Select each connection and click on the **Enable** button. Alternatively you can enable all the connections by selecting the **EnableAll** button.  Enable Disable EnableAll DisableAll Diagnose Start Diagnose End SCTP STATISTICS □ Pause updates Verify that the Operational State is Available.
41 □	**SOAM VIP GUI:** Enable Optional Features	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups Applications DA-MPs Select the optional feature application configured in **step 22**. Click the **Enable** button. 

Procedure 4: Recovery Scenario 4

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

Procedure 4: Recovery Scenario 4

45
□
	NOAM VIP: Verify all servers in Topology are accessible (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)**
		Establish an SSH session to the NOAM VIP. Login as ***admusr.***
		Execute following commands to check if all the servers in the Topology are accessible :
		`$ cd /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo –checkAccess`
		Example Output:
		
		`[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.`
		`FIPS integrity verification test failed.`
		`1450723086: [INFO] 'MP-1' is accessible.`
		`[admusr@NOAM-2 bin]$`
		Note: If any of the servers are not accessible, stop and contact Appendix L: My Oracle Support (MOS)

Procedure 4: Recovery Scenario 4

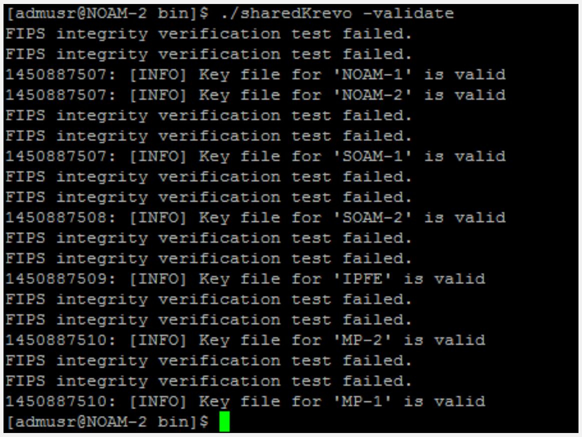
46 □

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 server is valid :

```
$ ./sharedKrevo -validate
```

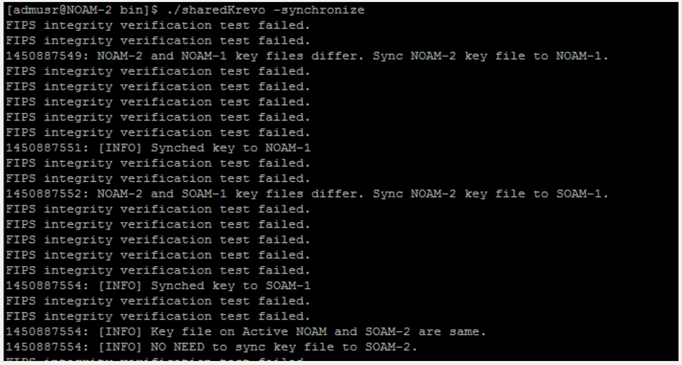


```
[admusr@NOAM-2 bin]$ ./sharedKrevo -validate
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450887507: [INFO] Key file for 'NOAM-1' is valid
1450887507: [INFO] Key file for 'NOAM-2' is valid
FIPS integrity verification test failed.
FIPS integrity verification test 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]$
```

If output of above command shows that existing key file is not valid then contact **Appendix L: My Oracle** Support (MOS)

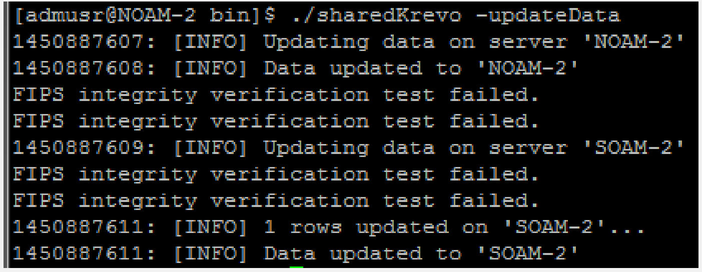
Execute following command to copy the key file to all the servers in the Topology :

```
$ ./sharedKrevo -synchronize
```

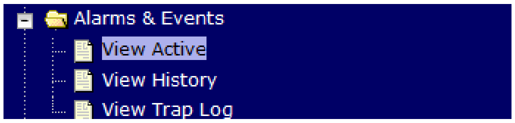
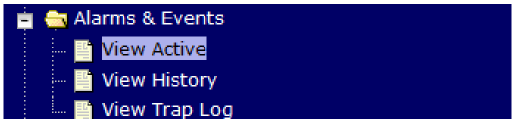


```
[admusr@NOAM-2 bin]$ ./sharedKrevo -synchronize
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450887549: NOAM-2 and NOAM-1 key files differ. Sync NOAM-2 key file to NOAM-1.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
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.
```

```
$ ./sharedKrevo -updateData
```



```
[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'
```

47 □	**SOAM VIP GUI:** Examine All Alarms	Navigate to **Main Menu->Alarms & Events->View Active**  Alarms & Events View Active View History View Trap Log Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix L: My Oracle** Support (MOS).
48 □	**NOAM VIP GUI:** Examine All Alarms	Login to the NOAM VIP if not already logged in. Navigate to **Main Menu->Alarms & Events->View Active**  Alarms & Events View Active View History View Trap Log Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix L: My Oracle** Support (MOS).

49
□
	Restart oampAgent if Needed	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.
		Establish an SSH session to each server that has the alarm., login as ***admusr***
		Execute the following commands:
		`$ sudo pm.set off oampAgent`
		`$ sudo pm.set on oampAgent`

50 □	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**: DSR Database Backup to back up the Configuration databases:
51 □	**Recover IDIH**	If IDIH were affected, refer to **Section 11** to perform disaster recovery on IDIH.

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

For a partial outage with both NOAM servers failed but a DR NOAM available, the DR NOAM is switched from secondary to primary then recovers the failed NOAM servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures' detailed steps are in Procedure 5. The major activities are summarized as follows:

Switch DR NOAM from secondary to primary

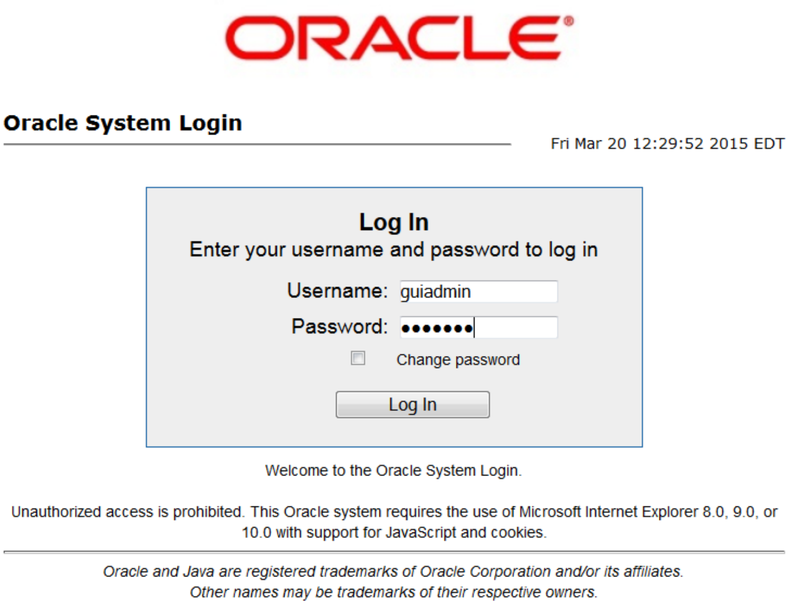
Recover the failed NOAM servers by recovering base hardware and software.

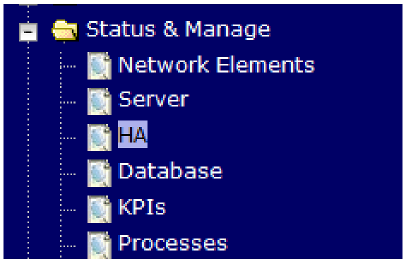
- Recover the base hardware.
- Recover the software.
- The database is intact at the newly active NOAM server and does not require restoration.

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

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

Procedure 5: Recovery Scenario 5

S T E P #	This procedure performs recovery if both NOAM servers have failed but a DR NOAM is available 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 □	**Workarounds**	Refer to **Appendix G**: Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
2 □	**Gather Required Materials**	Gather the documents and required materials listed in **Section 3.1** Required Materials
3 □	**Switch DR NOAM to Primary**	Execute **Appendix C**: Switching DR NOAM Site to Primary to have the DR NOAM become active.
4 □	**Recover Failed SOAMs**	If **ALL** SOAM servers have failed, execute Procedure 2
5 □	**DR-NOAM VIP GUI:** Login	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: `http://<Primary_DR-NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:  ORACLE **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*

6 □	**DR-NOAM VIP GUI:** Set Failed NOAM Servers to Standby	Navigate to **Main Menu -> Status & Manage -> HA**  Status & Manage Network Elements Server HA Database KPIs Processes Select **Edit** Set the Max Allowed HA Role drop down box to **Standby** for the failed NOAM servers. Select **Ok**
7 □	**RMS NOAM Failure:** Configure BIOS Settings and Update Firmware	If the failed server is **NOT** a rack mount server, **skip to step 11.** 1. Configure and verify the BIOS settings by executing procedure *"Configure the RMS Server BIOS Settings"* from reference [10] 2. Verify and/or upgrade server firmware by executing procedure *"Upgrade Management Server Firmware"* from reference[10] **Note:** Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.
8 □	**RMS NOAM Failure:** Backups Available	If the failed server is **NOT** a rack mount server, **skip to step 11.** This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, **skip this step**. 1. Restore the TVOE backup by executing Appendix H: Restore TVOE Configuration from Backup Media If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing 2. Appendix I: Restore PMAC from Backup

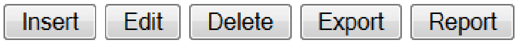
Procedure 5: Recovery Scenario 5

9 □	**Recover Failed Aggregation/ Enclosure Switches, and OAs**	Recover failed OAs, aggregation and enclosure switches if needed. Backups Available: 1. Refer to Appendix B: Recovering/Replacing Failed 3rd Party Components (Switches, OAs)to recover failed OAs, aggregation, and enclosure switches Backups **NOT** Available: 1. Execute section *“HP C-7000 Enclosure Configuration”* 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.
10 □	**RMS NOAM Failure:** Backups **NOT** Available	If the failed server is **NOT** a rack mount server, **skip to step 11.** This step assumes that TVOE and PMAC backups **NOT** are available, if the TVOE and PMAC have already been restored, **skip this step.** If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. Section *“Configure and IPM Management Server”* from reference [10]. 2. Section *“Install PM&C”* from reference [10]. 3. Section *“Configure PM&C”* from reference [10]. If the PMAC is **NOT** located on the same TVOE host as the failed NOAM, Execute the following sections/procedures 1. Section *“Installing TVOE on Rack Mount Server(s)”* from reference [10].
11 □	**HP-Class Blade Failure:** Configure Blade Server iLO, Update Firmware/BIOS Settings	If the failed server is **NOT** an HP C-Class Blade, **skip to step 14.** 1. Execute procedure *“Configure Blade Server iLO Password for Administrator Account”* from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing section *“Server Blades Installation Preparation”* from reference [10]

Procedure 5: Recovery Scenario 5

12 □	**HP-Class Blade Failure:** Backups Available	If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 14.** This step assumes that TVOE backups are available, if backups are **NOT** available, **skip this step**. 1. Install and configure TVOE on failed TVOE blade servers by executing section *"Install TVOE on Blade Servers"* 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.
13 □	**HP-Class Blade Failure:** Backups **NOT** Available	If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 14.** This step assumes that TVOE backups are **NOT** are available 1. Install and configure TVOE on failed TVOE blade servers by executing section *"Install TVOE on Blade Servers"* from reference [10].

14
□
	Execute Fast Deployment File for NOAMs	The backup fdconfig file used during the initial DSR 7.2 installation, this file will be available on the PMAC if a database backup was restored on the PMAC.
		If a backup fast deployment xml is NOT available, execute procedure *"Configure NOAM Servers"* from reference [8].
		If a backup fast deployment xml is already present on the PMAC, execute the following procedure:
		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:
		`$ cd /usr/TKLC/smac/etc`
		`$ screen`
		`$ sudo fdconfig config --file=<Created_FD_File>.xml`

15 □	**DR-NOAM VIP GUI:** Export the Initial Configuration	Navigate to **Main Menu -> Configuration -> Servers.** From the GUI screen, select the Failed NOAM server and then select **Export** to generate the initial configuration data for that server. 

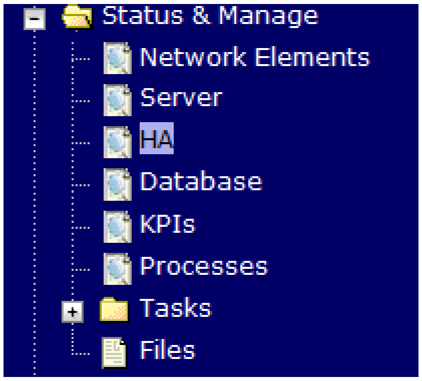
Procedure 5: Recovery Scenario 5

16 □	**DR-NOAM VIP GUI:** Copy Configuration File to Failed NOAM Server	Obtain a terminal session to the DR-NOAM VIP, login as the ***admusr*** user. Execute the following command to configure the failed NOAM server: **`$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<Faile_NOAM_Hostname>.sh admusr@<Failed_NOAM_xmi_IP_address>:/var/tmp/TKLCConfigData.sh`**
17 □	**Recovered NOAM Server:** Verify configuration was called and Reboot the Server	Establish an SSH session to the Recovered NOAM server (Recovered_NOAM_xmi_IP_address) Login as the ***admusr*** user. 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. Verify awpushcfg was called by checking the following file **`$ sudo cat /var/TKLC/appw/logs/Process/install.log`** Verify the following message is displayed: `[SUCCESS] script completed successfully!` Now Reboot the Server: **`$ sudo init 6`** Wait for the server to reboot

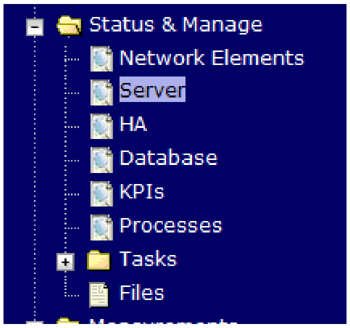
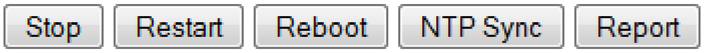
18
□
	Recovered NOAM Server: Configure Networking for Dedicated NetBackup Interface (Optional)	**Note:** You will only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP_Adress> --netmask=<NO2_NetBackup_NetMask>`
		`$ 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>`

Procedure 5: Recovery Scenario 5

19
□
	Recovered NOAM Server: Verify Server Health	Execute the following command on the failed NOAM server and make sure that no errors are returned:
		`$ 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`

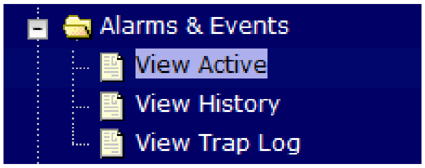
20 □	**Repeat for Additional 2nd Failed NOAM**	Repeat steps 16-19 for the 2nd failed NOAM server.
21 □	**Perform Key exchange between Active NOAM and Recovered NOAMs**	Perform a keyexchange between the newly active NOAM and the recovered NOAM servers: From a terminal window connection on the active NOAM as the ***admusr*** user, exchange SSH keys for ***admusr*** between the active NOAM and the recovered NOAM servers using the keyexchange utility, using the host names of the recovered NOAMs. When prompted for the password, enter the password for the ***admusr*** user of the recovered NOAM servers. **`$ keyexchange admusr@<Recovered_NOAM Hostname>`**
22 □	**NOAM VIP GUI:** Set HA on Recovered NOAMs	Navigate to **Status & Manage -> HA**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click on **Edit** at the bottom of the screen For each NOAM server whose Max Allowed HA Role is set to Standby, set it to **Active** Press **OK**

Procedure 5: Recovery Scenario 5

23 □	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select each recovered NOAM server and click on **Restart**. 
24 □	**Recovered Active NOAM:** Activate Optional Features	**Map-Diameter Interworking (MAP-IWF) and/or Policy and Charging Application (PCA) Only** Establish an SSH session to the recovered active NOAM, login as ***admusr.*** • Refer to [7] to activate Map-Diameter Interworking (MAP-IWF) • Refer to [13] to activate Policy and Charging Application (PCA) **Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: `iload#31000{S/W Fault}`

Procedure 5: Recovery Scenario 5

25
□
	DR-NOAM VIP: Copy key file to recovered NOAM 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)**
		Establish an SSH session to any of the Active DR NOAM which is intact and operational. Login as ***admusr***.
		Execute following commands to check if existing Key file on Active DR NOAM server is valid :
		`$ cd /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo -validate`
		Note: If errors are present, stop and contact **Appendix L: My Oracle Support (MOS)**
		If key file is valid, Execute following commands to copy Key file from Active DR NOAM server to recovered NOAMs :
		`$ ./sharedKrevo -copyKey -destServer <First NOAM>`
		`$ ./sharedKrevo -copyKey -destServer <Second NOAM>`

26 □	**Switch DR NOAM Back to Secondary**	Once the system have been recovered: Execute **Appendix D**: Returning a Recovered Site to Primary to have the recovered NOAM become primary again.
27 □	**Recovered Servers:** Verify Alarms	Navigate to **Main Menu -> Alarms & Events -> View Active**  Alarms & Events View Active View History View Trap Log Verify the recovered servers are not contributing to any active alarms (Replication, Topology misconfiguration, database impairments, NTP, etc.)
28 □	**NOAM VIP GUI:** Recover Standby/Spare SOAM and C-Level Servers	If necessary, refer to Procedure 3 to recover any standby or Spare SOAMs as well as any C-Level servers.

Procedure 5: Recovery Scenario 5

29 □	**NOAM VIP:** Verify all servers in Topology are accessible (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)** Establish an SSH session to the NOAM VIP. Login as ***admusr.*** Execute following commands to check if all the servers in the Topology are accessible : **`$ cd /usr/TKLC/dpi/bin/`** **`$ ./sharedKrevo –checkAccess`** **Note:** If any of the servers are not accessible, stop and Appendix L: My Oracle Support (MOS)
30 □	**NOAM VIP:** Copy key file to all the servers in Topology (RADIUS Only)	Establish an SSH session to the Active NOAM, login as ***admusr***. Execute following command to copy the key file to all the servers in the Topology : **`$ ./sharedKrevo -synchronize`** **`$ ./sharedKrevo -updateData`** **Note:** If errors are present, stop and contact Appendix L: My Oracle Support (MOS)
31 □	**Recover IDIH**	If IDIH were affected, refer to **Section 11** to perform disaster recovery on IDIH.

5.1.6 Recovery Scenario 6 (Database Recovery)

5.1.6.1 Recovery Scenario 6: Case 1

For a partial outage with

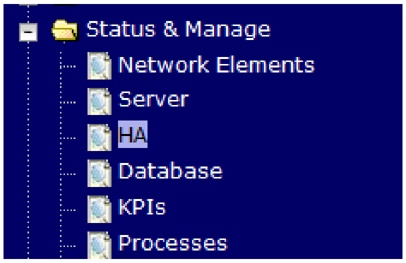
- Server having a corrupted database
- Replication channel from parent is inhibited because of upgrade activity or
- Server is in a different release then that of its Active parent because of upgrade activity.
- Verify that the Server Runtime backup files, performed at the start of the upgrade, are present in /var/TKLC/db/filemgmt area in the following format
    - Backup.DSR.HPC02-NO2.FullDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2
    - Backup.DSR.HPC02-NO2.FullRunEnv.NETWORK_OAMP.20140524_223507.UPG.tar.bz2

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

Procedure 6: Recovery Scenario 6 (Case 1)

S T E P #	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 □	**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)

2 □	**NOAM VIP GUI:** Set Failed Servers to Standby	Navigate to **Main Menu -> Status & Manage -> HA**  Status & Manage Network Elements Server HA Database KPIs Processes Select **Edit** Set the Max Allowed HA Role drop down box to **Standby** for the failed servers. Select **Ok**
3 □	**Server in Question:** Login	Establish an SSH session to the server in question. Login as ***admusr***.
4 □	**Server in Question:** Change runlevel to 3	Execute the following command to bring the system to runlevel 3. `$ sudo init 3`
5 □	**Server in Question:** Recover System	Execute the following command and follow the instructions appearing the console prompt `$ sudo /usr/TKLC/appworks/sbin/backout_restore`
6 □	**Server in Question:** Change runlevel to 4	Execute the following command to bring the system back to runlevel 4. `$ sudo init 6`

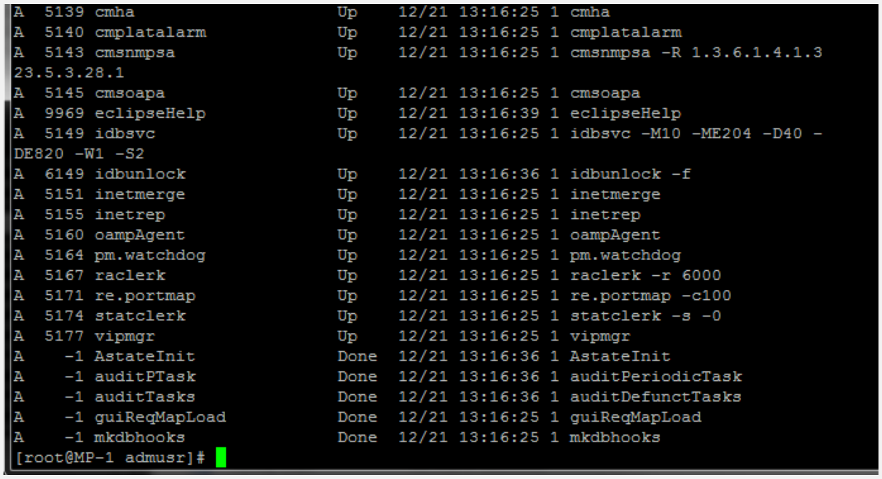
Procedure 6: Recovery Scenario 6 (Case 1)

<table>
<tr>
<td>7
□</td>
<td><b>Server in Question:</b>
Verify the server</td>
<td>

Execute the following command to verify if the processes are up and running

```
$ sudo pm.getprocs
```

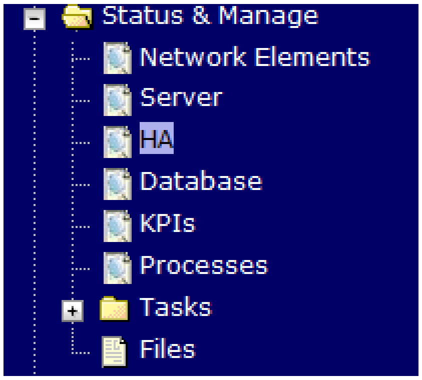
Example Output:



```
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]#
```

</td>
</tr>
<tr>
<td>8
□</td>
<td><b>NOAM VIP GUI:</b>
Set Failed Servers to Active</td>
<td>

Navigate to **Status & Manage -> HA**



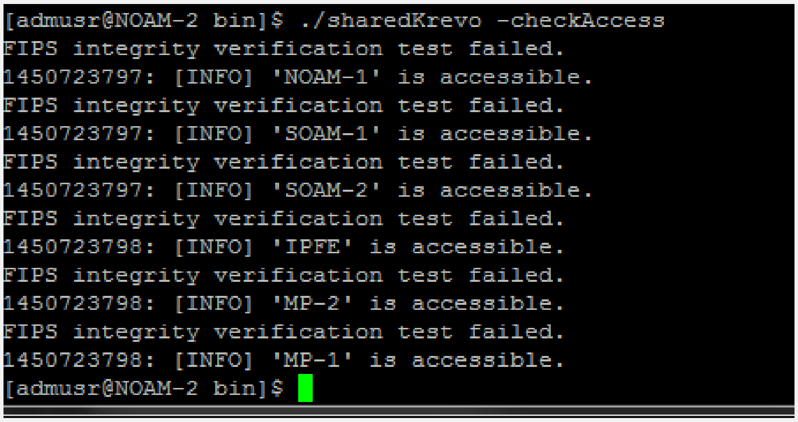
Click on **Edit** at the bottom of the screen

For each failed server whose Max Allowed HA Role is set to Standby, set it to **Active**

Press **OK**

</td>
</tr>
</table>

Procedure 6: Recovery Scenario 6 (Case 1)

9
□
	NOAM VIP: Verify all servers in Topology are accessible (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)**
		Establish an SSH session to the NOAM VIP. Login as ***admusr.***
		Execute following commands to check if all the servers in the Topology are accessible :
		`$ cd /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo –checkAccess`
		
		`[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]$`

Procedure 6: Recovery Scenario 6 (Case 1)

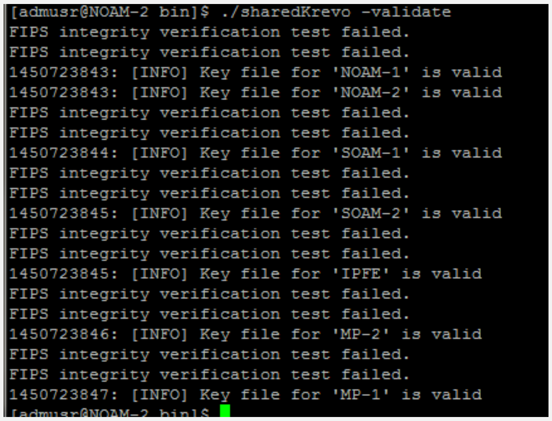
10 □

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 :

```
$ ./sharedKrevo -validate
```

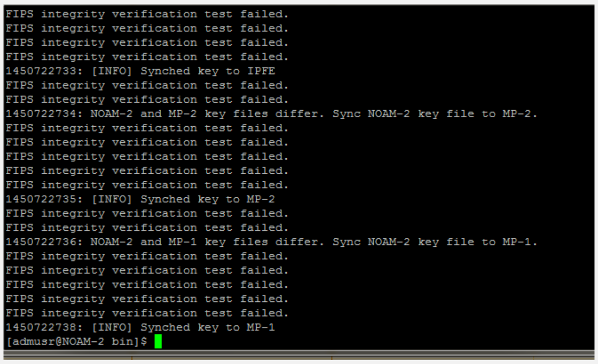


```
[admusr@NOAM-2 bin]$ ./sharedKrevo -validate
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723843: [INFO] Key file for 'NOAM-1' is valid
1450723843: [INFO] Key file for 'NOAM-2' is valid
FIPS integrity verification test failed.
FIPS integrity verification test 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]$
```

If output of above command shows that the existing key file is not valid, contact **Appendix L: My Oracle** Support (MOS)

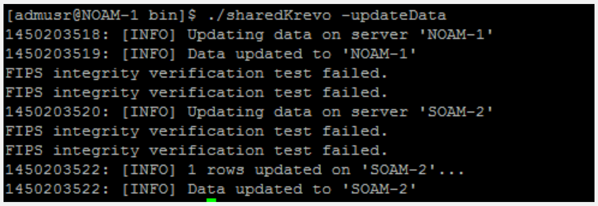
Execute following command to copy the key file to all the servers in the Topology :

```
$ ./sharedKrevo -synchronize
```



```
FIPS integrity verification test failed.
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.
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.
FIPS integrity verification test failed.
1450722738: [INFO] Synched key to MP-1
[admusr@NOAM-2 bin]$
```

```
$ ./sharedKrevo -updateData
```



```
[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'
```

Note: If any errors are present, stop and contact Appendix L: My Oracle Support (MOS)

Procedure 6: Recovery Scenario 6 (Case 1)

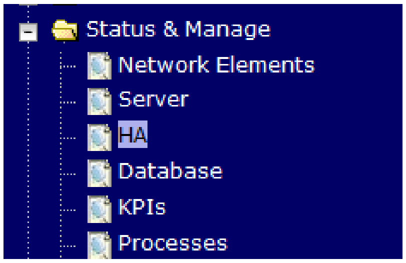
11 □	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**: DSR Database Backup to back up the Configuration databases:

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 #	This procedure performs recovery if database got corrupted in the system and system is in the state to get replicated Check off (√**)** each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix L:** My Oracle Support (MOS) and ask for assistance.	
1 □	**Workarounds**	Refer to **Appendix G**: Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
2 □	**NOAM VIP GUI:** Set Failed Servers to Standby	Navigate to **Main Menu -> Status & Manage -> HA**  Status & Manage Network Elements Server HA Database KPIs Processes Select **Edit** Set the Max Allowed HA Role drop down box to **Standby** for the failed servers. Select **Ok**

Procedure 7: Recovery Scenario 6 (Case 2)

3 □	**Server in Question:** Login	Establish an SSH session to the server in question. Login as ***admusr***.

4
□
	Server in Question: Take Server out of Service	Execute the following command to take the server out of service.
		`$ sudo bash –l`
		`$ prod.clobber`

5
□
	Server in Question: Take Server to DbUp State and Start the Application	Execute the following commands to take the server to Dbup and start the DSR application:
		`$ prod.start`
		Exit out of root:
		`$ exit`

Procedure 7: Recovery Scenario 6 (Case 2)

6

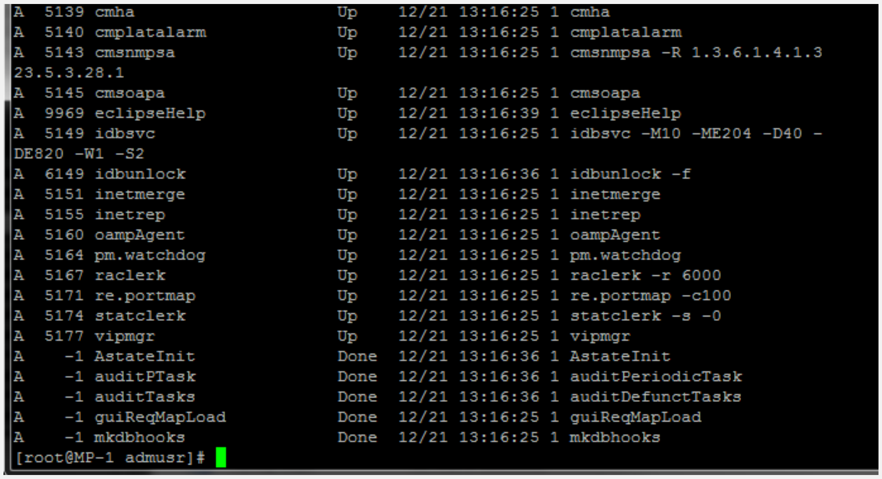
□

Server in Question: Verify the Server State

Execute the following commands to verify the processes are up and running:

```
$ sudo pm.getprocs
```

Example Output:

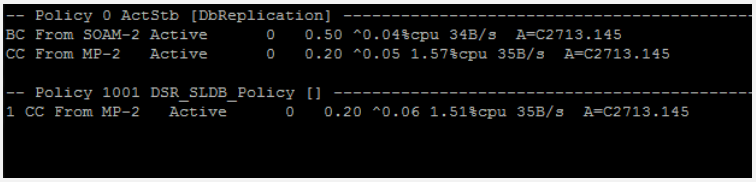


```
A  5139 cmha                   Up    12/21 13:16:25 1 cmha
A  5140 cmplatalarm            Up    12/21 13:16:25 1 cmplatalarm
A  5143 cmsnmpsa               Up    12/21 13:16:25 1 cmsnmpsa -R 1.3.6.1.4.1.3
23.5.3.28.1
A  5145 cmsoapa                Up    12/21 13:16:25 1 cmsoapa
A  9969 eclipseHelp            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]#
```

Execute the following command to verify if replication channels are up and running:

```
$ sudo irepstat
```

Example Output:

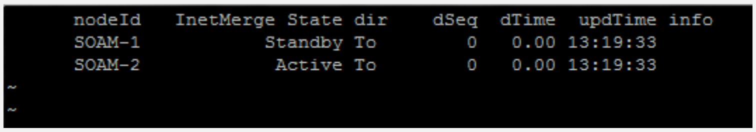


```
-- Policy 0 ActStb [DbReplication] ------------------------------------------
BC From SOAM-2 Active      0   0.50 ^0.04%cpu 34B/s  A=C2713.145
CC From MP-2   Active      0   0.20 ^0.05 1.57%cpu 35B/s  A=C2713.145

-- Policy 1001 DSR_SLDB_Policy [] -------------------------------------------
1 CC From MP-2   Active      0   0.20 ^0.06 1.51%cpu 35B/s  A=C2713.145
```

Execute the following command to verify if merging channels are up and running:

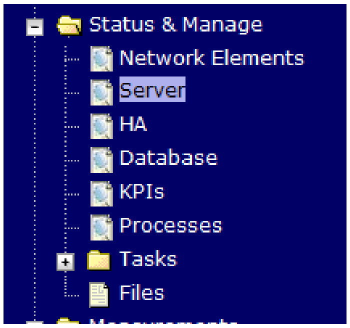
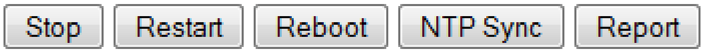
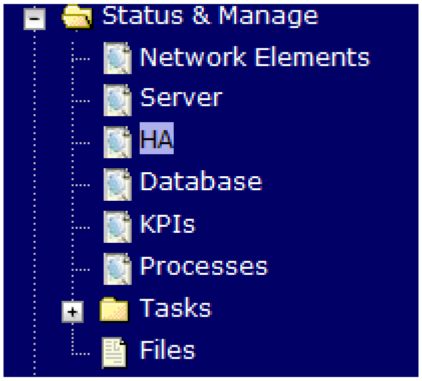
```
$ sudo inetmstat
```

Example Output:



```
       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
~
~
```

Procedure 7: Recovery Scenario 6 (Case 2)

7 □	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select each recovered server and click on **Restart**. 
8 □	**NOAM VIP GUI:** Set Failed Servers to Active	Navigate to **Status & Manage -> HA**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click on **Edit** at the bottom of the screen For each failed server whose Max Allowed HA Role is set to Standby, set it to **Active** Press **OK**

9
□
	NOAM VIP: Verify all servers in Topology are accessible (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)**
		Establish an SSH session to the NOAM VIP. Login as ***admusr.***
		Execute following commands to check if all the servers in the Topology are accessible :
		`$ cd /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo -checkAccess`

Procedure 7: Recovery Scenario 6 (Case 2)

<table>
<tr>
<td>10
□</td>
<td><b>NOAM VIP:</b> Copy key file to all the servers in Topology (RADIUS Only)</td>
<td>

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)

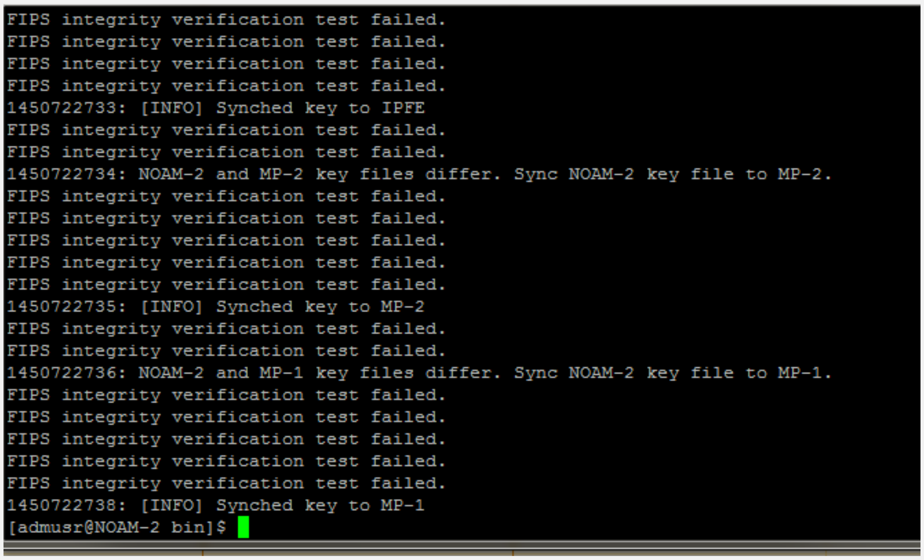
Execute following commands to check if existing Key file on Active NOAM (The NOAM which is intact and was not recovered) server is valid :

```
$ cd /usr/TKLC/dpi/bin/
$ ./sharedKrevo -validate
```

If output of above command shows that the existing key file is not valid, contact **Appendix L: My Oracle** Support (MOS)

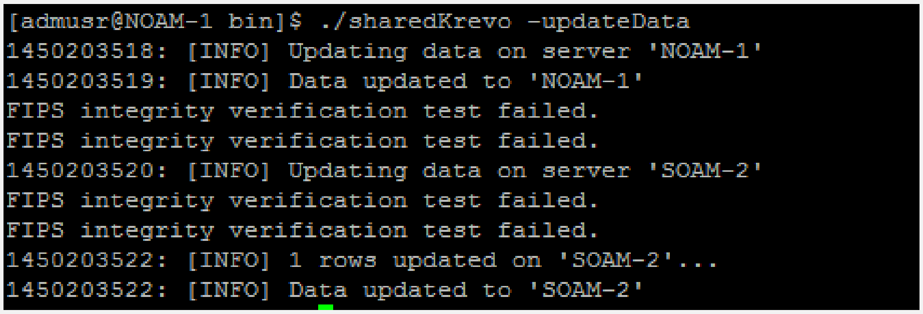
Execute following command to copy the key file to all the servers in the Topology :

```
$ ./sharedKrevo -synchronize
```



```
FIPS integrity verification test failed.
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.
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.
FIPS integrity verification test failed.
1450722738: [INFO] Synched key to MP-1
[admusr@NOAM-2 bin]$
```

```
$ ./sharedKrevo -updateData
```



```
[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'
```

Note: If any errors are present, stop and contact Appendix L: My Oracle Support (MOS)

</td>
</tr>
</table>

Procedure 7: Recovery Scenario 6 (Case 2)

12 □	**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.

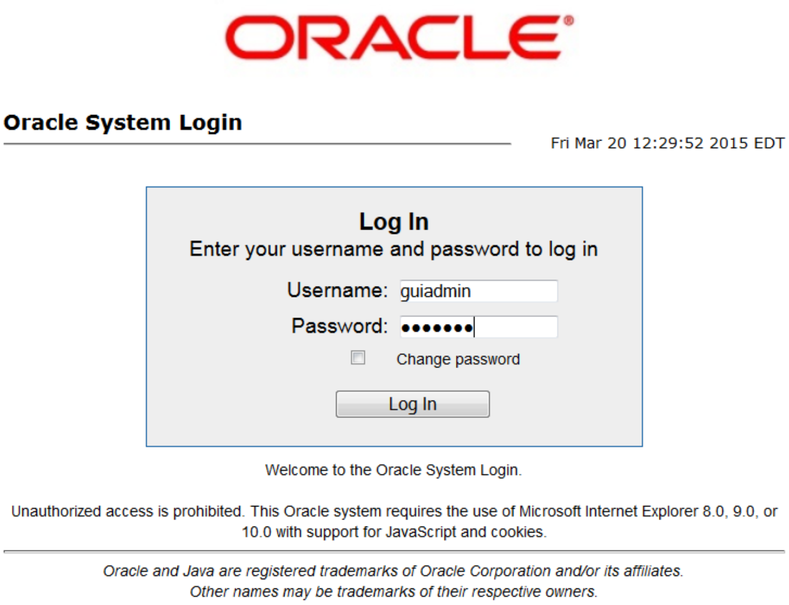
6.1 Restoring a Deleted User

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

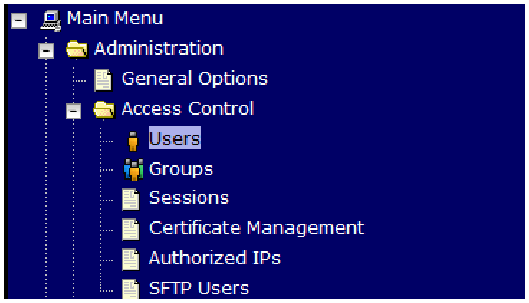
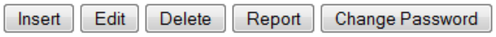
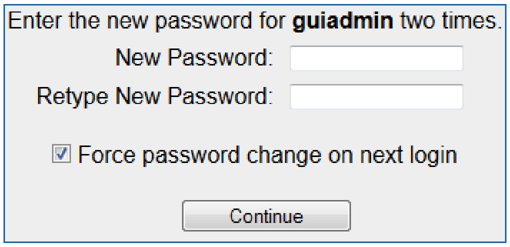
These users were removed prior to creation of the backup and archive file. They will be reintroduced by system restoration of that file.

6.2 Keeping a Restored user

Procedure 8: Keep Restored User

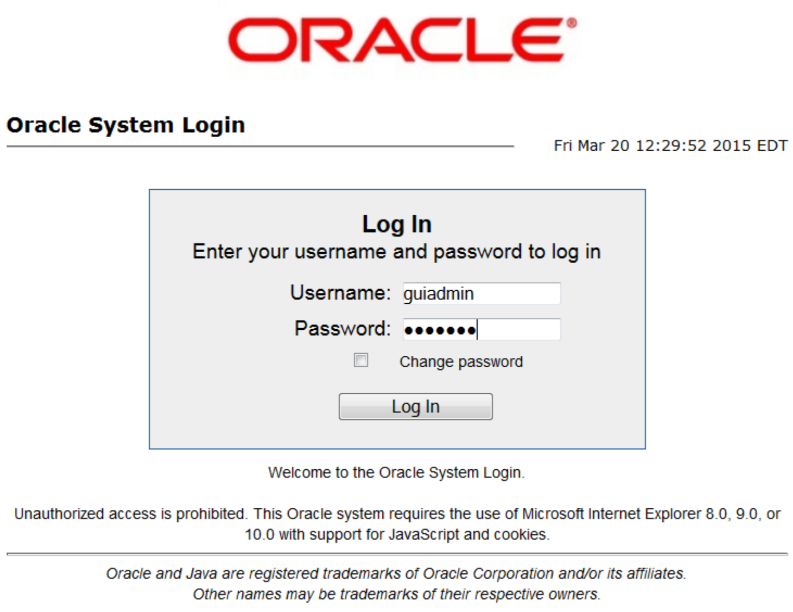
S T E P #	Perform this procedure to keep users that will be restored by system restoration. Check off (√**)** each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix L:** My Oracle Support (MOS) and ask for assistance.	
1 □	**Before Restoration:** Notify Affected Users Before Restoration	Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.
2 □	**After Restoration:** Login to the NOAM VIP	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:  ORACLE® **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*

Procedure 8: Keep Restored User

3 □	**After Restoration:** Reset User Passwords	Navigate to **Administration -> Access Control -> Users**  Main Menu Administration General Options Access Control Users Groups Sessions Certificate Management Authorized IPs SFTP Users Select the user Click the **Change Password** button  Enter a new password  Enter the new password for **guiadmin** two times. New Password: Retype New Password: ☑ Force password change on next login Click the **Continue** button

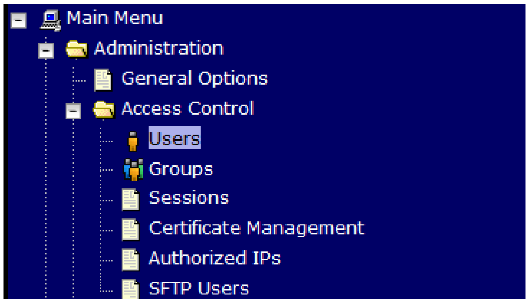
6.3 Removing a Restored User

Procedure 9: Remove the Restored User

S **T** **E** **P** **#**	Perform this procedure to remove users that will be restored by system restoration Check off (√**)** each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix L:** My Oracle Support (MOS) and ask for assistance.	
1 □	**After Restoration:** Login to the NOAM VIP	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_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: guiadmin Password: ••••••• □ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*

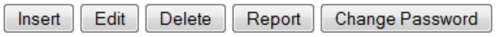
Procedure 9: Remove the Restored User

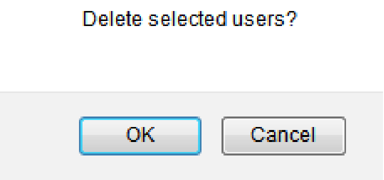
<table>
<tr>
<td>2
□</td>
<td><b>After Restoration:</b>
Reset User Passwords</td>
<td>
Navigate to <b>Administration -> Access Control -> Users</b>



Select the user

Click the <b>Delete</b> button





Delete selected users?

Click the <b>OK</b> button to confirm.
</td>
</tr>
</table>

6.4 Restoring a Modified User

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

```
- The password for user 'testuser' differs between the selected backup file
and the current database.
```

Before Restoration:

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

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

After Restoration:

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

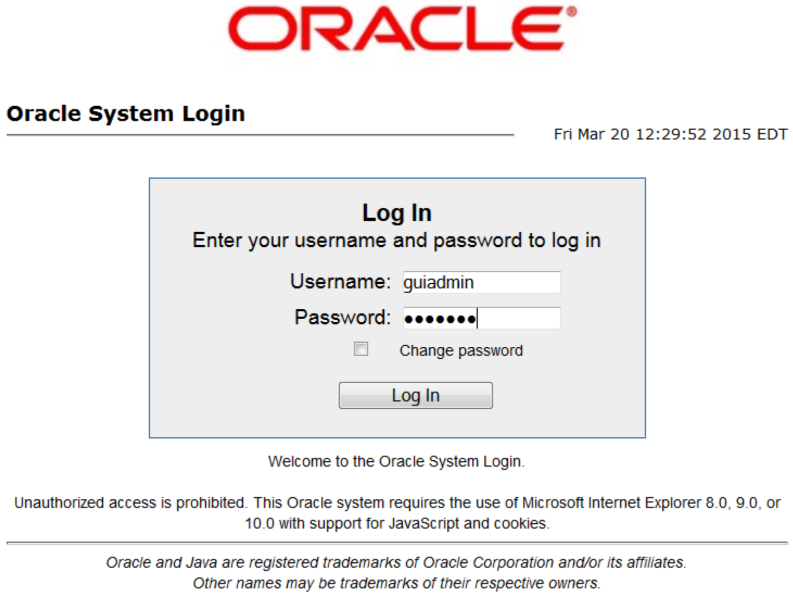
6.5 Restoring an Archive that does not contain a Current User

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

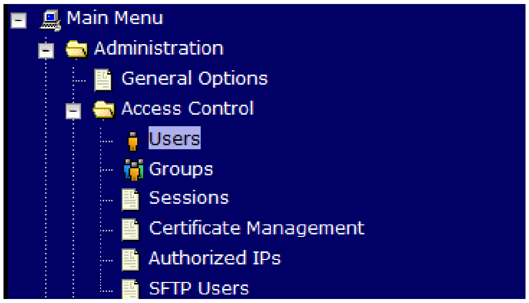
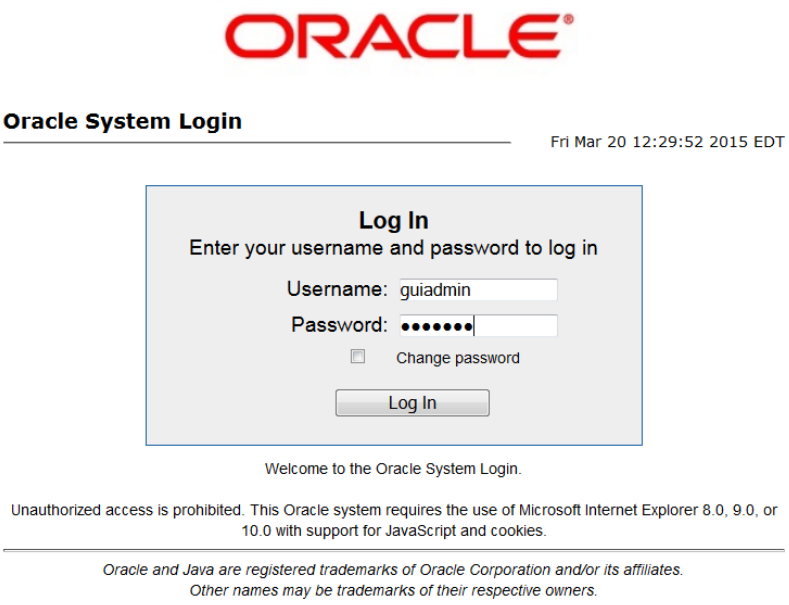
```
- User 'testuser' exists in current database but not in the selected backup
file.
```

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

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

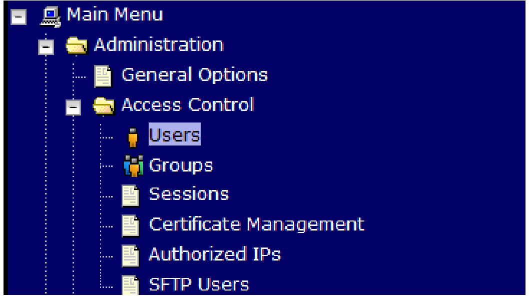
STEP #	Perform this procedure to remove users that will be restored by system restoration Check off (√**)** each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix L:** My Oracle Support (MOS) and ask for assistance.	
1 □	**Before Restoration:** Notify Affected Users Before Restoration	Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.
2 □	**Before Restoration:** Login to the NOAM VIP	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_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: guiadmin 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 10: Restoring an Archive that does not Contain a Current User

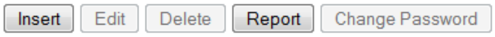
3 □	**Before Restoration:** Record user settings	Navigate to **Administration -> Access Control -> Users**  Main Menu Administration General Options Access Control Users Groups Sessions Certificate Management Authorized IPs SFTP Users Under each affected user, record the following: • Username, • Account status • Remote Auth • Local Auth • Concurrent Logins Allowed • Inactivity Limit • Comment • Groups
4 □	**After Restoration:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:  **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ••••••• ☐ Change password Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*

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

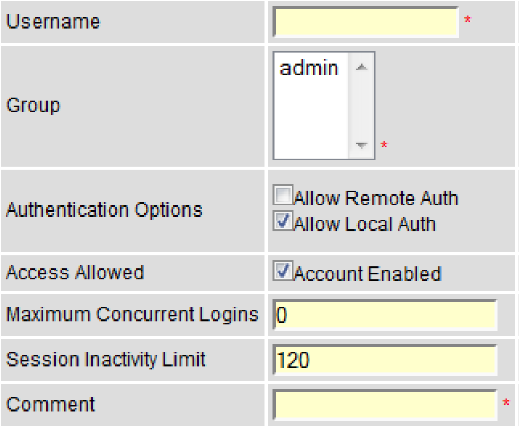
<table>
<tr>
<td>5
□</td>
<td><b>After Restoration:</b> Recreate affected user</td>
<td>
Navigate to <b>Administration -> Access Control -> Users</b>



Click <b>Insert</b>

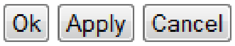


Recreate the user using the data collected in <b>Step 3.</b>



Username: *
Group: admin *
Authentication Options: ☐ Allow Remote Auth ☑ Allow Local Auth
Access Allowed: ☑ Account Enabled
Maximum Concurrent Logins: 0
Session Inactivity Limit: 120
Comment: *

Click <b>Ok</b>



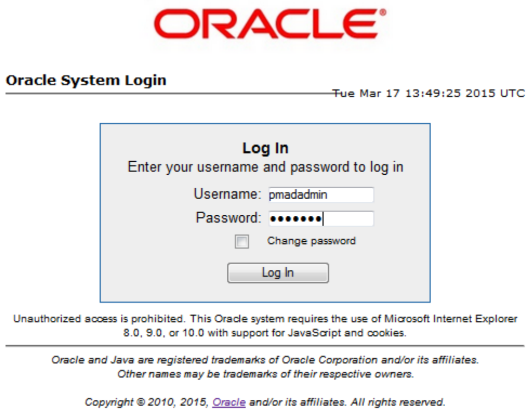
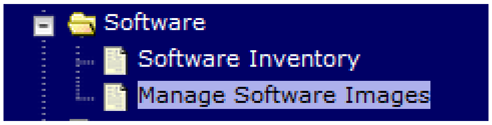
</td>
</tr>
<tr>
<td>6
□</td>
<td><b>After Restoration:</b> Repeat for Additional Users</td>
<td>Repeat <b>Step 5</b> to recreate additional users.</td>
</tr>
<tr>
<td>7
□</td>
<td><b>After Restoration:</b> Reset the Passwords</td>
<td>See <b>Procedure 8</b> for resetting passwords for a user.</td>
</tr>
</table>

11. 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

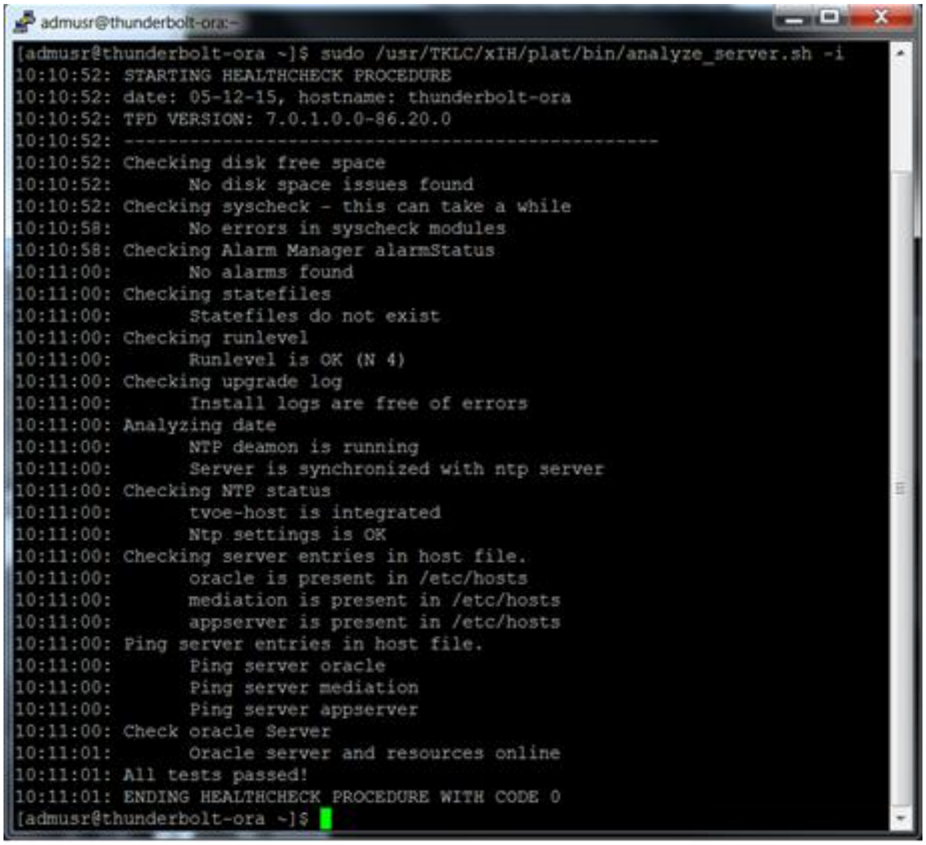
S **T** **E** **P** **#**	This procedure performs disaster recovery preparation steps for the IDIH. Check off (√**)** each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix L:** My Oracle Support (MOS) and ask for assistance.	
1 □	**PMAC GUI:** Login	Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` Login as ***pmacadmin*** user:  Oracle System Login Tue Mar 17 13:49:25 2015 UTC Log In Enter your username and password to log in Username: pmadadmin Password: ••••••• ☐ Change password Log In Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Copyright © 2010, 2015, Oracle and/or its affiliates. All rights reserved.
2 □	**PMAC GUI:** Verify necessary IDIH images are available	Navigate to **Main Menu -> Software -> Manage Software Images**  Verify the current IDIH **TVOE**, **TPD**, **Oracle**, **Application** and **Mediation** images are listed. **Note:** If the necessary software images are not available please follow the instructions from [8] to acquire and transfer the images.

Procedure 11: IDIH Disaster Recovery Preparation

<table>
<tr>
<td>3
□</td>
<td><b>Oracle Guest:</b>
Login</td>
<td>Establish an SSH session to the Oracle guest, login as <b><i>admusr</i></b>.</td>
</tr>
<tr>
<td>4
□</td>
<td><b>Oracle Guest:</b>
Perform Database Health check</td>
<td>Execute the following command to perform a database health check:

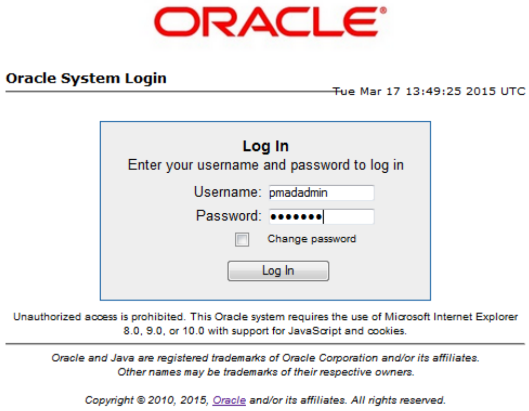
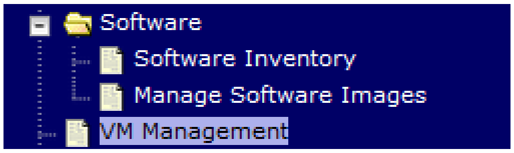
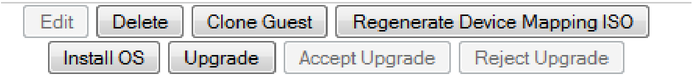
<pre>
$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i
</pre>

Output:

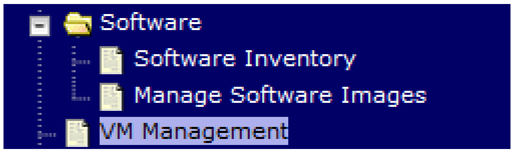
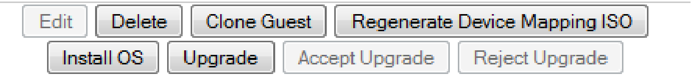


<pre>
[admusr@thunderbolt-ora ~]$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i
10:10:52: STARTING HEALTHCHECK PROCEDURE
10:10:52: date: 05-12-15, hostname: thunderbolt-ora
10:10:52: TPD VERSION: 7.0.1.0.0-86.20.0
10:10:52: ---
10:10:52: Checking disk free space
10:10:52:   No disk space issues found
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 deamon 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>
</td>
</tr>
</table>

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

STEP #	This procedure performs disaster recovery for the IDIH by re-installing the mediation and application servers. 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 □	**PMAC GUI:** Login	Open web browser and enter: **`http://<PMAC_Mgmt_Network_IP>`** Login as ***pmacadmin*** user:  Oracle System Login Tue Mar 17 13:49:25 2015 UTC Log In Enter your username and password to log in Username: pmadadmin Password: ••••••• □ Change password Log In Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2015, Oracle and/or its affiliates. All rights reserved.*
2 □	**Remove existing Application Server**	Navigate to **Main Menu -> VM Management**  Software Software Inventory Manage Software Images VM Management Select the application guest, Click on the **Delete** button.  Edit Delete Clone Guest Regenerate Device Mapping ISO Install OS Upgrade Accept Upgrade Reject Upgrade

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

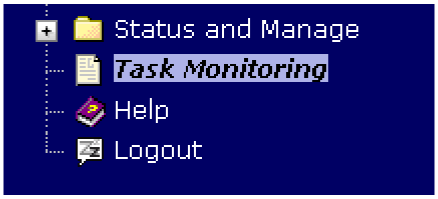
<table>
<tr><td>3
□</td><td><b>Remove existing Mediation Server</b></td><td>Navigate to <b>Main Menu -> VM Management</b>

Select the Mediation guest,
Click on the <b>Delete</b> button.
 </td></tr>
<tr><td>4
□</td><td><b>PMAC:</b> Establish SSH session and Login</td><td>Establish an SSH session to the PMAC, login as <b><i>admusr</i></b>.</td></tr>
<tr><td>5
□</td><td><b>PMAC:</b> Re-install the Mediation and Application Servers</td><td>Execute the following command (Enter your upgrade file) :<pre>
$ cd /var/TKLC/smac/guest-dropin

$ sudo fdconfig config –file=<hostname-upgrade_xx-xx-
xx>.xml
</pre><b>Warning:</b> 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.</td></tr>
</table>

<table>
<tr>
<td>6
□</td>
<td><b>PMAC GUI:</b> Monitor the Configuration</td>
<td>

If not already done so, establish a GUI session on the PMAC server.

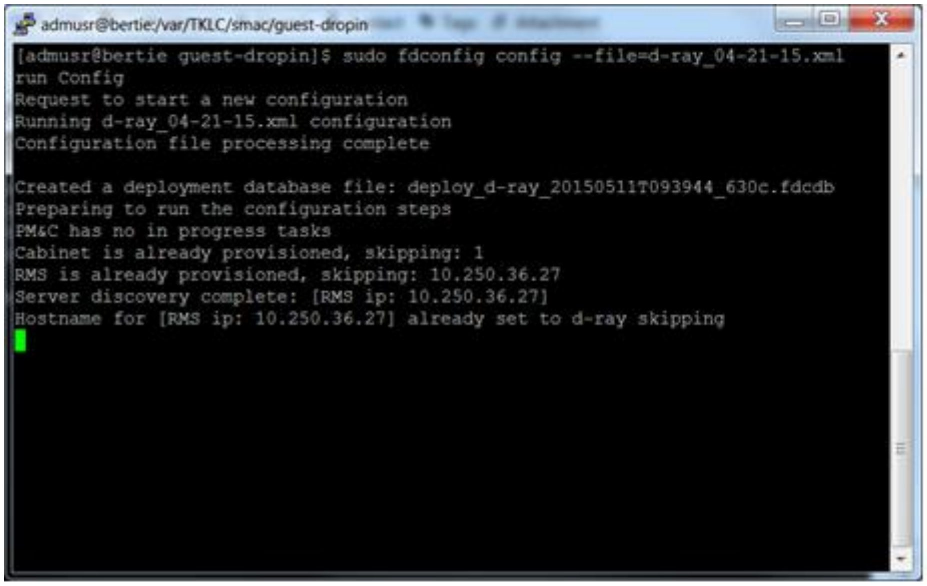
Navigate to **Main Menu -> Task Monitoring**



Monitor the IDIH configuration to completion.

Alternatively, you can monitor the fdconfig status through the command line after executing the fdconfig command:

Example:

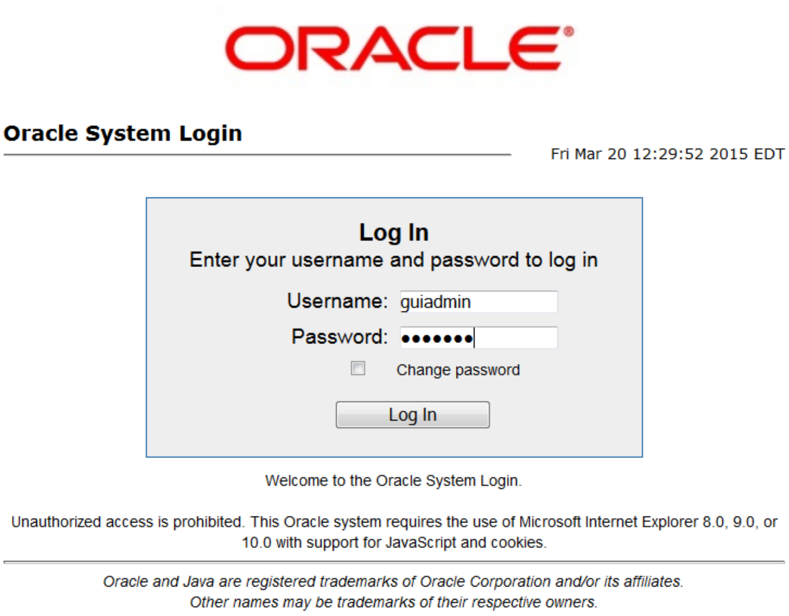


```
admusr@bertie:/var/TKLC/smac/guest-dropin
[admusr@bertie guest-dropin]$ sudo fdconfig config --file=d-ray_04-21-15.xml
run Config
Request to start a new configuration
Running d-ray_04-21-15.xml configuration
Configuration file processing complete

Created a deployment database file: deploy_d-ray_20150511T093944_630c.fdcdb
Preparing to run the configuration steps
PM&C has no in progress tasks
Cabinet is already provisioned, skipping: 1
RMS is already provisioned, skipping: 10.250.36.27
Server discovery complete: [RMS ip: 10.250.36.27]
Hostname for [RMS ip: 10.250.36.27] already set to d-ray skipping
```

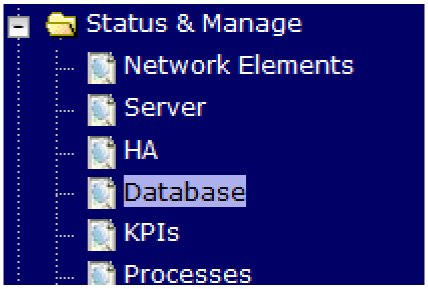
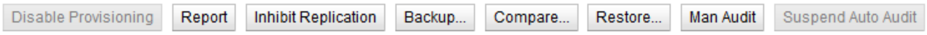
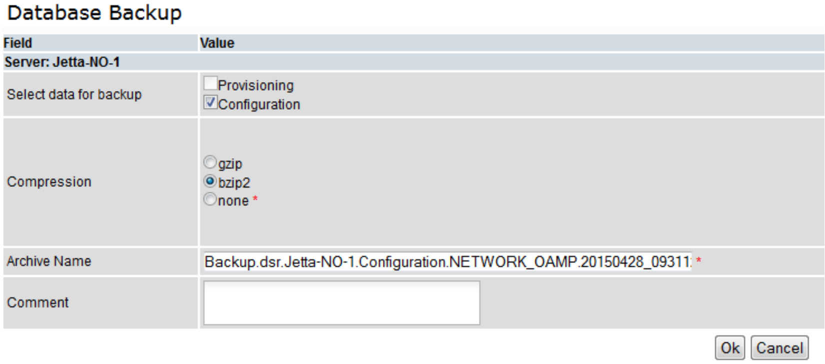
</td>
</tr>
</table>

Appendix A: DSR Database Backup

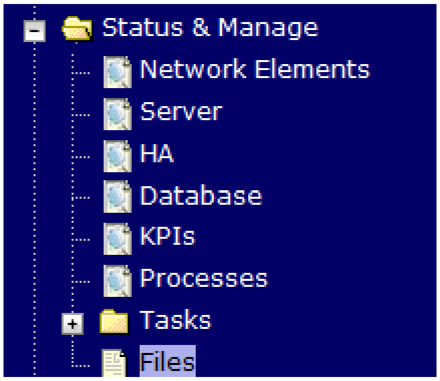
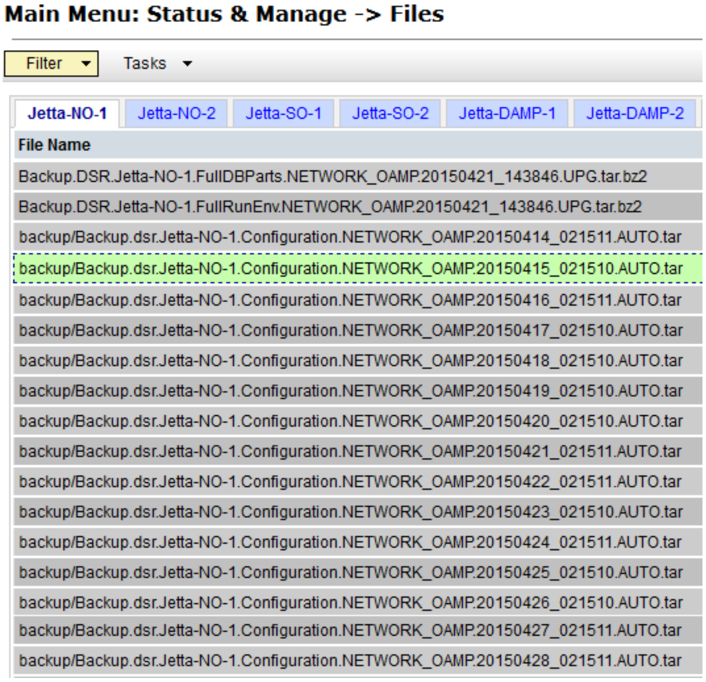
Procedure 13: DSR Database Backup

S T E 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 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 □	**NOAM/SOAM VIP:** Login	Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM/SOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:  Oracle System Login Fri Mar 20 12:29:52 2015 EDT Log In Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password 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.*

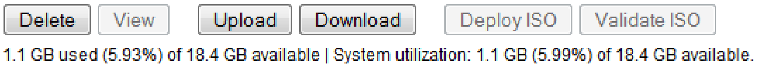
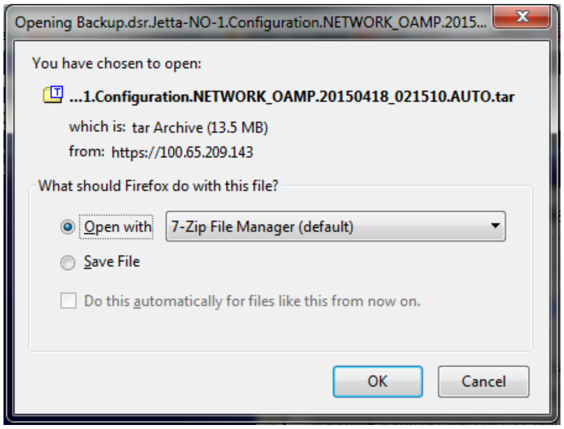
Procedure 13: DSR Database Backup

2 □	**NOAM/SOAM VIP:** Backup Configuration Data for the System	Navigate to **Main Menu -> Status & Manage -> Database**  Status & Manage Network Elements Server HA Database KPIs Processes Select the Active NOAM Server and Click on **Backup** button  Disable Provisioning Report Inhibit Replication Backup... Compare... Restore... Man Audit Suspend Auto Audit Make sure that the checkboxes next to “Configuration” is checked.  Database Backup Field Value Server: Jetta-NO-1 Select data for backup ☐ Provisioning ☑ Configuration Compression ○ gzip ● bzip2 ○ none * Archive Name Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150428_09311 * Comment Ok Cancel Enter a filename for the backup and press **OK**

Procedure 13: DSR Database Backup

3 □	**NOAM/SOAM VIP:** Verify the backup file existence.	Navigate to **Main Menu -> Status & Manage -> Files**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Main Menu: Status & Manage -> Files Filter Tasks Jetta-NO-1 Jetta-NO-2 Jetta-SO-1 Jetta-SO-2 Jetta-DAMP-1 Jetta-DAMP-2 File Name Backup.DSR.Jetta-NO-1.FullDBParts.NETWORK_OAMP.20150421_143846.UPG.tar.bz2 Backup.DSR.Jetta-NO-1.FullRunEnv.NETWORK_OAMP.20150421_143846.UPG.tar.bz2 backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150414_021511.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150415_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150416_021511.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150417_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150418_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150419_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150420_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150421_021511.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150422_021511.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150423_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150424_021511.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150425_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150426_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150427_021511.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150428_021511.AUTO.tar 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

4 □	**NOAM/SOAM VIP:** Download the file to a local machine.	From the previous step, choose the backup file. Select the **Download** button  Delete View Upload Download Deploy ISO Validate ISO 1.1 GB used (5.93%) of 18.4 GB available | System utilization: 1.1 GB (5.99%) of 18.4 GB available. Select **OK** to confirm the download.  Opening Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.2015... You have chosen to open: ...1.Configuration.NETWORK_OAMP.20150418_021510.AUTO.tar which is: tar Archive (13.5 MB) from: https://100.65.209.143 What should Firefox do with this file? ● Open with 7-Zip File Manager (default) ○ Save File □ Do this automatically for files like this from now on.
5 □	**Upload the Image to Secure Location**	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.
6 □	**Backup Active SOAM**	Repeat **Steps 2 through 5** to back up the Active SOAM

Procedure 13: DSR Database Backup

7
□
	Take Secured backup of 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)**
		Login to ssh shell of Active NOAM server using user admusr
		Take secure backup of updated key file “RADIUS shared secret encryption key” for disaster scenarios.
		Execute following command to encrypt the key file before being backed up to secure customer setup :
		`$ ./sharedKrevo -encr`
		Execute following command to copy the encrypted key file to secure customer setup :
		`$ sudo scp /var/TKLC/db/filemgmt/DpiKf.bin.encr  user@<customer IP>:<path of customer setup>`
		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

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 #	The intent of this procedure is to recover a failed Aggregation (4948E / 4948E-F) Switch. Prerequisites for this procedure are: • A copy of the networking xml configuration files • A copy of HP Misc Firmware DVD or ISO • IP address and hostname of the failed switch • Rack Mount position of the failed switch Check off (√***)*** each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix L:** My Oracle Support (MOS) and ask for assistance.	
1 □	**Recover failed Aggregation Switches:** Cisco 4948E/4948E-F	Login to the PMAC via SSH as ***admusr*** Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell: `sudo ssh-keygen -R <4948_switch_ip>` Refer to procedure *"Replace a failed 4948/4948E/4948E-F switch (c-Class s*ystem) (netConfig)" to replace a failed Aggregation switch from reference [2] **Note:** You will need a copy of the HP Misc Firmware DVD or ISO *(or firmware file obtained from the appropriate hardware vendor)* and of the original networking xml files custom for this installation. These will either be stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.

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

<table>
<tr><td><b>S
T
E
P
#</b></td><td colspan="2">The intent of this procedure is to recover a failed Enclosure (3020) Switch.

Prerequisites for this procedure are:
• A copy of the networking xml configuration files
• A copy of HP Misc Firmware DVD or ISO
• IP address and hostname of the failed switch
• Interconnect Bay position of the enclosure switch

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

If this procedure fails, contact <b>Appendix L:</b> My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1
□</td><td><b>Recover failed Enclosure Switch:</b> Cisco 3020</td><td>Login to the PMAC via SSH as <b><i>admusr</i></b>

Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell:

<b>sudo ssh-keygen -R <enclosure_switch_ip></b>

Refer to procedure <i>“Reconfigure a failed 3020 switch (netConfig)”</i> to replace the failed enclosure switch from reference [2]

<b>Note:</b> 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.</td></tr>
</table>

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

S T E P #	The intent of this procedure is to recover a failed Enclosure (6120XG) Switch. Prerequisites for this procedure are: • A copy of the networking xml configuration files • IP address and hostname of the failed switch • Interconnect Bay position of the enclosure switch Check off (√***)*** each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix L:** My Oracle Support (MOS) and ask for assistance.	
1 □	**Recover failed Enclosure Switch:** HP 6120XG	Login to the PMAC via SSH as ***admusr*** Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell: `sudo ssh-keygen -R <enclosure_switch_ip>` Refer to procedure *"Reconfigure a failed HP 6120XG switch (netConfig)"* to replace the failed enclosure switch from reference [2]**.** **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.

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

STEP #	The intent of this procedure is to recover a failed Enclosure (6125XLG/6125G) Switch. Prerequisites for this procedure are: • A copy of the networking xml configuration files Check off (√**)** each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix L:** My Oracle Support (MOS) and ask for assistance.	
1 □	**Recover failed Enclosure Switch:** HP 6125XLG/6125G	Login to the PMAC via SSH as ***admusr*** Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell: **`sudo ssh-keygen -R <enclosure_switch_ip>`** Refer to procedure *“Reconfigure a failed HP 6125XG, 6125XLG switch (netConfig)”* to replace the failed enclosure switch from reference [2]**.** **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.

Procedure 18: Recovering a Failed Enclosure OA

S T E P #	The intent of this procedure is to recover a failed Enclosure Onboard Administrator. Check off (√***)*** each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix L:** My Oracle Support (MOS) and ask for assistance.	
1 □	Recover Failed Enclosure OA	Refer to procedure *“Restore OA Configuration from Management Server”* to replace a failed Enclosure OA from reference [2]**.**

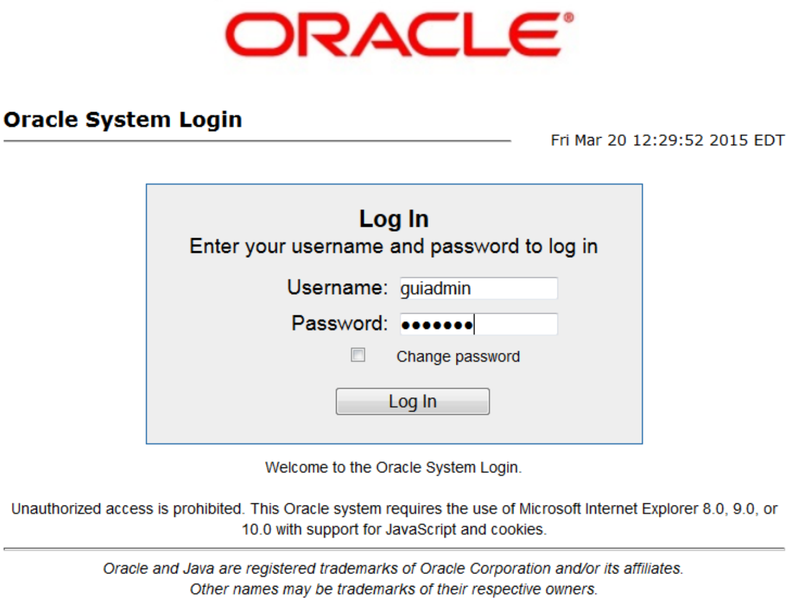
Appendix C: Switching DR NOAM Site to Primary

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.

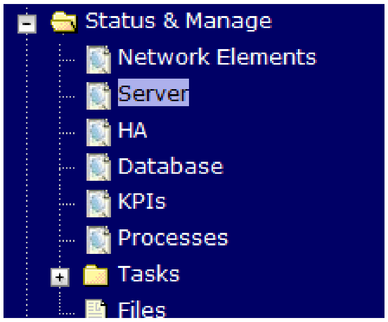
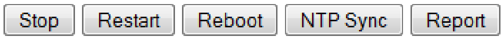
Preconditions:

- 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 19: Switching a DR NOAM Site to Primary

S **T** **E** **P** **#**	The intent of this procedure is to switch a DR site to Primary. 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 □	**Active DR-NOAM:** Login	Establish a GUI session on the active DR-NOAM server by using the xmi IP address of the DR-NOAM. Open the web browser and enter a URL of: `http://<Primary_DR_NOAM_VIP_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: guiadmin 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 19: Switching a DR NOAM Site to Primary

2 □	**Active DR-NOAM:** Disable DSR Application on DR-NOAM Servers	Navigate to **Main Menu -> Status & Manage -> Server**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the row that has the Active DR-NOAM server. Select the **Stop** button. 
4 □	**DR-NOAM:** Repeat	Repeat **steps 1-2** to disable the DSR application on the standby DR NOAM. Note: The DSR application should now be stopped on all DR-NOAMs.
5 □	**DR-NOAM:** Verify DSR application is stopped.	Verify that **"PROC"** column on both DR DSR servers show **"Man"** indicating that application is manually stopped
6 □	**Primary DR-NOAM:** Establish an SSH session	Login via SSH to the physical IP of the chosen primary DR-NOAM server as ***admusr*** user.

Procedure 19: Switching a DR NOAM Site to Primary

7 □ **Primary DR-NOAM:** Change Role to Primary

Execute the command

```
$ sudo top.setPrimary
```

Note: This step makes the DR DSR take over as the Primary.

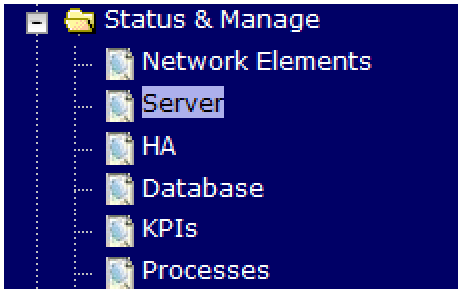
Execute the following command to verify the role was changed to primary:

```
$ sudo top.myrole

myNodeId=A1250.248
myMasterCapable=true
myMateNodeId=A1250.249
myParentCluster=00000
myClusterRole=Primary
myClusterTimestamp=02/26/16 09:35:58.922
```

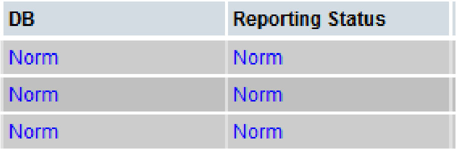
System generates several replication and collection alarms as replication/collection links to/from former Primary NOAM servers becomes inactive.

8 □ **Primary DR-NOAM:** Verify Replication

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

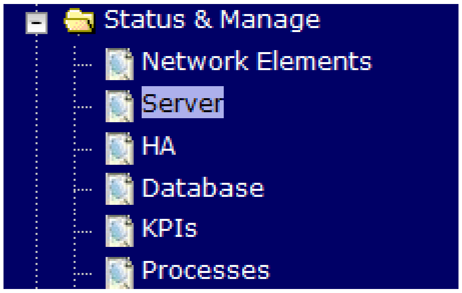
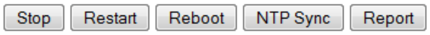
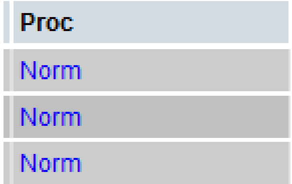


It may take several minutes for replication; afterward the **"DB"** and **"Reporting Status"** columns should show **"Normal"**.



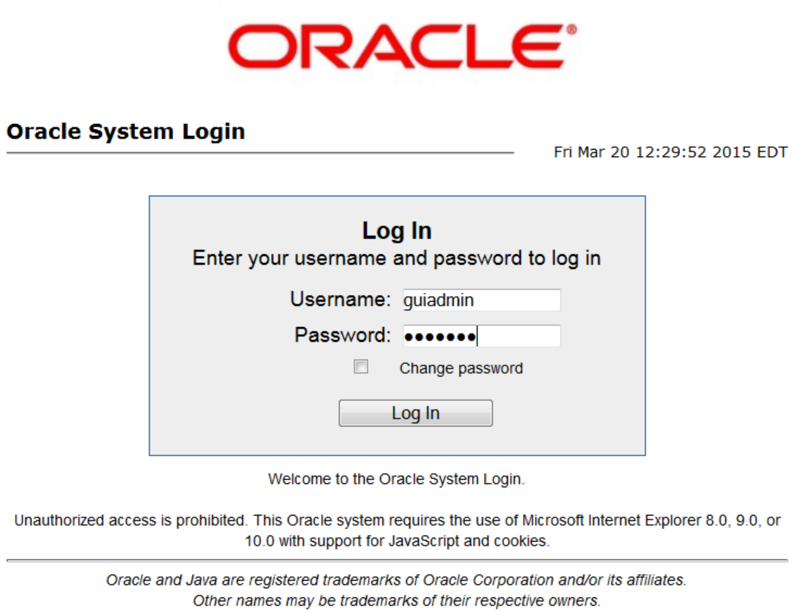
DB	Reporting Status
Norm	Norm
Norm	Norm
Norm	Norm

Procedure 19: Switching a DR NOAM Site to Primary

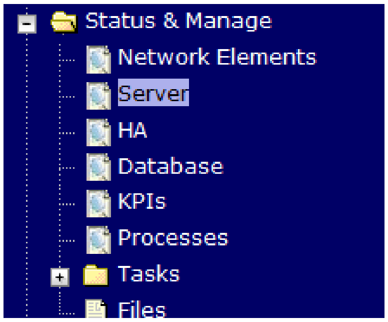
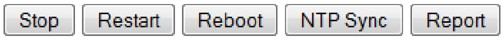
9 □	**New Primary NOAM:** Re-enable the application.	Navigate to **Main Menu -> Status & Manage -> Server**  Status & Manage Network Elements Server HA Database KPIs Processes Select the row that has the active New-Primary NOAM server. Click the **Restart** button and then click the OK button.  Verify that **"PROC"** column now shows "Norm".  Proc Norm Norm Norm Provisioning can now resume to the VIP of the new-Primary DSR.
10 □	**New Primary NOAM:** Repeat for standby of new-primary NOAM Server	Repeat **steps 8-9** for standby of the new-Primary NOAM server.

Appendix D: Returning a Recovered Site to Primary

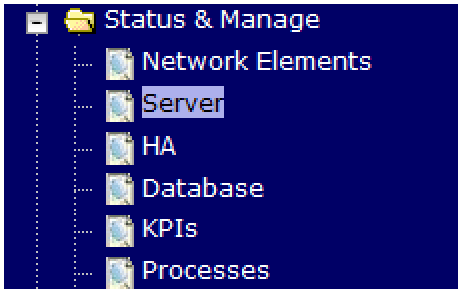
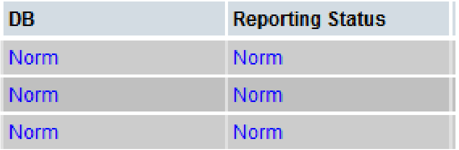
Procedure 20: Returning a Recovered Site to Primary

S **T** **E** **P** **#**	The intent of this procedure is to return a recovered site to primary. 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 □	**Primary Active NOAM:** Login	Establish a GUI session on the primary NOAM server by using the VIP IP address of the primary NOAM. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:  Oracle System Login Fri Mar 20 12:29:52 2015 EDT Log In Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password Log In Welcome to the Oracle System Login. Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.* *Other names may be trademarks of their respective owners.*

Procedure 20: Returning a Recovered Site to Primary

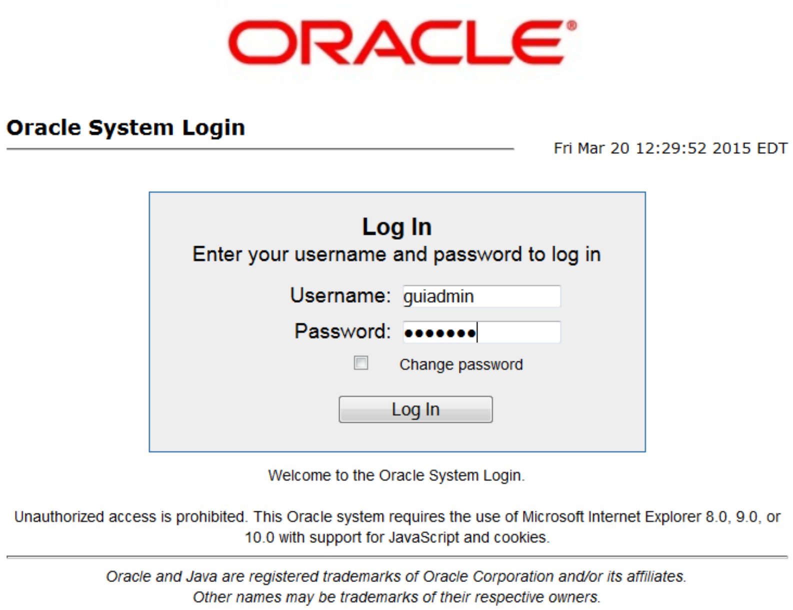
2 □	**Primary Active NOAM:** Disable DSR Application on DR-NOAM Servers	Navigate to **Main Menu -> Status & Manage -> Server**  Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the row that has the Active DR-NOAM server. Select the **Stop** button. 
3 □	**Primary Standby NOAM:** Repeat	Repeat **steps 1-2** to disable the DSR application on the standby DR NOAM. **Note:** The DSR application should now be stopped on all DR-NOAMs.
4 □	**Primary NOAM VIP:** Verify DSR application is stopped.	Verify that **"PROC"** column on both DR DSR servers show **"Man"** indicating that application is manually stopped
5 □	**Primary NOAM VIP:** Establish an SSH session	Login via SSH to the physical IP of the chosen primary DR-NOAM server as ***admusr***user.

6
□
	Primary NOAM VIP: Change Role to Secondary	Execute the command
		`$ sudo top.setSecondary`
		Note: This step makes the primary NOAM to revert to DR-NOAM
		Execute the following command to verify the role was changed to secondary:
		`$ sudo top.myrole`
		`myNodeId=A1250.249`
		`myMasterCapable=true`
		`myMateNodeId=A1250.248`
		`myParentCluster=00000`
		`myClusterRole=Secondary`
		`myClusterTimestamp=02/26/16 10:00:20.047`

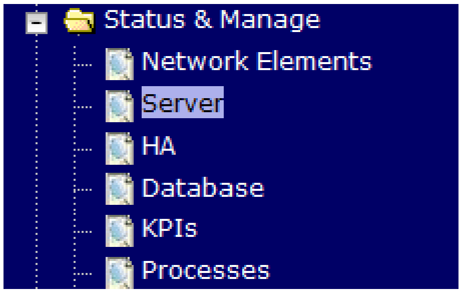
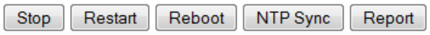
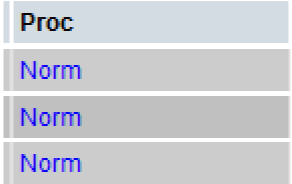
7 □	**New DR-NOAM VIP:** Verify Replication	Navigate to **Main Menu -> Status & Manage -> Server**  Status & Manage Network Elements Server HA Database KPIs Processes It may take several minutes for replication; afterward the **"DB"** and **"Reporting Status"** columns should show **"Normal"**.  DB — Reporting Status Norm — Norm Norm — Norm Norm — Norm
8 □	**To-Be-Primary NOAM VIP:** Establish an SSH session	Login via SSH to the VIP of the chosen primary DR-NOAM server as ***admusr*** user.

9
□
	To-Be-Primary DSR NOAM VIP: Set To-be-Primary DSR NOAM to Primary	Execute the following command:
		`$ sudo top.setPrimary`
		Note: This step makes the DSR take over as the Primary.
		Execute the command to verify the server role was changed to Primary:
		`$ sudo top.myrole`
		`myNodeId=A1055.206`
		`myMasterCapable=true`
		`myMateNodeId=A1055.214`
		`myParentCluster=00000`
		`myClusterRole=Primary`
		`myClusterTimestamp=02/26/16 10:01:52.162`
		System generates several replication and collection alarms as replication/collection links to/from former Primary NOAM servers becomes inactive.

Procedure 20: Returning a Recovered Site to Primary

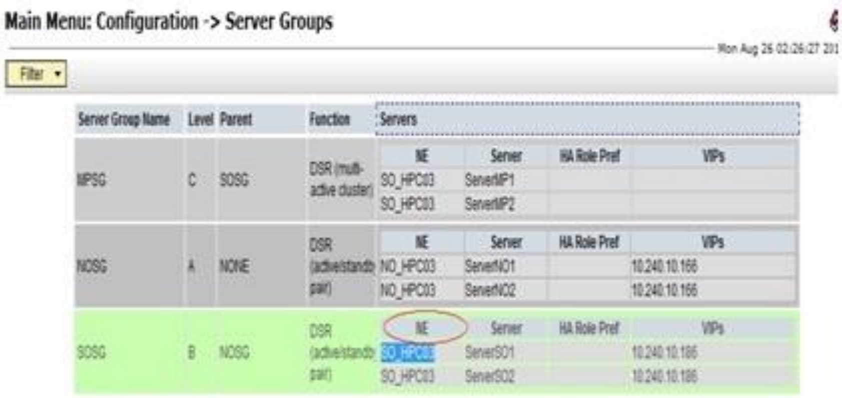
10 □	**Primary Active NOAM:** Login	Establish a GUI session on the primary NOAM server by using the VIP IP address of the primary NOAM. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:  **Oracle System Login** Fri Mar 20 12:29:52 2015 EDT **Log In** Enter your username and password to log in Username: guiadmin Password: ••••••• □ Change password 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 20: Returning a Recovered Site to Primary

11 □	**New Primary DSR NOAM VIP:** Re-enable the application.	Navigate to **Main Menu -> Status & Manage -> Server**  Status & Manage Network Elements Server HA Database KPIs Processes Select the row that has the new primary active NOAM server. Click the **Restart** button and then click the OK button.  Verify that **“PROC”** column now shows “Norm”.  Proc Norm Norm Norm
12 □	**New Primary DSR NOAM VIP:** Repeat on Standby NOAM	Repeat Step 11 on the standby primary NOAM server Provisioning can now resume to the VIP of the new-Primary DSR.
13 □	**New Primary DSR NOAM VIP:** Repeat on DR-NOAMs	Repeat Step 11 on the active and standby DR-NOAMs

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

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

S T E P #	The intent of this procedure is to inhibit A and B level replication on all C Level servers of this site Check off (√**)** each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix L:** My Oracle Support (MOS) and ask for assistance.	
1 □	**Active NOAM:** Login	Login to the Active NOAM server via SSH as ***admusr***user.
2 □	**Active NOAM:** Inhibit replication on all C level Servers	Execute the following command: `$ 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` **Note:** SOAM Site_NE name of the site can be found out by logging into the Active NOAM GUI and going to **Configuration->Server Groups** screen. Please see the snapshot below for more details. E.g. if ServerSO1 belong to the site which is being recovered then siteId will be SO_HPC03. 

Main Menu: Configuration -> Server Groups

Mon Aug 26 02:26:27 201

Filter ▾

Server Group Name	Level	Parent	Function	Servers			
				NE	Server	HA Role Pref	VIPs
MPSG	C	SOSG	DSR (multi-active cluster)	SO_HPC03	ServerMP1		
				SO_HPC03	ServerMP2		
				NE	Server	HA Role Pref	VIPs
NOSG	A	NONE	DSR (active/standby pair)	NO_HPC03	ServerNO1		10.240.10.166
				NO_HPC03	ServerNO2		10.240.10.166
				NE	Server	HA Role Pref	VIPs
SOSG	B	NOSG	DSR (active/standby pair)	SO_HPC03	ServerSO1		10.240.10.186
				SO_HPC03	ServerSO2		10.240.10.186

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

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

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

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

<table>
<tr><td><b>S
T
E
P
#</b></td><td colspan="2">The intent of this procedure is to Un-inhibit A and B level replication on all C Level servers of this site

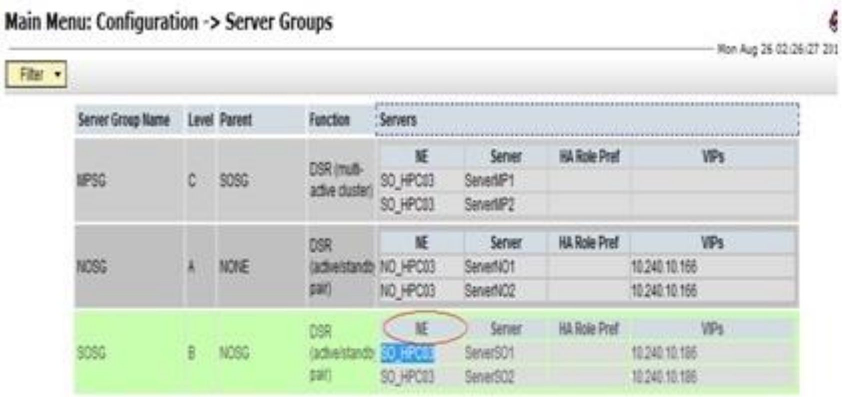
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact <b>Appendix L:</b> My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1
□</td><td><b>Active NOAM:</b> Login</td><td>Login to the Active NOAM server via SSH as <b><i>admusr</i></b>user.</td></tr>
<tr><td>2
□</td><td><b>Active NOAM:</b> Un-Inhibit replication on all C level Servers</td><td>Execute the following command:

<pre><code>$ for i in $(iqt -p -z -h -fhostName NodeInfo where
"nodeId like 'C*' and siteId='<SOAM_Site_NE_namee>'"); do
iset -finhibitRepPlans='' NodeInfo where "nodeName='$i'";
done</code></pre>

<b>Note:</b> SOAM Site NE name of the site can be found out by logging into the Active NOAM GUI and going to <b>Configuration->Server Groups</b> screen.

Please see the snapshot below for more details. E.g. if ServerSO1 belong to the site which is being recovered then siteId will be SO_HPC03.



<b>Main Menu: Configuration -> Server Groups</b>
Mon Aug 26 02:26:27 201
Filter ▾

<table>
<tr><th>Server Group Name</th><th>Level</th><th>Parent</th><th>Function</th><th>Servers</th></tr>
<tr><td>MPSG</td><td>C</td><td>SOSG</td><td>DSR (multi-active cluster)</td><td><table><tr><th>NE</th><th>Server</th><th>HA Role Pref</th><th>VIPs</th></tr><tr><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></table></td></tr>
<tr><td>NOSG</td><td>A</td><td>NONE</td><td>DSR (active/standb pair)</td><td><table><tr><th>NE</th><th>Server</th><th>HA Role Pref</th><th>VIPs</th></tr><tr><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></table></td></tr>
<tr><td>SOSG</td><td>B</td><td>NOSG</td><td>DSR (active/standb pair)</td><td><table><tr><th>NE</th><th>Server</th><th>HA Role Pref</th><th>VIPs</th></tr><tr><td>SO_HPC03</td><td>ServerSO1</td><td></td><td>10.240.10.186</td></tr><tr><td>SO_HPC03</td><td>ServerSO2</td><td></td><td>10.240.10.186</td></tr></table></td></tr>
</table>
</td></tr>
</table>

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

3 □

Active NOAM: Verify Replication has been Inhibited.

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.

Verification of replication un-inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site e.g. Site SO_HPC03 shall be set as ‘A B’:

Perform the following command:

```
$ sudo iqt NodeInfo
```

Expected output:

```
   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:
		`$ pm.set off inetsync`
		`$ pm.set on inetsync`

Appendix H: Restore TVOE Configuration from Backup Media

Procedure 23: Restore TVOE Configuration from Backup Media

S **T** **E** **P** **#**	This procedure provides steps to restore the TVOE application configuration from backup media. 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 □	**Install TVOE Application**	• If the PMAC is **NOT** hosted on the failed rack mount server, follow procedure *“IPM Servers Using PM&C Application”* from reference [10] • If the PMAC is hosted on the failed rack mount server, follow procedure *“Installing TVOE on the Management Server”* from reference [10]
2 □	**Establish network connectivity**	• 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] **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.
3 □	**Restore TVOE Backup ISO image to the TVOE host (NetBackup)**	**If using NetBackup to restore the TVOE backup ISO image execute this step, otherwise skip this step** 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. **Note:** Once restored, the ISO image will be in */var/TKLC/bkp/* on the TVOE server.

Procedure 23: Restore TVOE Configuration from Backup Media

4
□
	Transfer TVOE Backup ISO image to the TVOE host	**Restoring TVOE backup ISO using SCP**
		Using the IP of the TVOE host, transfer the backup ISO image to the TVOE.
		Linux:
		From the command line of a Linux machine use the following command to copy the backup ISO image to the TVOE host:
		`# scp <path_to_image> tvoexfer@<TVOE_IP>:backup/`
		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.
		Note: If the IP is an IPv4 address then **`<TVOE_IP>`** will be a normal dot-decimal notation (e.g. "10.240.6.170").
		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 *control* 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.
		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.
		IPv4 Example:
		`# scp /path/to/image.iso tvoexfer@10.240.6.170:backup/`
		IPv6 Example:
		`# scp /path/to/image.iso`
		`tvoexfer@[fe80::21e:bff:fe76:5e1c%control]:backup/`
		Windows:
		Use WinSCP to copy the Backup ISO image into the */var/TKLC/smac/bkp* directory. Please refer to [10] procedure *Using WinSCP* to copy the backup image to the customer system.

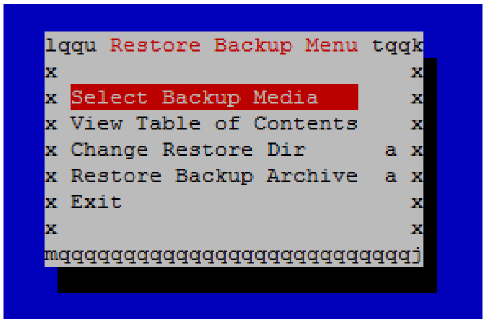
5 □	**TVOE Server:** Login	Establish an SSH session to the TVOE server, login as ***admusr.***

6 □ **Restore TVOE Backup ISO image**

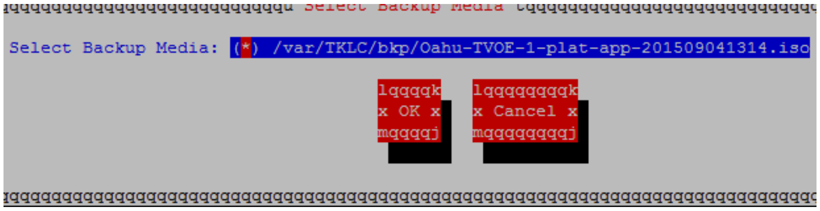
Restore the TVOE backup ISO by executing the following:

```
$ sudo  su – platcfg
```

Navigate to **Maintenance -> Backup and Restore -> Restore Platform -> Select Backup Media**



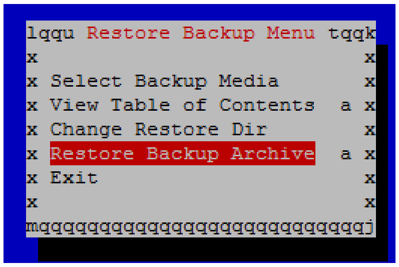
Select the desired archive:



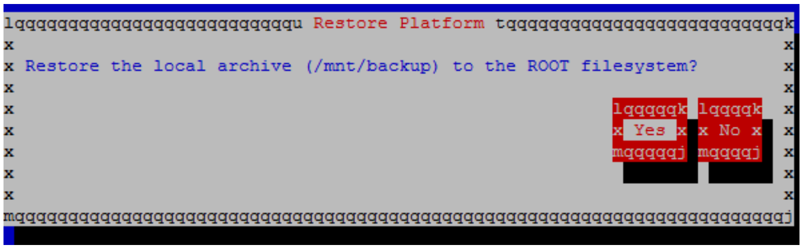
Select Backup Media: (*) /var/TKLC/bkp/Oahu-TVOE-1-plat-app-201509041314.iso

Select **OK**

Select **Restore Backup Archive**

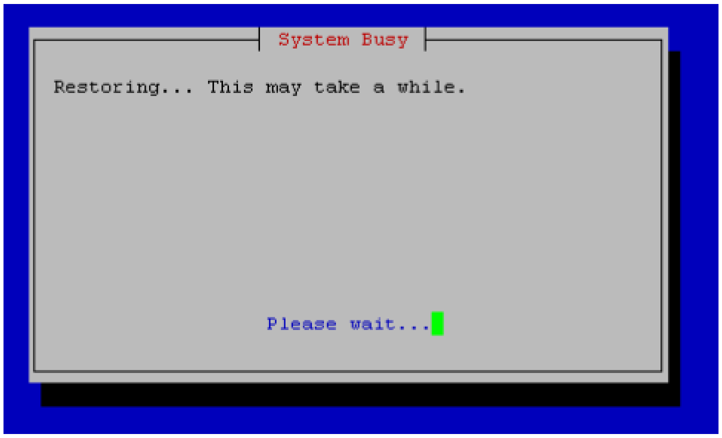
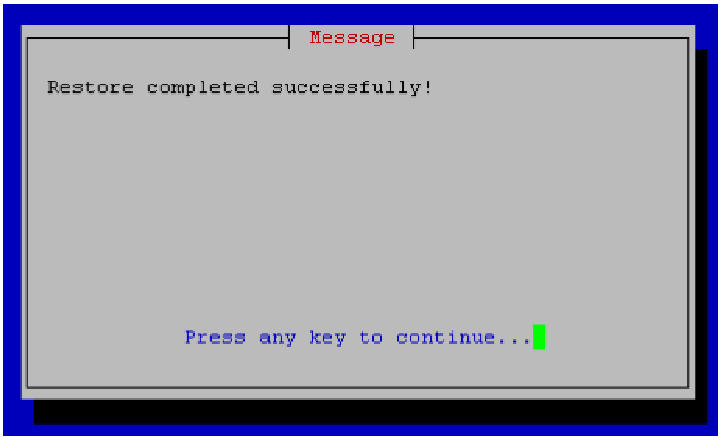


Confirm restore:



Restore the local archive (/mnt/backup) to the ROOT filesystem?

Procedure 23: Restore TVOE Configuration from Backup Media

7 □	**Monitor TVOE Backup process**	Wait for the restore to complete.  System Busy Restoring... This may take a while. Please wait... **Note:** This will typically take less than 5 minutes Restore complete:  Message Restore completed successfully! Press any key to continue... **Exit** Platcfg
8 □	**PMAC:** Login	**If PMAC is NOT located on the this TVOE host, execute this step** Establish an SSH session to the PMAC server, login as ***admusr.***
9 □	**PMAC:** Remove Old TVOE Host Key	**If PMAC is NOT located on the this TVOE host, execute this step** Remove the old TVOE host key by executing the following command: `$ sudo pmacadm removeHostKeys --ip=<TVOE Host Control IPv6 Address>`
10 □	**TVOE Server:** Reboot	Restart the TVOE server by executing the following command: `$ sudo init 6`

Appendix I: Restore PMAC from Backup

Procedure 24: Restore PMAC from Backup Media

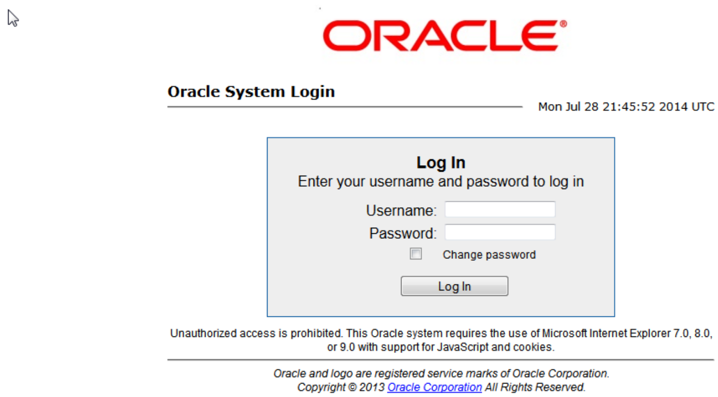
S T E P #	This procedure provides steps to restore the PMAC application configuration from backup media. **Prerequisite:** TVOE management server has been restored. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix L: My Oracle Support (MOS) and ask for assistance.	
1 □	**Deploy the PMAC Guest**	Execute section *"Install PM&C"* from reference [10]
2 □	**PMAC:** Login	Establish an SSH session to the PMAC server, login as ***admusr.***

3
□
	Restore PMAC Backup image to the TVOE host	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.
		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>
		`$ sudo /usr/bin/scp -p \`
		`admsur@<remoteserver>:/var/TKLC/smac/backup/*.pef \`
		`/var/TKLC/smac/backup/`
		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.

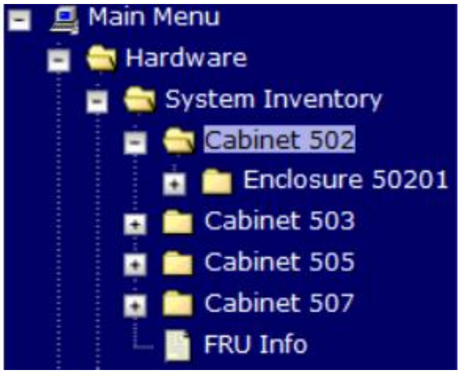
4 □	**PMAC:** Verify no Alarms are present	Verify no alarms are present by executing the following command: `$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus`

Procedure 24: Restore PMAC from Backup Media

5
□
	Restore the PMAC Data from Backup	Restore the PMAC data from backup by executing the following command:
		`$ sudo /usr/TKLC/smac/bin/pmacadm restore`
		`PM&C Restore been successfully initiated as task ID 1`
		To check the status of the background task, issue the following command:
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		Note: The result will eventually display *PMAC Restore successful.*

6 □	**PMAC GUI:** Login	Open web browser and navigate to the PMAC GUI, Login as ***PMACadmin*** user: `https://<pmac_network_ip>`  Oracle System Login Mon Jul 28 21:45:52 2014 UTC Log In Enter your username and password to log in Username: Password: □ Change password Log In Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 7.0, 8.0, or 9.0 with support for JavaScript and cookies. *Oracle and logo are registered service marks of Oracle Corporation.* *Copyright © 2013 Oracle Corporation All Rights Reserved.*
7 □	**PMAC GUI:** Verify Restore Task completed	Navigate to **Task Monitoring** Verify the restore background task completed successfully. **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. **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.

Procedure 24: Restore PMAC from Backup Media

8 □	**PMAC GUI:** Verify System Inventory	Navigate to **Main Menu -> System Inventory**  Main Menu Hardware System Inventory Cabinet 502 Enclosure 50201 Cabinet 503 Cabinet 505 Cabinet 507 FRU Info Verify previously provisioned enclosures are present

9
□
	PMAC: Verify PMAC	Perform a system health check on the PMAC
		`$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus`
		This command should return no output on a healthy system.
		`$ sudo /usr/TKLC/smac/bin/sentry status`
		`All Processes should be running, displaying output similar to the following:`
		`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.`

10 □	**PMAC:** Add ISO images to the PMAC	Re-add any needed ISO images to the PMAC by executing procedure *“Load Application and TPD ISO onto PMAC Server”* from reference [8]

Procedure 24: Restore PMAC from Backup Server

STEP #

This procedure provides steps to restore the PMAC application configuration from backup server.

Prerequisite: TVOE management server has been restored.

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 □ **Deploy the PMAC Guest**

Execute section *"Install PM&C"* from reference [10]

Note: This procedure is for restoring from a NetBackup server, so specify the appropriate options when deploying PM&C for use with NetBackup.

2 □ **PMAC TVOE Host:** Login

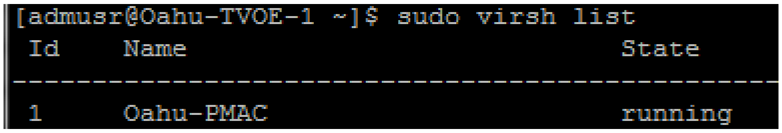
Establish an SSH session to the PMAC TVOE Host, login as ***admusr.***

3 □ **PMAC TVOE Host:** Login to PMAC Guest Console

On the TVOE host, execute the following command:

```
$sudo virsh list
```

This will produce a listing of currently running virtual machines.



```
[admusr@Oahu-TVOE-1 ~]$ sudo virsh list
 Id    Name                           State
----------------------------------------------------
 1     Oahu-PMAC                      running
```

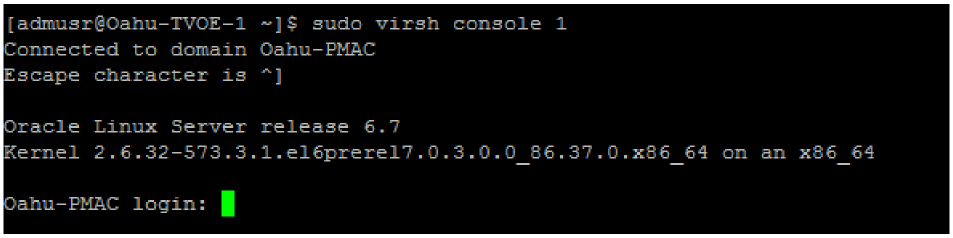
Find the VM name for your PMAC and note its ID number in the first column.

4 □ Connect to console of the VM using the VM number obtained in Step 3.

On the TVOE host, execute:

```
$sudo virsh console <PMAC-VMID>
```

Where **PMAC-VMID** is the VM ID you obtained in **Step 3**:



```
[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.el6prerel7.0.3.0.0_86.37.0.x86_64 on an x86_64

Oahu-PMAC login:
```

You are now connected to the PMAC guest console.

If you wish to return to the TVOE host, you can exit the session by pressing **CTRL +]**

Procedure 24: Restore PMAC from Backup Server

5 □	**PMAC:** Prepare PMAC guest to transfer the appropriate backup from Backup Server. Disable iptables, and enable the TPD platcfg backup configuration menus.	Run the following commands on the PMAC:

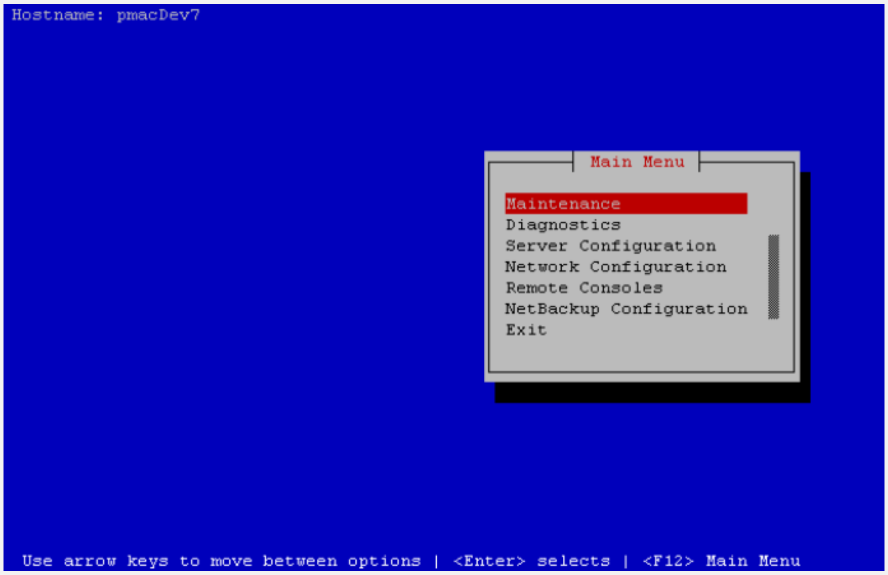
```
$ sudo /sbin/service iptables stop

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=
```

Procedure 24: Restore PMAC from Backup Server

<table>
<tr>
<td>6
□</td>
<td><b>PMAC:</b> Verify the TPD platcfg backup menus are visible, then exit the TPD platcfg Utlility</td>
<td>

Issue the following command to verify the TPD platcfg backup menus are visible:

```
$ sudo /bin/su – platcfg
```



```
Hostname: pmacDev7
```

```
Use arrow keys to move between options | <Enter> selects | <F12> Main Menu
```

Note: In the example image above of the TPD platcfg utility Main Menu the backup menu is identified as “NetBackup Configuration”.

</td>
</tr>
<tr>
<td>7
□</td>
<td><b>PMAC:</b> Verify the iptables rules are disabled on the PMAC guest</td>
<td>

Verify the iptables rules are disabled on the PMAC guest by executing the following command:

```
$ sudo /sbin/iptables -nL

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
```

</td>
</tr>
<tr>
<td>8
□</td>
<td><b>PMAC:</b> Install backup utility client software on the PMAC Guest</td>
<td>

Execute section *“PM&C NetBackup Client Installation and Configuration”* from [10] - Start at step 4.

Note: The *“Initialize PM&C Application”* and *“Configure PM&C application”* prereuistes can be igrnored.

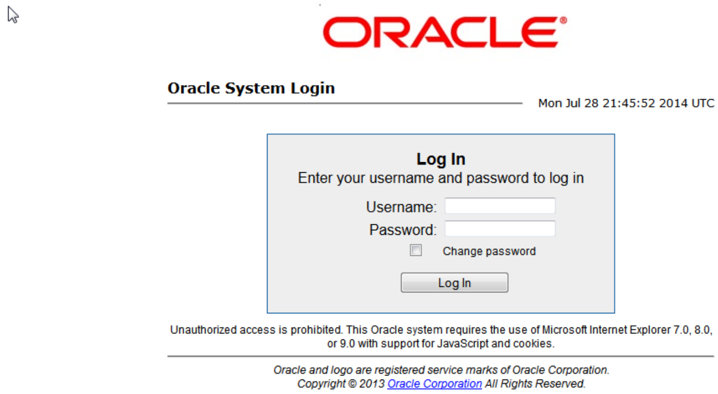
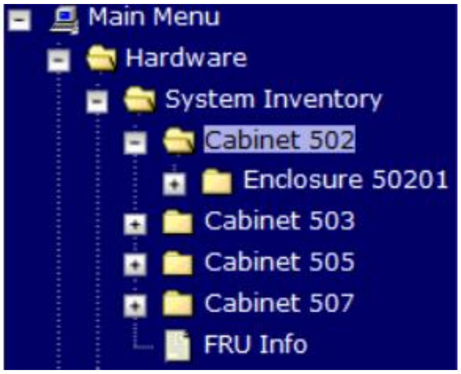
</td>
</tr>
</table>

Procedure 24: Restore PMAC from Backup Server

9 □	**Backup Server:** Verify appropriate PMAC backup exists.	This step will likely be executed by customer IT personnel. Log in to the Backup Server as the appropriate user, using the user password. Execute the appropriate commands to verify the PMAC backup exists for the desired date. **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. **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.
10 □	**Backup Server:** Verify appropriate PMAC backup exists.	This step will likely be executed by customer IT personnel. Log in to the Backup Server as the appropriate user, using the user password. Execute the appropriate commands to verify the PMAC backup exists for the desired date. Execute the appropriate commands to restore the PM&C Management Server backup for the desired date. **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.
11 □	**PMAC:** Verify no Alarms are present	Verify no alarms are present by executing the following command: `$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus`

12
□
	Restore the PMAC Data from Backup	Restore the PMAC data from backup by executing the following command:
		`$ sudo /usr/TKLC/smac/bin/pmacadm restore`
		`PM&C Restore been successfully initiated as task ID 1`
		To check the status of the background task, issue the following command:
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		Note: The result will eventually display *PMAC Restore successful.*

Procedure 24: Restore PMAC from Backup Server

13 □	**PMAC GUI:** Login	Open web browser and navigate to the PMAC GUI, Login as ***PMACadmin*** user: `https://<pmac_network_ip>`  Oracle System Login Mon Jul 28 21:45:52 2014 UTC **Log In** Enter your username and password to log in Username: Password: □ Change password Log In Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 7.0, 8.0, or 9.0 with support for JavaScript and cookies. *Oracle and logo are registered service marks of Oracle Corporation.* *Copyright © 2013 Oracle Corporation All Rights Reserved.*
14 □	**PMAC GUI:** Verify Restore Task completed	Navigate to **Task Monitoring** Verify the restore background task completed successfully. **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. **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.
15 □	**PMAC GUI:** Verify System Inventory	Navigate to **Main Menu -> System Inventory**  Main Menu Hardware System Inventory Cabinet 502 Enclosure 50201 Cabinet 503 Cabinet 505 Cabinet 507 FRU Info Verify previously provisioned enclosures are present

Procedure 24: Restore PMAC from Backup Server

<table>
<tr>
<td>16
□</td>
<td><b>PMAC:</b> Verify PMAC</td>
<td>

Perform a system health check on the PMAC

```
$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus
```

This command should return no output on a healthy system.

```
$ sudo /usr/TKLC/smac/bin/sentry status

All Processes should be running, displaying output
similar to the following:

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.
```

</td>
</tr>
<tr>
<td>17
□</td>
<td><b>PMAC:</b> Add ISO images to the PMAC</td>
<td>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]</td>
</tr>
</table>

Appendix J: Configure TVOE Hosts

Procedure 25: Configure TVOE

STEP #	This procedure will configure networking on TVOE Hosts **Prerequisite:** Server has been IPM'ed with TVOE OS as described in [10] 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

1 □	Determine Bridge names and interfaces for XMI and IMI, and NetBackup (if used) networks.	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. If the NetBackup bridge and interface were not previously configured on this server when PMAC was installed, determine those values as well. Fill in the appropriate values in the table below:

NOAM Guest Interface Name	TVOE Bridge Name	TVOE Bridge Interface
xmi	xmi	**Interface Bond** (e.g- bond0, bond1, etc) ____________________ <TVOE_XMI_Bridge_Interface_Bond> **Interface Name** (e.g. - bond0.3, bond1, bond0.100): ____________________ <TVOE_XMI_Bridge_Interface>
imi	imi	**Interface Bond**:(e.g. - bond0, bond1, etc) ____________________ <TVOE_IMI_Bridge_Interface_Bond> **Interface Name**: (e.g. - bond0.4, bond1, bond0.100) ____________________ <TVOE_IMI_Bridge_Interface
NetBackup	NetBackup	: **Interface Name** (e.g. - eth11, eth04, eth03, etc) ____________________ <TVOE_NetBackup_Bridge_Interface>
management	management	**Interface Name** (e.g. bond0.2, bond0.37, etc) ____________________ <TVOE_Mgmt_Bridge_Interface>

Procedure 25: Configure TVOE

2 □	**RMS Server:** Login	Log in to the TVOE prompt of the RMS Server as ***admusr*** using the iLO facility.

4

□

RMS Server: Configure XMI Bridge Interface Bond

Verify the xmi bridge interface bond by running the following command:

Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured.

```
$ 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
```

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.

Create bonding interface and associate subordinate interfaces with bond:

```
$ 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]
```

Note: All other existing bonds should be included in the 'val=' statement. E.g. if TVOE_XMI_Bridge_Bond = bond1, val=bond0,bond1

```
$ sudo syscheckAdm net ipbond –enable
```

Procedure 25: Configure TVOE

4
□
	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:
		`$ sudo /usr/TKLC/plat/bin/netAdm add`
		`--device=<TVOE_XMI_Bridge_Interface>  --onboot=yes`
		`Interface <TVOE_XMI_Bridge_Interface> created.`

5
□
	RMS Server: Create XMI Bridge	Now , create the XMI bridge:
		`$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --`
		`name=xmi --onboot=yes`
		`--bridgeInterfaces=<TVOE_XMI_Bridge_Interface>`
		`Interface <TOE_XMI_Bridge_Interface> updated.`
		`Bridge xmi created.`

Procedure 25: Configure TVOE

6 □

RMS Server: Configure IMI Bridge Interface Bond

Verify the imi bridge interface bond by running the following command:

Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured.

```
$ 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
```

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.

Create bonding interface and associate subordinate interfaces with bond:

```
$ 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
```

Execute the following 2 commands ONLY IF <TVOE_XMI_Bridge_Bond> is **different** from <TVOE_IMI_Bridge_Bond>

```
$ sudo syscheckAdm net ipbond --set --var=DEVICES
--val=<TVOE_XMI_Bridge_Interface_Bond>,
<TVOE_IMI_Bridge_Interface_Bond>,[other bonds…]
```

```
$ sudo syscheckAdm net ipbond –enable
```

Procedure 25: Configure TVOE

7
□
	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:
		`$ sudo /usr/TKLC/plat/bin/netAdm add`
		`--device=<TVOE_IMI_Bridge_Interface> --onboot=yes`
		
		`Interface <TVOE_IMI_Bridge_Interface> created.`

8
□
	RMS Server: Create IMI Bridge	Create the IMI bridge:
		
		`$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --`
		`name=imi --onboot=yes`
		`--bridgeInterfaces=<TVOE_IMI_Bridge_Interface>`
		
		`Interface <TVOE_IMI_Bridge_Interface> updated.`
		`Bridge imi created.`

9 □

RMS server iLO: Create management bridge and assign TVOE Management IP

Execute this Step only if the TVOE Host is a rack mount server and is NOT the PMAC server.

Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (*network devices, bonds, and bond enslaved devices*), to configure.

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:

```
$ 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
```

```
$ 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
```

```
$ 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
```

EXAMPLE 1: Create Management bridge using untagged interfaces

```
$ 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>
```

EXAMPLE 2: Create Management bridge using tagged interfaces

```
$ 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>
```

<table>
<tr>
<td>10
□</td>
<td><b>RMS server iLO:</b> Add Default route</td>
<td>

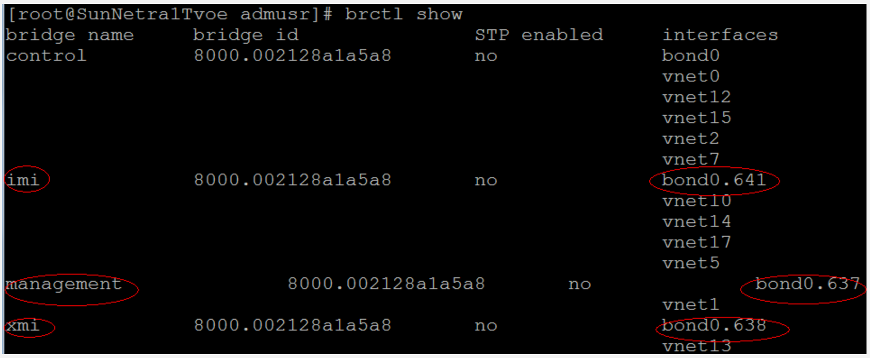
Add a default route using the xmi or management address (if configured)

```
$ sudo /usr/TKLC/plat/bin/netAdm add --route=default
--gateway=<TVOE_Mgmt_gateway_IP_address>
--device=<management or xmi>
Route to management created.
```

</td>
</tr>
<tr>
<td>11
□</td>
<td><b>RMS Server:</b> Verify bridge creation status</td>
<td>

Verify that the XMI and IMI bridges have been created successfully (Example output for illustrative purposes only):

```
$ brctl show
```



```
[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
```

- 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>

</td>
</tr>
<tr>
<td>12
□</td>
<td><b>RMS Server iLO:</b> Create NetBackup bridge (Optional)</td>
<td>

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)

```
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge
--name=NetBackup --onboot=yes --MTU=<NetBackup_MTU_size>
--bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface>
```

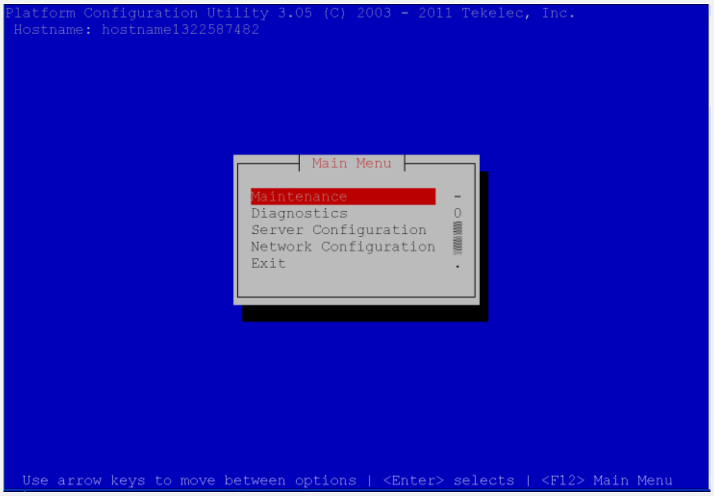
</td>
</tr>
</table>

Procedure 25: Configure TVOE

13 □

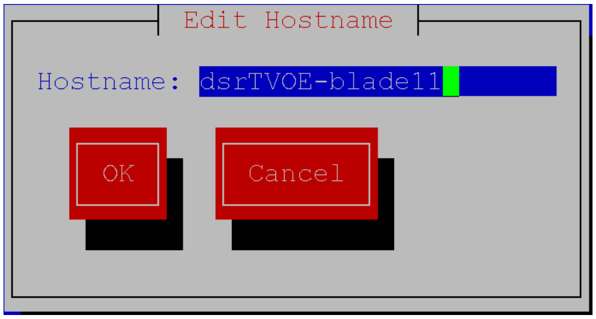
RMS Server iLO: Set Hostname

```
$ sudo su – platcfg
```



```
Platform Configuration Utility 3.05 (C) 2003 - 2011 Tekelec, Inc.
 Hostname: hostname1322587482

                         Main Menu
                 Maintenance
                 Diagnostics
                 Server Configuration
                 Network Configuration
                 Exit

  Use arrow keys to move between options | <Enter> selects | <F12> Main Menu
```

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



```
        Edit Hostname

 Hostname: dsrTVOE-blade11

    OK      Cancel
```

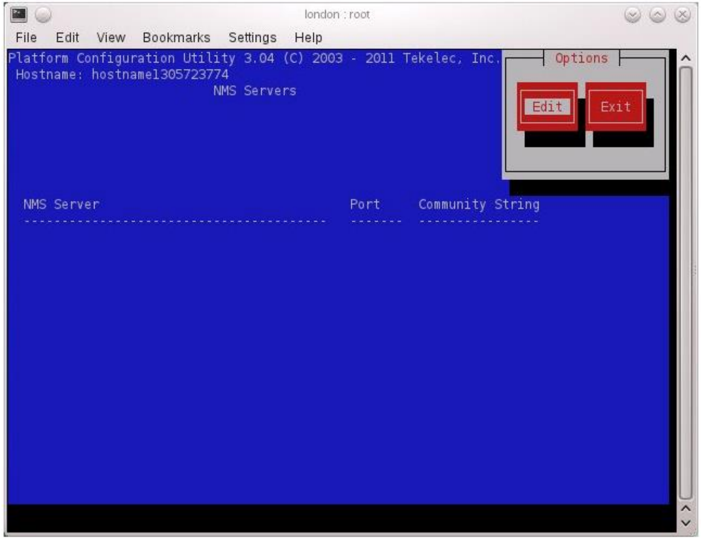
Press **OK** and select and continue to press Exit until you are at the platcfg main menu again.

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

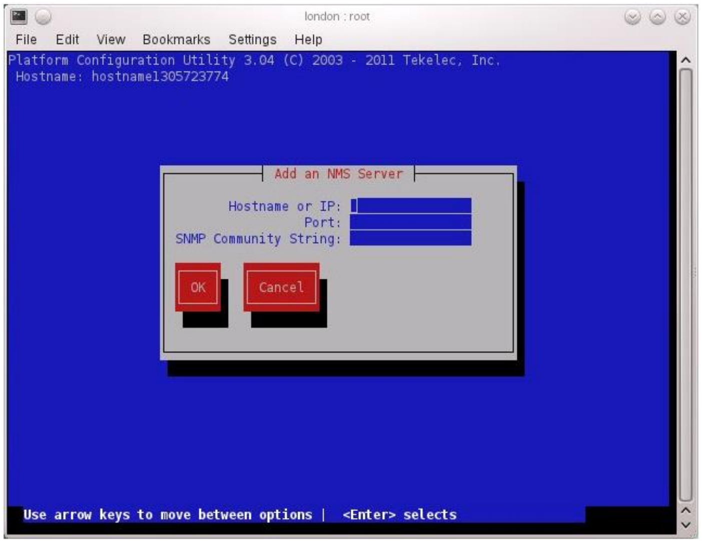
14 □ **RMS Server iLO:** Configure SNMP

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



```
Platform Configuration Utility 3.04 (C) 2003 - 2011 Tekelec, Inc.
 Hostname: hostname1305723774
                           NMS Servers

  NMS Server                                Port     Community String
  ----------------------------------------  -------  ----------------
```

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



```
Platform Configuration Utility 3.04 (C) 2003 - 2011 Tekelec, Inc.
 Hostname: hostname1305723774

          Hostname or IP:
                    Port:
   SNMP Community String:

  Use arrow keys to move between options |  <Enter> selects
```

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

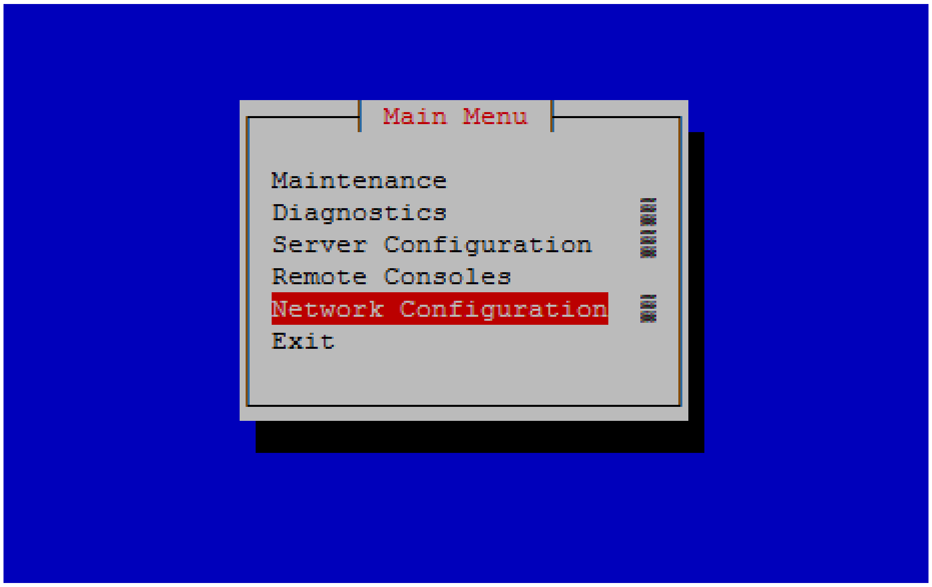
1. Enter the Hostname/IP of the Customer NMS Server, for port enter 162, and for Community String enter the community string provided in the customer NAPD Document.
2. Enter the IP of the NOAM VIP, for port enter 162, and for Community String enter the community string provided in the customer NAPD Document

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

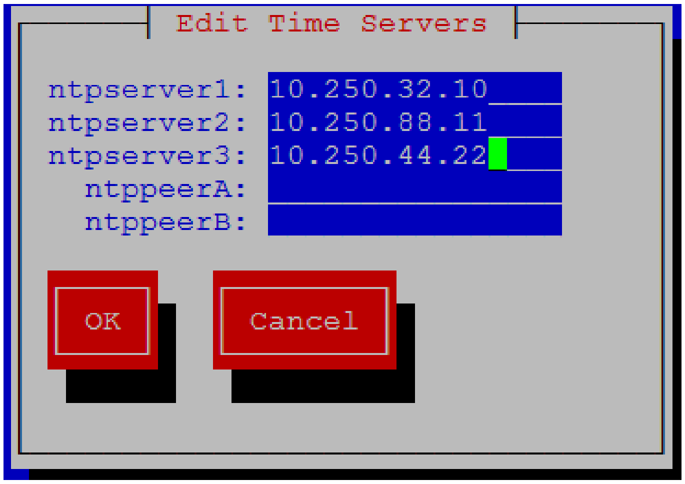
15 ☐

RMS Server iLO: Configure NTP

Navigate to **Network Configuration**



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



```
ntpserver1: 10.250.32.10
ntpserver2: 10.250.88.11
ntpserver3: 10.250.44.22
  ntppeerA:
  ntppeerB:
```

- 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.

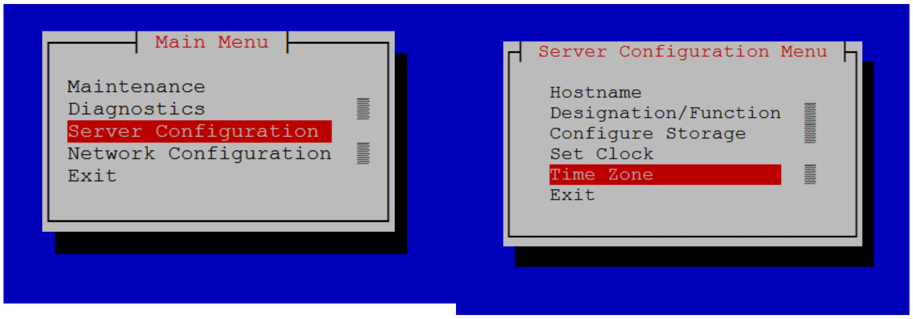
Press **OK**
Press **Exit** to return to the platcfg menu.

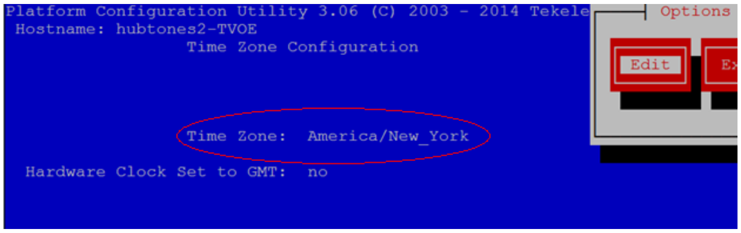
Procedure 25: Configure TVOE

16 □ **RMS Server iLO:** Configure Time Zone

```
$ sudo su - platcfg
```

Navigate to **Server Configuration->Time Zone**

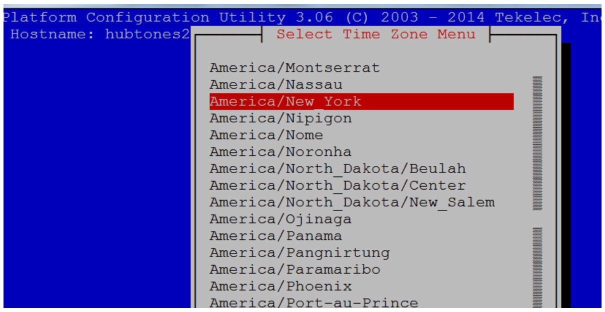




```
Platform Configuration Utility 3.06 (C) 2003 - 2014 Tekele
 Hostname: hubtones2-TVOE
                  Time Zone Configuration


                  Time Zone:  America/New_York

  Hardware Clock Set to GMT:  no
```

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.

Click **Edit**



```
Platform Configuration Utility 3.06 (C) 2003 - 2014 Tekelec, In
 Hostname: hubtones2
```

Select the desired time zone from the list and press **Enter**
Continue pressing **Exit** until you are out of the platcfg program.

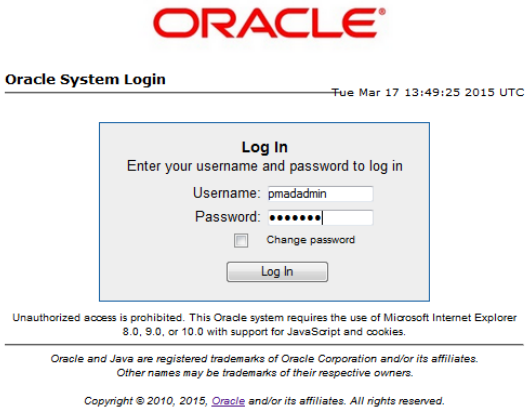
17 □ **RMS Server iLO:** Reboot Server

Reboot the server by executing the following command:

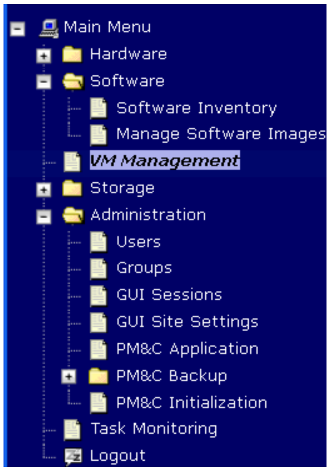
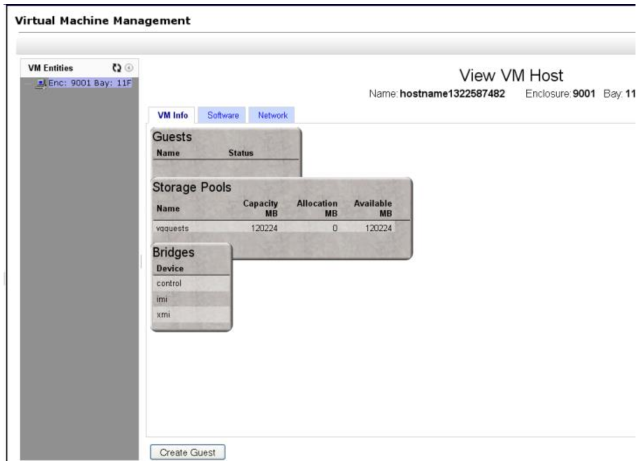
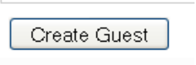
```
$ sudo su - platcfg
```

Appendix K: Create NOAM/SOAM Virtual Machines

Procedure 26: Create NOAM Guest VMs

S T E 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. **Prerequisite**: TVOE has been installed and configured on the target blade server or RMS 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 □	**PMAC GUI:** Login	Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` Login as ***pmacadmin*** user:  Oracle System Login Tue Mar 17 13:49:25 2015 UTC **Log In** Enter your username and password to log in Username: pmadadmin Password: ••••••• □ Change password Log In Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2015, Oracle and/or its affiliates. All rights reserved.*

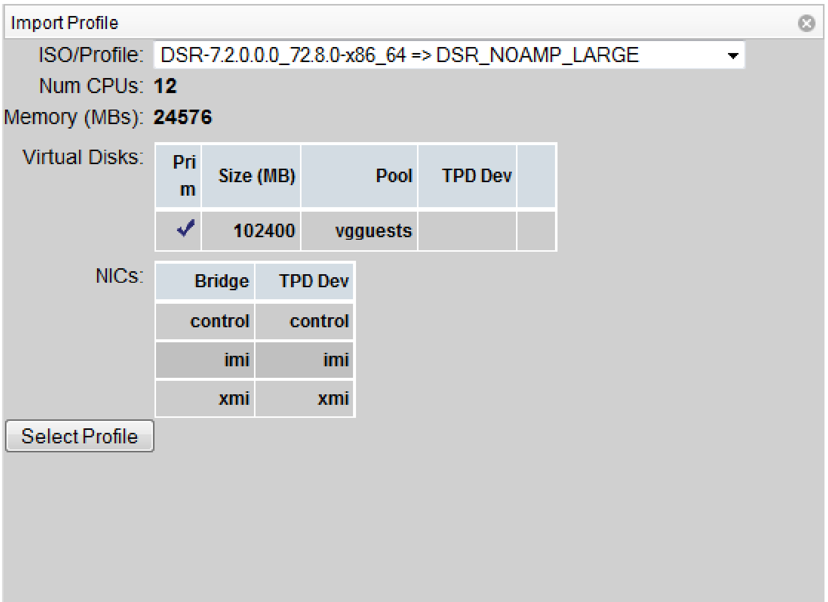
Procedure 26: Create NOAM Guest VMs

2 □	**PMAC GUI:** Navigate to VM Management of the Target Server Blade	Navigate to **Main Menu -> VM Management**  Main Menu Hardware Software Software Inventory Manage Software Images VM Management Storage Administration Users Groups GUI Sessions GUI Site Settings PM&C Application PM&C Backup PM&C Initialization Task Monitoring Logout 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.  Virtual Machine Management VM Entities Enc: 9001 Bay: 11F View VM Host Name: **hostname1322587482** Enclosure: **9001** Bay: **11** VM Info · Software · Network Guests Name · Status Storage Pools Name · Capacity MB · Allocation MB · Available MB vgguests · 120224 · 0 · 120224 Bridges Device control imi xmi  Click **Create Guest**

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:

Prim	Size (MB)	Pool	TPD Dev	
✓	102400	vgguests		

NICs:

Bridge	TPD Dev
control	control
imi	imi
xmi	xmi

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**

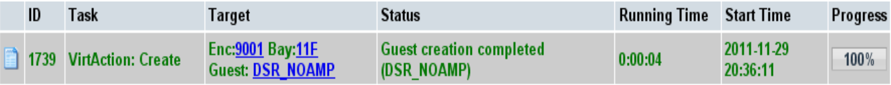
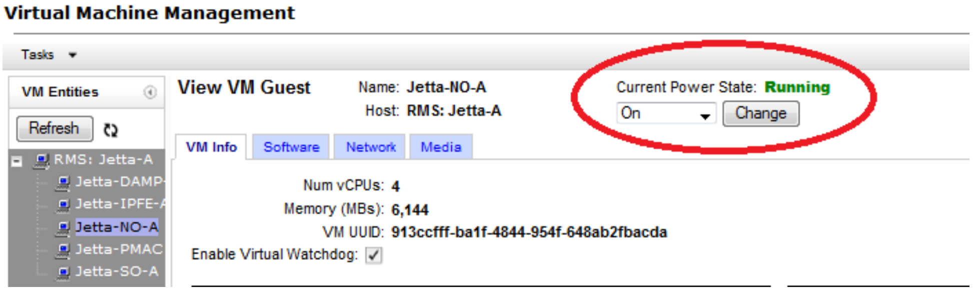
Note: Application_ISO_NAME is the name of the DSR Application ISO to be installed on this NOAM

Press **Select Profile**.

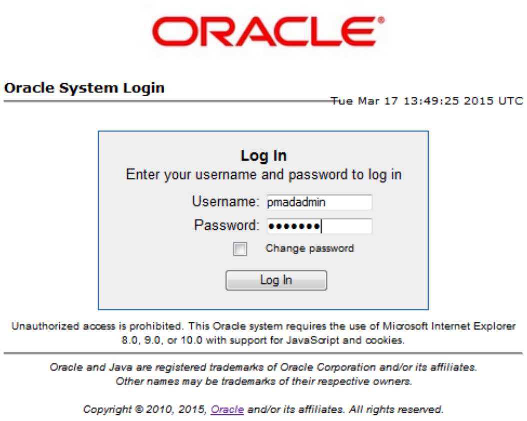
Press **Create**

Create

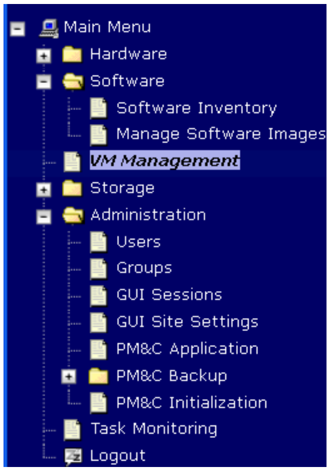
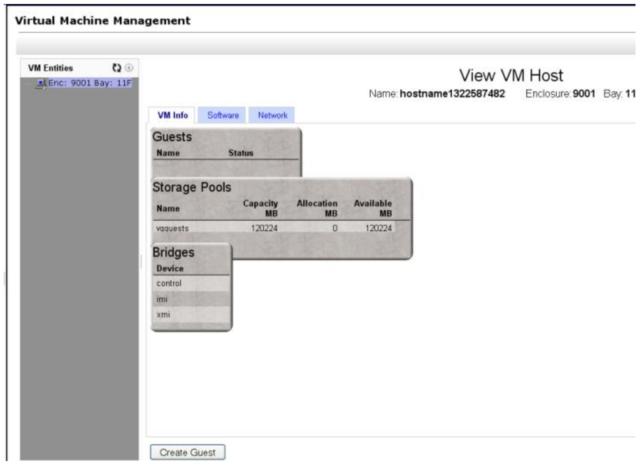
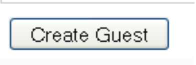
Procedure 26: Create NOAM Guest VMs

4 □	**PMAC GUI:** Wait for Guest Creation to Complete	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. Wait or refresh the screen until you see that the guest creation task has completed successfully.  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%
5 □	**PMAC GUI:** Verify Guest Machine is Running	Navigate to **Main Menu -> VM Management** Select the TVOE server blade on which the guest machine was just created. 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".***  Virtual Machine Management View VM Guest Name: Jetta-NO-A Host: RMS: Jetta-A Current Power State: Running Num vCPUs: 4 Memory (MBs): 6,144 VM UUID: 913ccfff-ba1f-4844-954f-648ab2fbacda Enable Virtual Watchdog: ☑ VM Creation for this guest is complete. Repeat from **Step 2** for any remaining NOAM VMs (*for instance, the standby NOAM*) that must be created.

Procedure 27: Create SOAM Guest VMs

S T E 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. **Prerequisite**: TVOE has been installed and configured on the target blade server. Check off (√***)*** each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix L: My Oracle Support (MOS) and ask for assistance.	
1 □	**PMAC GUI:** Login	Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` Login as ***pmacadmin*** user:  Oracle System Login Tue Mar 17 13:49:25 2015 UTC Log In Enter your username and password to log in Username: pmadadmin Password: ••••••• □ Change password Log In Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2015, Oracle and/or its affiliates. All rights reserved.*

Procedure 27: Create SOAM Guest VMs

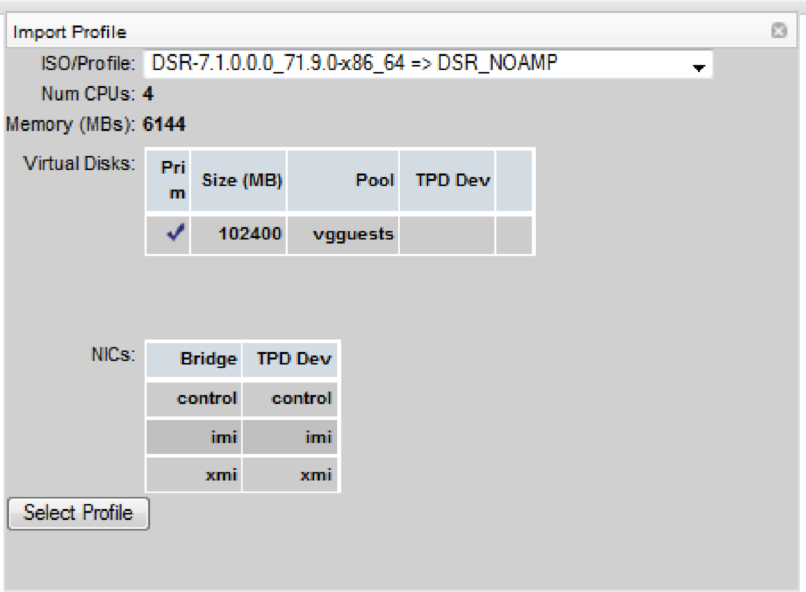
2 □	**PMAC GUI:** Navigate to VM Management of the Target Server Blade	Navigate to **Main Menu -> VM Management**  Main Menu Hardware Software Software Inventory Manage Software Images VM Management Storage Administration Users Groups GUI Sessions GUI Site Settings PM&C Application PM&C Backup PM&C Initialization Task Monitoring Logout 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.  Virtual Machine Management VM Entities Enc: 9001 Bay: 11F View VM Host Name: **hostname1322587482** Enclosure: **9001** Bay: **11** VM Info Software Network Guests Name Status Storage Pools Name / Capacity MB / Allocation MB / Available MB vgguests / 120224 / 0 / 120224 Bridges Device control imi xmi Create Guest  Click **Create Guest**

Procedure 27: Create SOAM Guest VMs

3 □

PMAC GUI: Configure VM Guest Parameters

Select **Import Profile**



Import Profile

ISO/Profile: DSR-7.1.0.0.0_71.9.0-x86_64 => DSR_NOAMP

Num CPUs: **4**

Memory (MBs): **6144**

Virtual Disks:

Prim	Size (MB)	Pool	TPD Dev
✓	102400	vgguests	

NICs:

Bridge	TPD Dev
control	control
imi	imi
xmi	xmi

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:

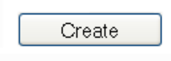
SOAM VM TVOE Hardware Type(s)	Dedicated Netbackup Interface?	Choose Profile (<Application ISO NAME>)➔
HP BL460 Gen 8 Blade, HP BL460 Gen 6 Blade, HP BL460 Gen 9 Blade	No	**DSR_SOAM**
HP BL460 Gen 8 Blade, HP BL460 Gen 6 Blade, HP BL460 Gen 9 Blade	Yes	**DSR_SOAM_NBD**

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

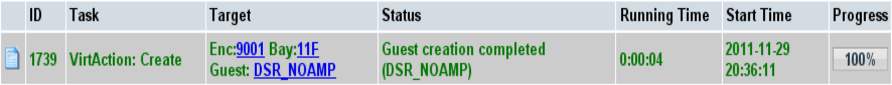
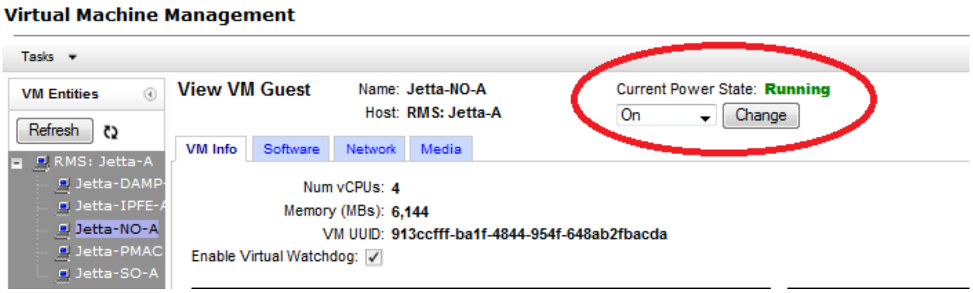
Press **Select Profile**.

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

<table>
<tr>
<td>4
□</td>
<td><b>PMAC GUI:</b> Wait for Guest Creation to Complete</td>
<td>
<p>Navigate to <b>Main Menu -> Task Monitoring</b> 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>
<tr><th></th><th>ID</th><th>Task</th><th>Target</th><th>Status</th><th>Running Time</th><th>Start Time</th><th>Progress</th></tr>
<tr><td></td><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>
</table>
</td>
</tr>
<tr>
<td>5
□</td>
<td><b>PMAC GUI:</b> Verify Guest Machine is Running</td>
<td>
<p>Navigate to <b>Main Menu -> VM Management</b></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 <b><i>“Running”.</i></b></p>

<p><b>Virtual Machine Management</b></p>
<p><b>View VM Guest</b></p>
<p>Name: Jetta-NO-A
Host: RMS: Jetta-A</p>
<p>Current Power State: Running
On</p>
<p>Num vCPUs: 4
Memory (MBs): 6,144
VM UUID: 913ccfff-ba1f-4844-954f-648ab2fbacda
Enable Virtual Watchdog: ✓</p>

<p>VM Creation for this guest is complete. Repeat from <b>Step 2</b> for any remaining NOAM VMs (<i>for instance, the standby SOAM</i>) that must be created.</p>
</td>
</tr>
</table>

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 menus selections. Make the selections in the sequence shown below on the Support telephone menu:

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

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

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