Oracle® Communications

Diameter Signaling Router

DSR Cloud Disaster Recovery Guide

Release 7.0.1 / 7.1.1/7.2/7.3

E64815 Revision 04

September 2016

ORACLE

Oracle Communications Diameter Signaling Router DSR Cloud Disaster Recovery Guide

CAUTION: Use only the Upgrade procedure included in the Upgrade Kit.

Before upgrading any system, please access My Oracle Support (MOS) (https://support.oracle.com) and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

My Oracle Support (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.

See more information on MOS in the Appendix section.

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 7.0.1 / 7.1.1/7.2/7.3 (3-tier deployments). This includes recovery of partial or a complete loss of one or more DSR servers. The audience for this document includes GPS groups such as Software Engineering, Product Verification, Documentation, and Customer Service including Software Operations and First Office Application. This document can also be executed by Oracle customers, as long as Oracle Customer Service personnel are involved and/or consulted. This document provides step-by-step instructions to execute disaster recovery for DSR 7.0.1 / 7.1.1/7.2/7.3. Executing this procedure also involves referring to and executing procedures in existing support documents.

Note that components dependent on DSR might need to be recovered as well, for example SDS and IDIH.

1.2 References

[1] DSR 7.2/7.3 Cloud Installation Guide, E64814-04

1.3 Acronyms

Table 1: Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CD	Compact Disk
DSR	Diameter Signaling Router
ESXi	Elastic Sky X Integrated
FABR	Full Address Based Resolution
iDIH	Integrated Diameter Intelligence Hub
IPFE	IP Front End
IWF	Inter Working Function
NAPD	Network Architecture Planning Diagram
OS	Operating System
OVA	Open Virtualization Appliance
PDRA	Policy Diameter Routing Agent
PCA	Policy and Charging Application
RBAR	Range Based Address Resolution
SAN	Storage Area Network
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
TPD	Tekelec Platform Distribution
VM	Virtual Machine

1.4 Terminology

Table 2: Terminology

Base software	Base software includes deploying the VM image.
Failed server	A failed server in disaster recovery context refers to a server that has suffered partial or complete software failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-install the software.
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
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 7.0 PCA Activation and Configuration Procedure, E58667

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 • 1 or more MP 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.	

2.1 Complete Server Outage (All Servers)

This is the worst case scenario where all the servers in the network have suffered complete software failure. The servers are recovered using OVA images 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 OVA images. 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

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 software. Database replication from the active NOAM and SOAM servers will recover the database to all 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 (E64815-02) and hardcopies of all documents in the reference list
2. Hardcopy of all NAPD performed at the initial installation and network configuration of this customer's site. If the NAPD cannot be found, escalate this issue within My Oracle Support (MOS) until the NAPD documents can be located.
3. DSR recent backup files: electronic backup file (preferred) or hardcopy of all DSR configuration and provisioning data.
4. Latest Network Element report: Electronic file or hardcopy of Network Element report.
5. The network element XML file used for the VMs initial configuration.

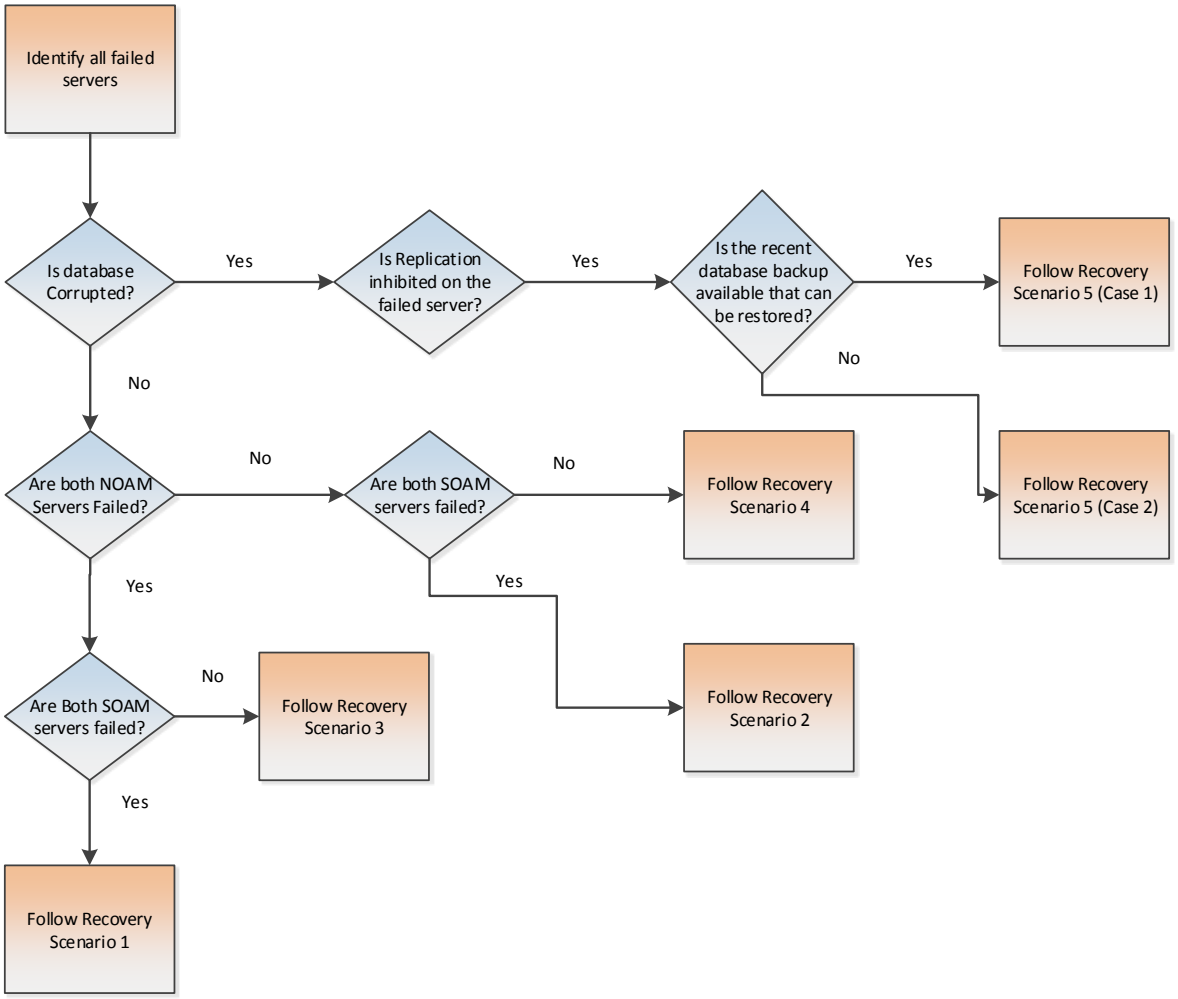
Note: For all Disaster Recovery scenarios, we assume that the NOAM Database backup and the SOAM database backup were performed around the same time, and that no synchronization issues exist among them.

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.
5. Execute appropriate recovery procedures (listed in section 5.0).

Figure 1. Determining Recovery Scenario



4.0 Procedure Preparation

Disaster recovery procedure execution is dependent on the failure conditions in the network. The severity of the failure determines the recovery scenario for the network. Use Table 4: Recovery Scenarios below to evaluate the correct recovery scenario and follow the procedure(s) listed to restore operations.

Note: A failed server in disaster recovery context refers to a server that has suffered partial or complete software failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-deploy base software.

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.	Section 5.1.2 Recovery Scenario 2 (Partial Server Outage with one NOAM server intact and both 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	• 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 5.1.5 Recovery Scenario 5 (Database Recovery)
5: Case 1	• Server is intact • Database gets corrupted on the server • Replication is occurring to the server with corrupted database	Section 5.1.5.1 Recovery Scenario 5: Case 1

5: 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 5.1.5.2 Recovery Scenario 5: Case 2

5.0 Disaster Recovery Procedure

Call the CAS main number at **1-800-223-1711** (toll-free in the United States), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html prior to executing this procedure to ensure that the proper recovery planning is performed.

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

****** WARNING *******

****** WARNING *******

Note: *Disaster recovery is an exercise that requires collaboration of multiple groups and is expected to be coordinated by the TAC prime. Based on TAC's assessment of Disaster, it may be necessary to deviate from the documented process.*

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 7 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 for software and then executing a database restore to the active NOAM server. All other servers are recovered using recovery procedures for 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 . The major activities are summarized as follows:

Recover Base software for all VMs:

- Recover the Virtual Machines hosting the NOAMs and SOAMs
- Recover the **Active NOAM** server by recovering the NOAMs base software
- Recover the NOAM database
- Reconfigure the application

Recover the **Standby NOAM** server by recovering base software, for a Non-HA deployment this can be skipped.

- Reconfigure the DSR Application

Recover all SOAM and MP servers by recovering software, In a Non-HA deployment the Standby/Spare SOAM servers can be skipped.

- Recover the SOAM database
- Reconfigure the DSR Application
- Reconfigure the signaling interface and routes on the MPs, the DSR software will automatically reconfigure the signaling interface from the recovered database.

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.

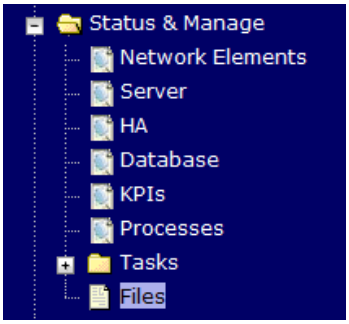
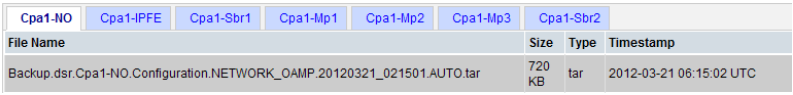
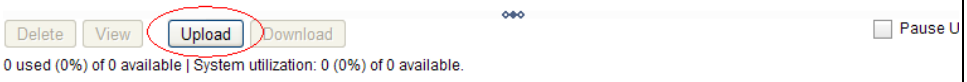
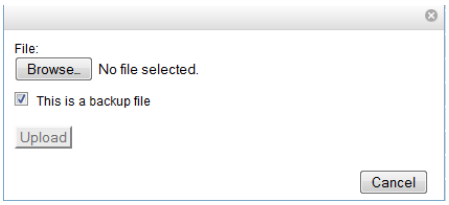
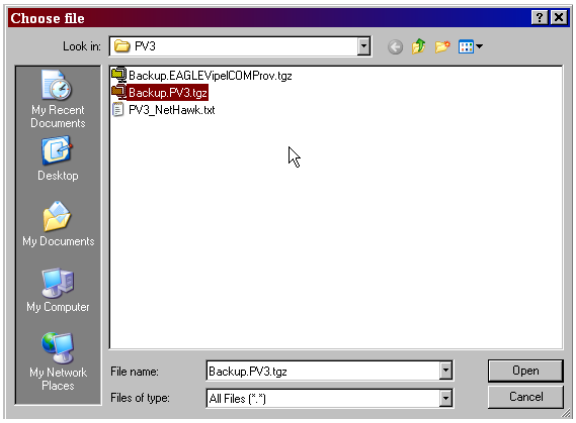
Procedure 1: Recovery Scenario 1

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 E. My Oracle** Support (MOS), and ask for assistance.	
1. ☐	**Workarounds**	Refer to **Appendix D**. 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. ☐	**Recover the Failed Software**	For VMWare based deployments: 1. For NOAM execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA b. Procedure 2 (VMWare Only). Configure NOAM guests role based on resource profile 2. For SOAM execute the following procedures from reference [1]: c. Procedure 1 (VMWare). Import DSR OVA d. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile 3. For failed MPs execute the following procedures from reference [1]: e. Procedure 1 (VMWare). Import DSR OVA f. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile For KVM / Openstack based deployments: 1. For NOAM execute the following procedures from reference [1]: a. Procedure 4 (KVM / Openstack). Import DSR OVA b. Procedure 5 (KVM / Openstack Only). Configure NOAM guests role based on resource profile 2. For SOAM execute the following procedures from reference [1]: c. Procedure 4 (KVM / Openstack). Import DSR OVA d. Procedure 6 (KVM / Openstack Only). Configure Remaining DSR guests based on resource profile 3. For failed MPs execute the following procedures from reference [1]: e. Procedure 4 (KVM / Openstack). Import DSR OVA f. Procedure 6 (KVM / Openstack Only). Configure Remaining DSR guests based on resource profile

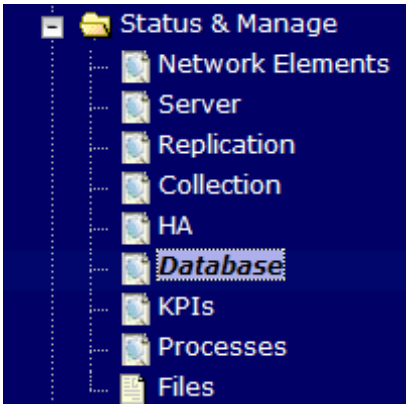
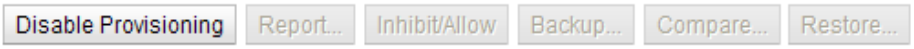
Procedure 1: Recovery Scenario 1

4. ☐	**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.
5. ☐	**Execute DSR Installation Procedure for the First NOAM**	Verify the networking data for Network Elements **Note:** Use the backup copy of network configuration data and site surveys (Step 2) **Execute** installation procedures for the first NOAM server from reference [1]: Procedure 7 “Configure the First NOAM NE and Server” and Procedure 8 “Configure the NOAM Server Group”.
6. ☐	**NOAM GUI:** Login	Login to the NOAM GUI as the ***guiadmin*** user: 

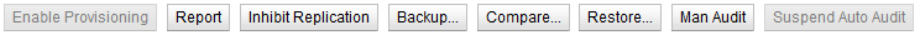
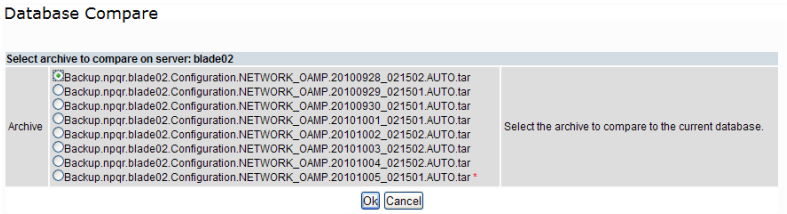
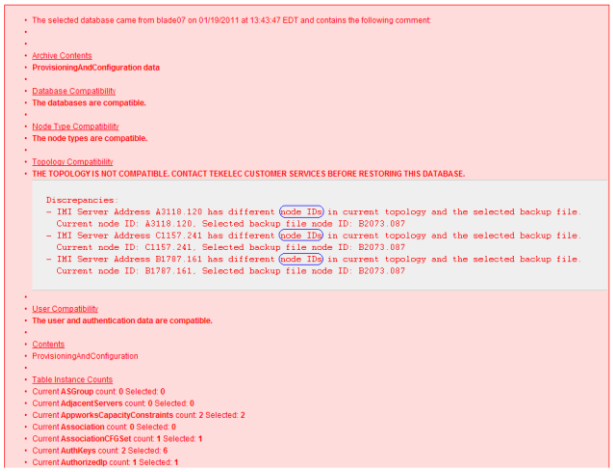
Procedure 1: Recovery Scenario 1

7. ☐	**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:  Click on **Upload** as shown below and select the file *"NO Provisioning and Configuration:"* file backed up after initial installation and provisioning.  1. Click on **Browse** and locate the backup file 2. Check **This is a backup file** Box 3. Click on Open as shown below.   Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.

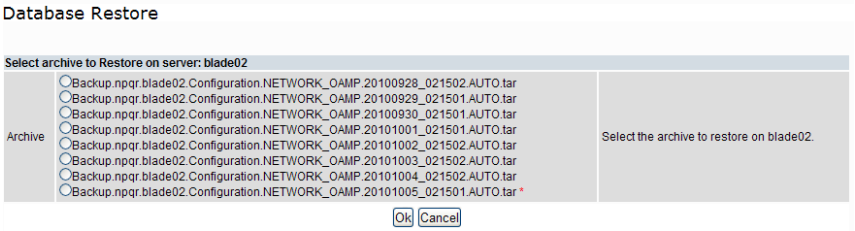
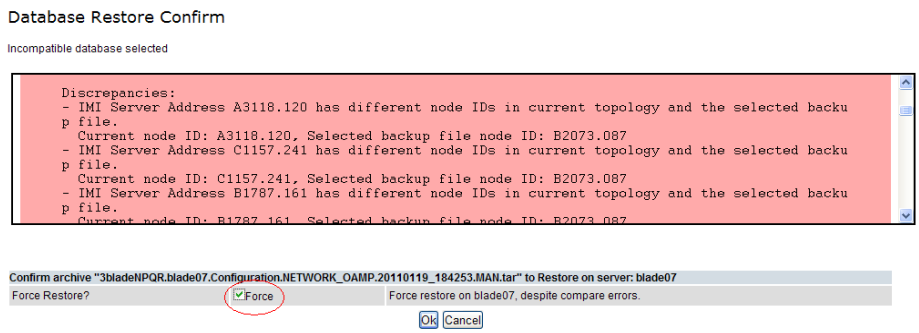
Procedure 1: Recovery Scenario 1

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

Procedure 1: Recovery Scenario 1

9. ☐	**NOAM GUI:** Verify the Archive Contents and Database Compatibility	Select the **Active NOAM** server and click on the **Compare**.  The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 13** of this procedure.  **Verify** that the output window matches the screen below. **Note:** You will get a database mismatch regarding the NodeIDs of the VMs. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix E. My Oracle Support (MOS).  **Note:** Archive Contents and Database Compatibilities must be the following: **Archive Contents:** Configuration data **Database Compatibility:** The databases are compatible. **Note:** The following is expected Output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one NOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. **Note:** We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility. If the verification is successful, Click BACK button, Cancel button and continue to **next step** in this procedure.

Procedure 1: Recovery Scenario 1

10. ☐	**ACTIVE NOAM:** Restore the Database	Click on **Main Menu->Status & Manage->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.  Click **OK** Button. The following confirmation screen will be displayed. **Note:** You will get a database mismatch regarding the NodeIDs of the servers. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix E. My Oracle Support (MOS). Select the **Force** checkbox as shown above and Click **OK** to proceed with the DB restore.  **Note:** After the restore has started, the user will be logged out of XMI NO GUI since the restored Topology is old data.

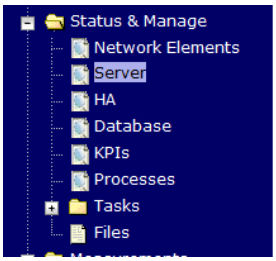
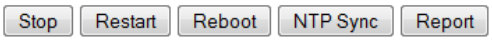
Procedure 1: Recovery Scenario 1

11. ☐	**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: 
12. ☐	**NOAM VIP GUI:** Monitor and Confirm database restoral	Wait for **5-10 minutes** for the System to stabilize with the new topology: Monitor the Info tab for **"Success"**. This will indicate that the backup is complete and the system is stabilized. Following alarms **must** be ignored for NOAM and MP Servers until all the Servers are configured: Alarms with Type Column as **"REPL"** , **"COLL", "HA"** (with mate NOAM), **"DB"** (about Provisioning Manually Disabled) **Note:** Do not pay attention to alarms until all the servers in the system are completely restored. **Note:** The Configuration and Maintenance information will be in the same state it was backed up during initial backup.
13. ☐	**ACTIVE NOAM:** Login	Login to the recovered Active NOAM via SSH terminal as ***admusr*** user.

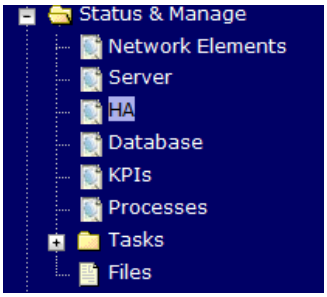
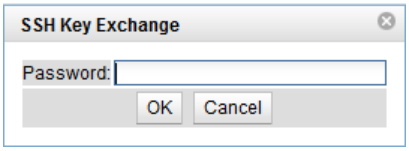
Procedure 1: Recovery Scenario 1

14. ☐	**ACTIVE NOAM:** Restore /etc/hosts/ File of the Active NOAM	**IF DSR 7.1 or later, SKIP THIS STEP** Execute the following command: `$ sudo AppWorks AppWorks_AppWorks updateServerAliases <NOAM Host Name>`
15. ☐	**NOAM VIP GUI:** Recover Standby NOAM (**OPTIONAL**) for Non-HA sites.	**NOTE:** For Non-HA sites **SKIP** this step. Install the second NOAM server by executing procedures from reference [1]: Procedure 9 “Configure the Second NOAM Server” steps 1, 3-7 Procedure 10 “Complete Configuring the NOAM Server Group” Step 5

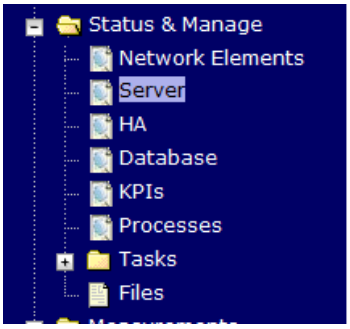
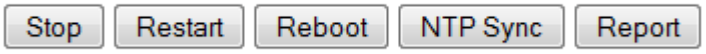
16. ☐	**Active NOAM:** Correct the RecognizedAuthority table	Establish an SSH session to the active NOAM, login as ***admusr***.
		
		Execute the following command:
		
		`$ sudo top.setPrimary`
		`- Using my cluster: A1789`
		`- New Primary Timestamp: 11/09/15 20:21:43.418`
		`- Updating A1789.022: <DSR_NOAM_B_hostname>`
		`- Updating A1789.144: <DSR_NOAM_A_hostname>`

17. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered standby NOAM server and click on **Restart**. 

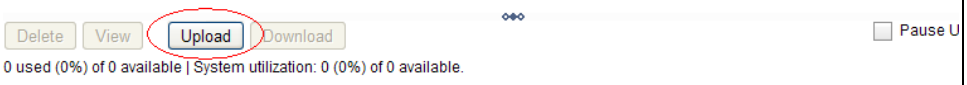
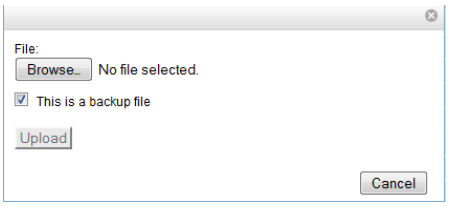
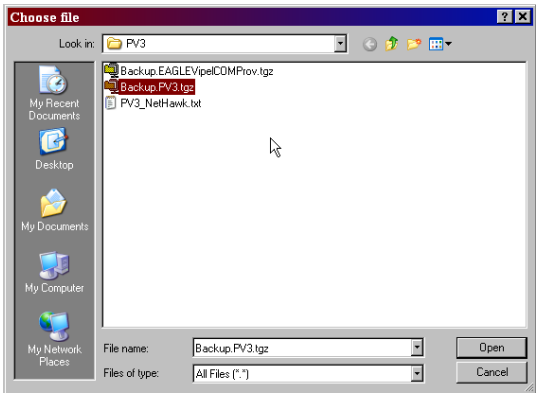
Procedure 1: Recovery Scenario 1

18. ☐	**NOAM VIP GUI:** Set HA on Standby NOAM	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**
19. ☐	**NOAM VIP GUI:** Perform Keyexchange with Export Server	Navigate to **Main Menu -> Administration -> Remote Servers -> Data Export**  Click on **SSH Key Exchange** at the bottom of the screen Enter the Password and press **OK** 
20. ☐	**NOAM VIP GUI:** Stop Replication to the C-Level Servers of this Site.	Inhibit Replication to the working C Level Servers which belong to the **same site** as of the failed SOAM servers, as the recovery of Active SOAM will cause the database wipeout in the C level servers because of the replication Execute **Appendix B**. Inhibit A and B Level Replication on C-Level Servers

Procedure 1: Recovery Scenario 1

21. ☐	**NOAM VIP GUI:** Recover Active SOAM Server	Install the SOAM servers by executing procedure from reference [1]: 1.2 References Procedure 12 “Configure the SOAM Servers”, steps 1, 3- 7 **NOTE:** Wait for server to reboot before continuing.
22. ☐	**NOAM VIP GUI:** Restart DSR application on Recovered Active SOAM Server	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered server and click on **Restart**. 

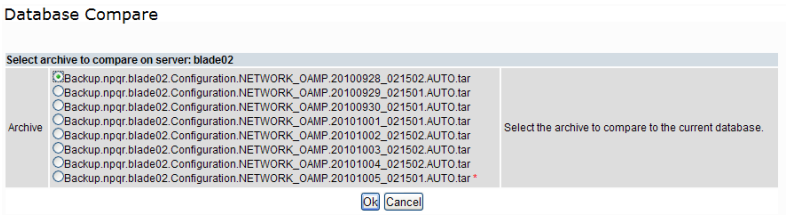
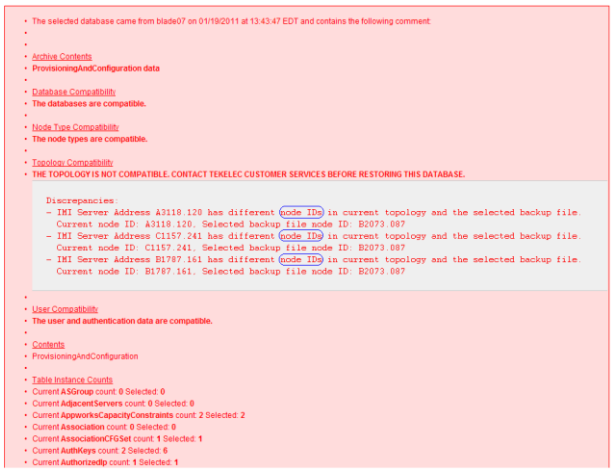
Procedure 1: Recovery Scenario 1

23. ☐	**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.  1. Click on **Browse** and locate the backup file 2. Check **This is a backup file** Box 3. Click on Open as shown below.   Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.

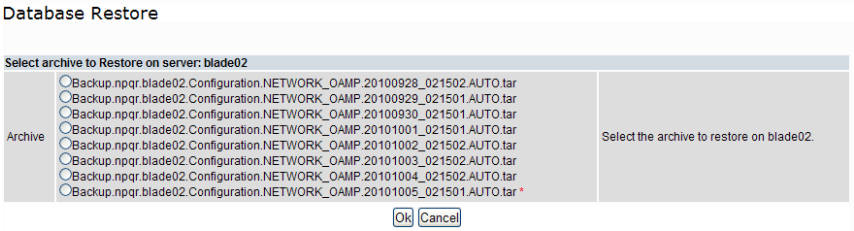
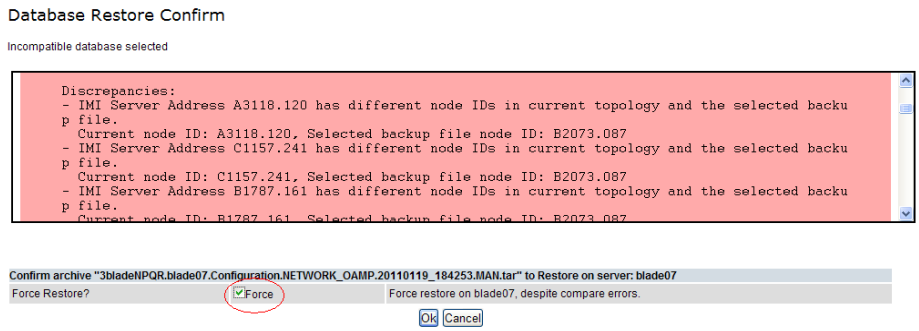
Procedure 1: Recovery Scenario 1

24. ☐	**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: 

Procedure 1: Recovery Scenario 1

25. ☐	**Recovered SOAM GUI:** Verify the Archive Contents and Database Compatibility	Navigate to **Main Menu->Status & Manage->Database** Select the **Active SOAM** server and click on the **Compare**.  The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 13** of this procedure.  **Verify** that the output window matches the screen below. **Note:** You will get a database mismatch regarding the NodeIDs of the VMs. That is expected. If that is the only mismatch, proceed, otherwise stop and contact **Appendix E. My Oracle** Support (MOS)  **Note:** Archive Contents and Database Compatibilities must be the following: **Archive Contents:** Configuration data **Database Compatibility:** The databases are compatible. **Note:** The following is expected Output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. **Note:** We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility. If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.

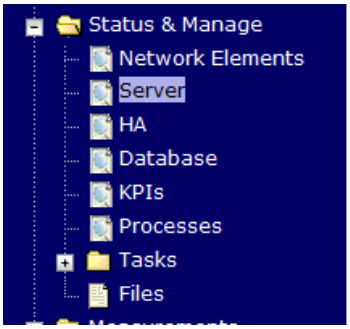
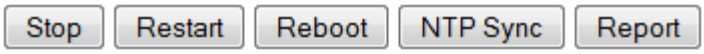
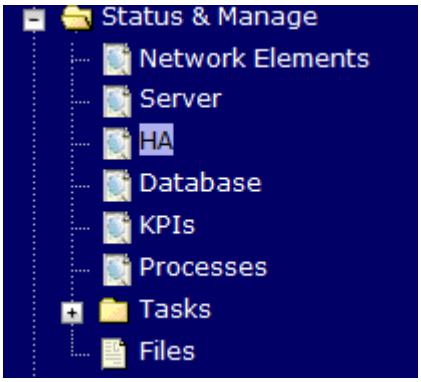
Procedure 1: Recovery Scenario 1

26. ☐	**Recovered SOAM GUI:** Restore the Database	Click on **Main Menu->Status & Manage->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.  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 below and Click **OK** to proceed with the DB restore.  **Note:** After the restore has started, the user will be logged out of XMI SOAM GUI since the restored Topology is old data.
27. ☐	**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 backup 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.

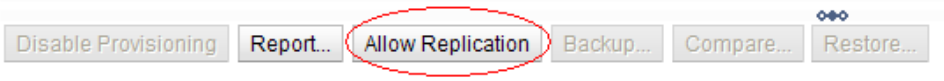
Procedure 1: Recovery Scenario 1

28. ☐	**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: 
29. ☐	**NOAM VIP GUI:** Recover remaining SOAM Server (**OPTIONAL**) for Non-HA sites	**NOTE:** For Non-HA sites **SKIP** this step. Install the SOAM servers by executing procedure from reference [1] Procedure 12 “Configure the SOAM Servers”, steps 1, 3- 6 **NOTE:** Wait for server to reboot before continuing.

Procedure 1: Recovery Scenario 1

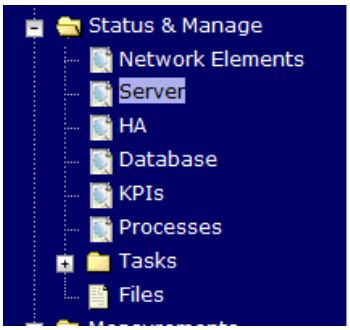
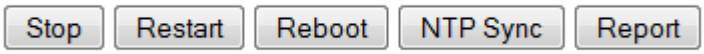
30.	**NOAM VIP GUI:** Restart DSR application on remaining SOAM Server(s) (**OPTIONAL**) for Non-HA sites	**NOTE:** For Non-HA sites **SKIP** this step. Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered server and click on **Restart**. 
31. ☐	**NOAM VIP GUI:** Set HA on Recovered Standby SOAM Server (**OPTIONAL**) for Non-HA sites	**NOTE:** For Non-HA sites **SKIP** this step. Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Set Max Allowed HA Role to **Active** Press **OK**

Procedure 1: Recovery Scenario 1

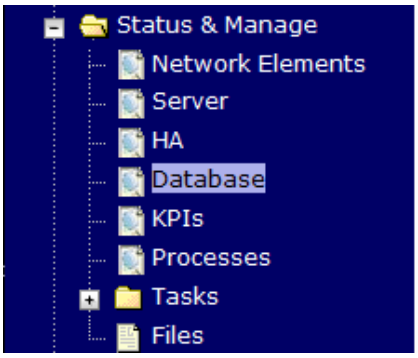
32. ☐	**NOAM VIP GUI:** Start Replication on Working C-Level Servers	Un-Inhibit *(Start)* Replication to the **working** C-Level Servers which belong to the same site as of the failed SOAM servers. Execute **Appendix C**. Un-Inhibit A and B Level Replication on C-Level Servers Navigate to **Main Menu->Status & Manage->Database** 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)* • 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". 

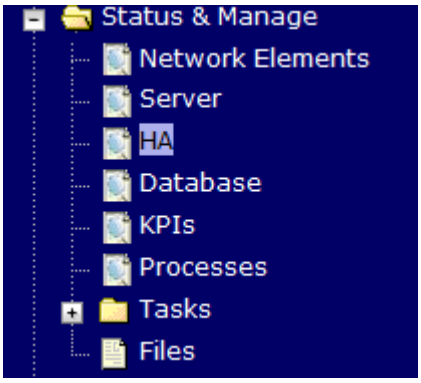
33. ☐	**NOAM VIP GUI:** Recover the C-Level Server (DA-MP, SBRs, IPFE, SS7-MP)	Establish a SSH session to the C Level server being recovered, login as ***admusr.***
		
		Execute following command to set shared memory to unlimited:
		
		`$ sudo shl.set -m 0`
		
		Execute following command ONLY when the recovered C-Level server is of type IPFE:
		
		`$ sudo ipfeNetUpdate.sh`
		
		Execute the following procedures from [1] **FOR EACH** server that has been recovered:
		
		Procedure 15 "Configure the MP Virtual Machines", Steps 1, 4-11.

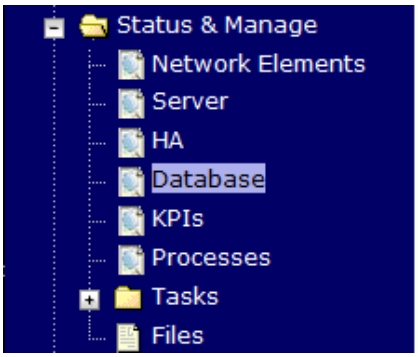
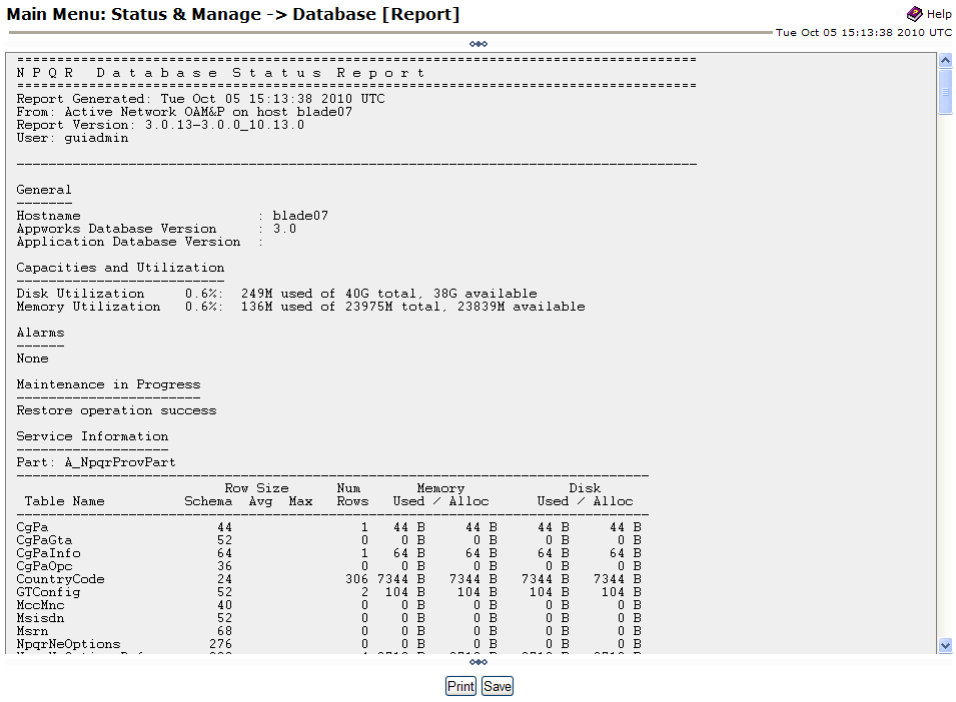
Procedure 1: Recovery Scenario 1

34. ☐	**NOAM VIP GUI:** Restart DSR application for Recovered C-Level Server	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered server and click on **Restart**. 

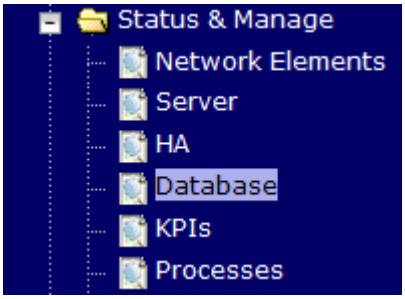
Procedure 1: Recovery Scenario 1

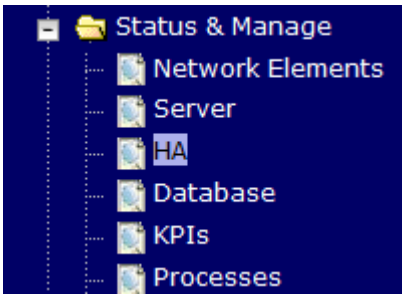
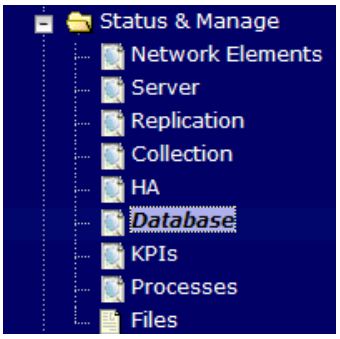
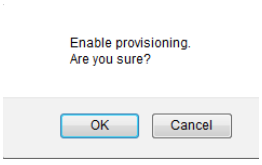
35. ☐	**NOAM VIP GUI:** Start Replication on all C-Level Servers	Un-Inhibit *(Start)* Replication to the **ALL** C-Level Servers Navigate to **Status & Manage -> Database**  If the *"Repl Status"* is set to "Inhibited", click on the Allow Replication button as shown below using the following order: • Active NOAM Server • Standby NOAM Server • Active SOAM Server • Standby SOAM Server • Spare SOAM Server *(if applicable)* • 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". 

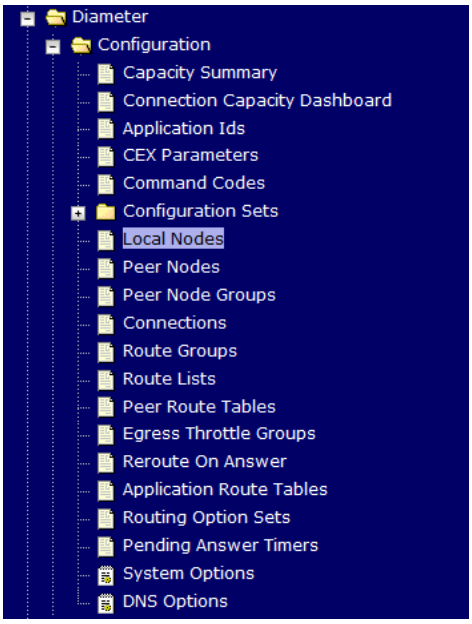
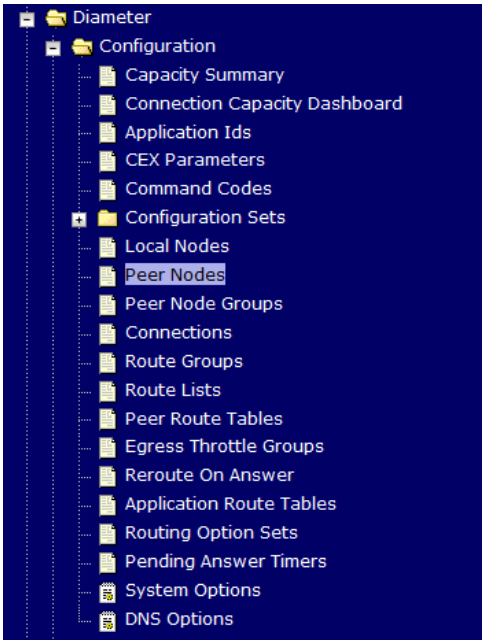
36. ☐	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen For each server whose Max Allowed HA Role is set to Standby, set it to **Active** Press **OK**
37. ☐	**ACTIVE NOAM:** Perform key exchange between the active-NOAM 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.
38. ☐	**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.

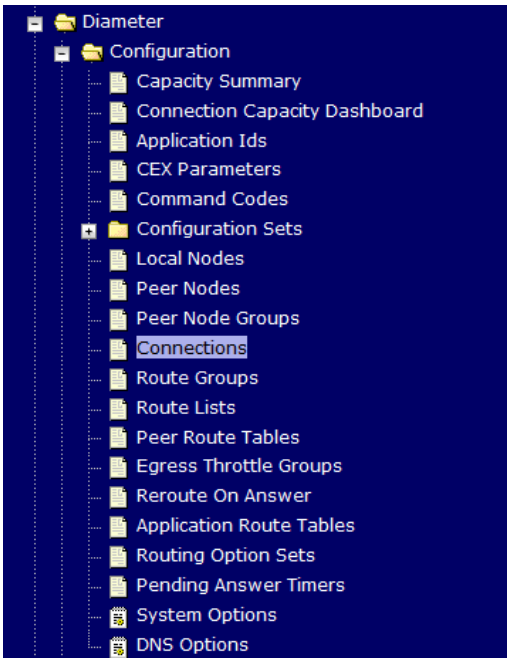
39. ☐	**NOAM VIP GUI:** Fetch and Store the database Report for the Newly Restored Data and Save it	Navigate to **Main Menu->Status & Manage->Database**  Select the **active** NOAM server and click on the **Report** button at the bottom of the page. The following screen is displayed:  Click on **Save** and save the report to your local machine.

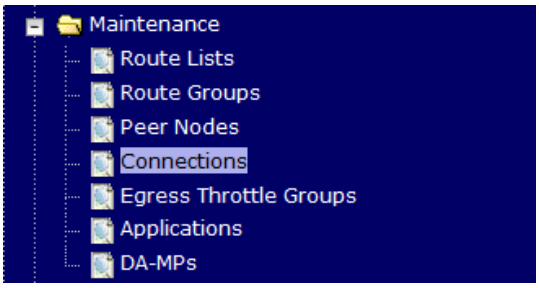
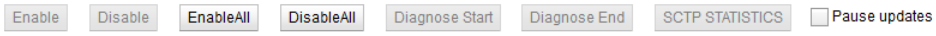
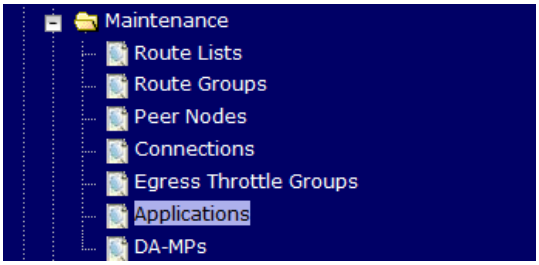
40. ☐	**ACTIVE NOAM:** Verify Replication Between Servers.	Login to the Active NOAM via SSH terminal as ***admusr*** user.
		Execute the following command:
		$ sudo irepstat –m
		Output like below shall be generated:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`RDU06-MP1 -- Stby`
		`BC From RDU06-SO1 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`
		Ctrl+c to exit the screen.

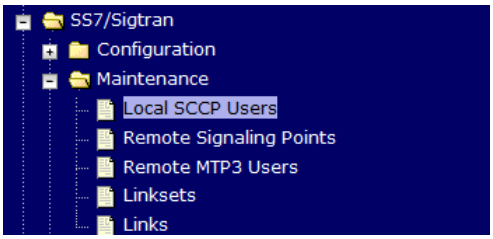
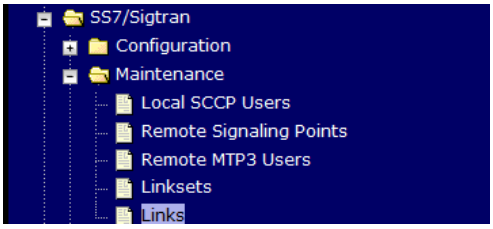
41. ☐	**NOAM VIP GUI:** Verify the Database states	Click on **Main Menu->Status and Manager->Database**  Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below: Network Element | 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

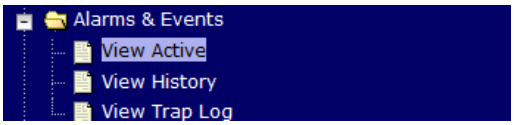
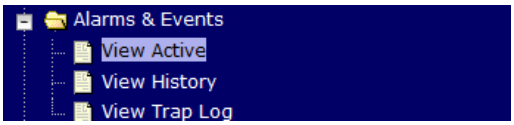
42. ☐	**NOAM VIP GUI:** Verify the HA Status	Click on **Main Menu->Status and Manage->HA**  Select the row for all of the servers Verify that the "OAM HA Role" is either "Active" or "Standby". Hostname | OAM Max HA Role | Application Max HA Role | Max Allowed HA Role | Mate Hostname List | Network Element | 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 |
43.	**NOAM GUI:** Enable Provisioning	Click on **Main Menu->Status & Manage->Database**  Enable Provisioning by clicking on **Enable Provisioning** button at the bottom of the screen as shown below.  A confirmation window will appear, press **OK** to enable Provisioning. 

44. ☐	**SOAM VIP GUI:** Verify the Local Node Info	Navigate to **Main Menu->Diameter->Configuration->Local Node**  Verify that all the local nodes are shown.
45. ☐	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.

46. ☐	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections**  Verify that all the connections are shown.
47.	**MP Servers:** Disable SCTP Auth Flag (DSR 7.1 Only)	For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [1]. Execute this procedure on all Failed MP Servers.

48. ☐	**SOAM VIP GUI:** Enable Connections if needed	Navigate to **Main Menu->Diameter->Maintenance->Connections**  Select each connection and click on the **Enable** button. Alternatively you can enable all the connections by selecting the **EnableAll** button.  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
49. ☐	**SOAM VIP GUI:** Enable Optional Features	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Select the optional feature application configured before. Click the **Enable** button. 

50.	**SOAM VIP GUI:** Re-enable Transports if Needed [Applicable when MAP-IWF application is activated]	Navigate to **Main Menu->Transport Manager -> Maintenance -> Transport**  Select each transport and click on the **Enable** button  Verify that the Operational Status for each transport is Up.
51.	**SOAM VIP GUI:** Re-enable MAPIWF application if needed [Applicable when MAP-IWF application is activated]	Navigate to **Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users**  Click on the **Enable** button corresponding to MAPIWF Application Name.  Verify that the SSN Status is Enabled.
52.	**SOAM VIP GUI:** Re-enable links if needed [Applicable when MAP-IWF application is activated]	**DSR Only, if SDS (Oracle X5-2 Only), Skip This Step** Navigate to **Main Menu->SS7/Sigtran->Maintenance->Links**  Click on **Enable** button for each link.  Verify that the Operational Status for each link is Up.

53. ☐	**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 E. My Oracle** Support (MOS).
54. ☐	**NOAM VIP GUI:** Examine All Alarms	Login to the NOAM VIP if not already logged in. Navigate to **Main Menu->Alarms & Events->View Active**  Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix E. My Oracle** Support (MOS).
55. ☐	**Restore GUI Usernames and Passwords**	If applicable, Execute steps in **Section 6.0** to recover the user and group information restored.
56. ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**. DSR Database Backup to back up the Configuration databases:

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

For a partial server outage with an NOAM server intact and available; SOAM servers are recovered using recovery procedures for 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 for 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 software and the database.

- Recover the software.

Recover **Active SOAM** server by recovering software.

- Recover the software.
- Recover the Database.

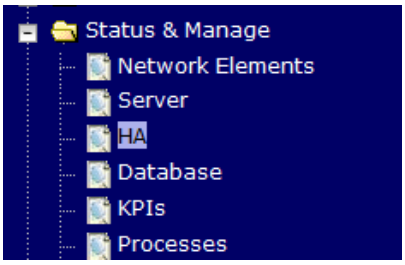
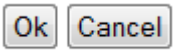
Recover any failed **SOAM and MP** servers by recovering software.

- 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 E. My Oracle Support (MOS), and ask for assistance.	
1. ☐	**Workarounds**	Refer to **Appendix D**. Workarounds for Issues not fixed in this Releaseto 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: 

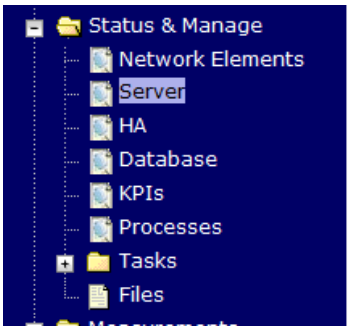
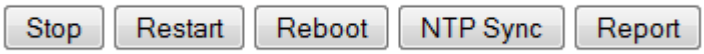
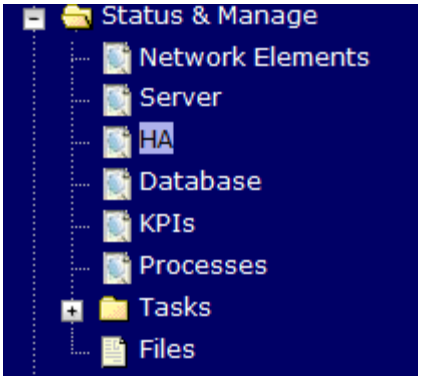
Procedure 2: Recovery Scenario 2

4. ☐	**Active NOAM:** Set Failed Servers to Standby	Navigate to **Main Menu -> Status & Manage -> HA**  Select **Edit** Set the Max Allowed HA Role drop down box to **Standby** for the failed servers. Select **Ok** 
5. ☐	**Create VMs Recover the Failed Software**	For VMWare based deployments: 1. For NOAM execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA b. Procedure 2 (VMWare Only). Configure NOAM guests role based on resource profile 2. For SOAM execute the following procedures from reference [1]: c. Procedure 1 (VMWare). Import DSR OVA d. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile For KVM/Openstack based deployments: 1. For NOAM execute the following procedures from reference [1]: a. Procedure 4 (KVM/Openstack). "Import DSR OVA" b. Procedure 5 (KVM/Openstack). "Configure NOAM guests role based on resource profile" 2. For SOAM execute the following procedures from reference [1]: c. Procedure 4 (KVM/Openstack). "Import DSR OVA" d. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests role based on resource profile"
6. ☐	**Repeat for Remaining Failed Servers**	If necessary, repeat **step 5** for all remaining failed servers.

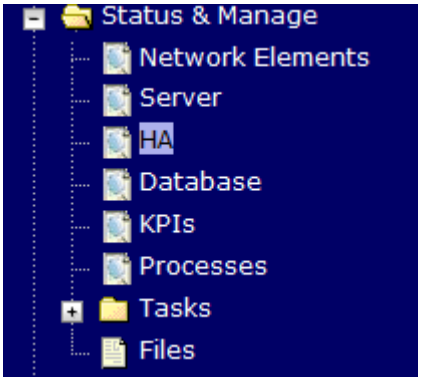
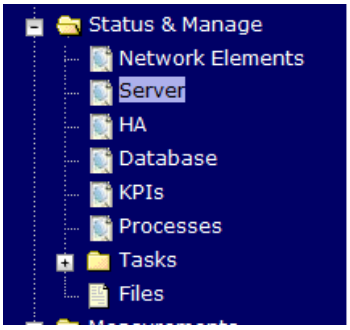
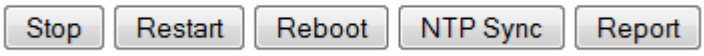
Procedure 2: Recovery Scenario 2

7. ☐	**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: 
8. ☐	**NOAM VIP GUI:** Recover Standby NOAM	Install the second NOAM server by executing procedures from reference [1]: Procedure 9 “Configure the Second NOAM Server” steps 1, 3-7 Procedure 10 “Complete Configuring the NOAM Server Group” Step 5 **Note:** If Topology or nodeId alarms are persistent after the database restore, refer to Appendix D. Workarounds for Issues not fixed in this Release or the next step below.

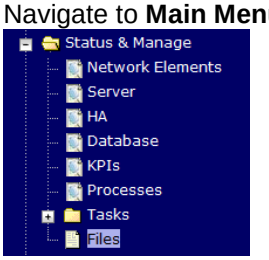
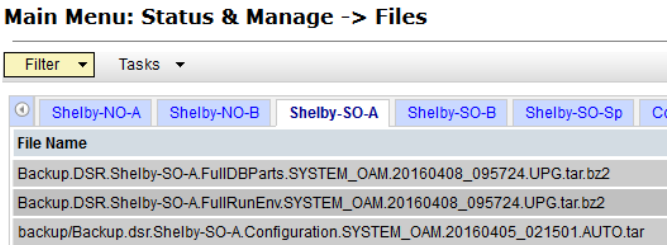
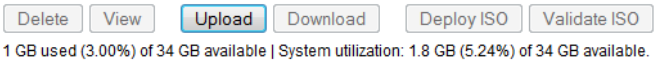
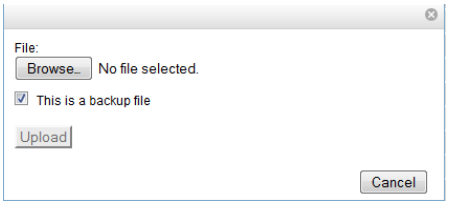
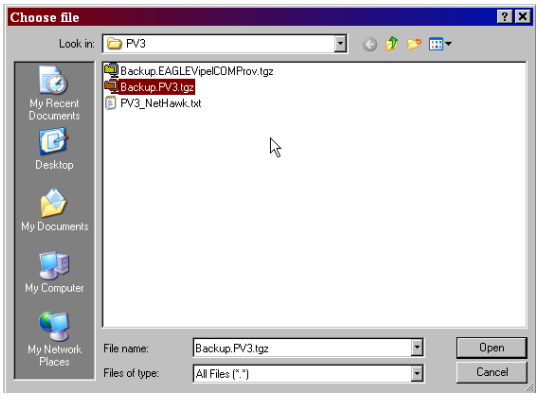
Procedure 2: Recovery Scenario 2

9.	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered standby NOAM server and click on **Restart**. 
10.	**NOAM VIP GUI:** Set HA on Standby NOAM	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**
11.	**NOAM VIP GUI:** Stop Replication to the C-Level Servers of this Site.	Inhibit Replication to the working C Level Servers which belong to the **same site** as the failed SOAM servers, as the recovery of Active SOAM will cause the database wipeout in the C level servers because of the replication  Execute **Appendix B**. Inhibit A and B Level Replication on C-Level Servers 

Procedure 2: Recovery Scenario 2

12. ☐	**NOAM VIP GUI:** Recovered Active SOAM Server	Install the SOAM servers by executing procedure from reference [1]: Procedure 12 “Configure the SOAM Servers”, steps 1, 3- 6 **NOTE:** Wait for server to reboot before continuing.
13.	**NOAM VIP GUI:** Set HA on Active SOAM	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Select the Active SOAM server, set it to **Active** Press **OK**
14.	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered Active SOAM server and click on **Restart**. 

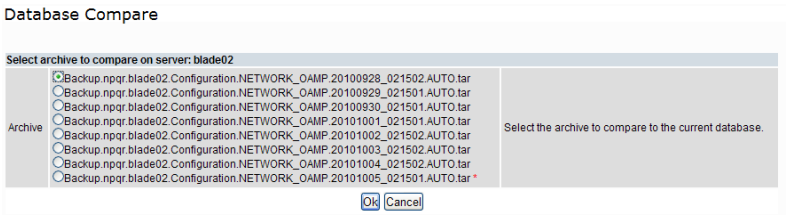
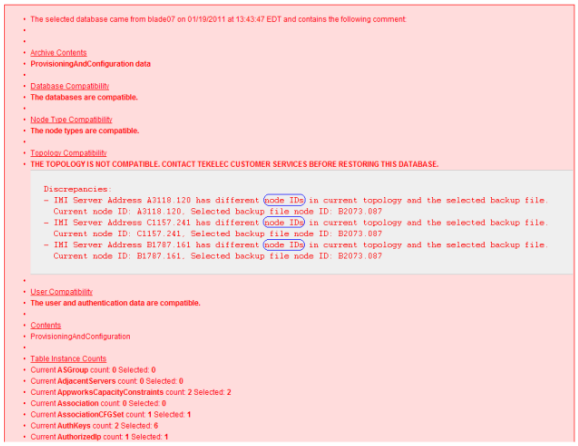
Procedure 2: Recovery Scenario 2

15. ☐	**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 *"NO Provisioning and Configuration:"* file backed up after initial installation and provisioning.  1. Click on **Browse** and locate the backup file 2. Check **This is a backup file** Box 3. Click on Open as shown below.   Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.

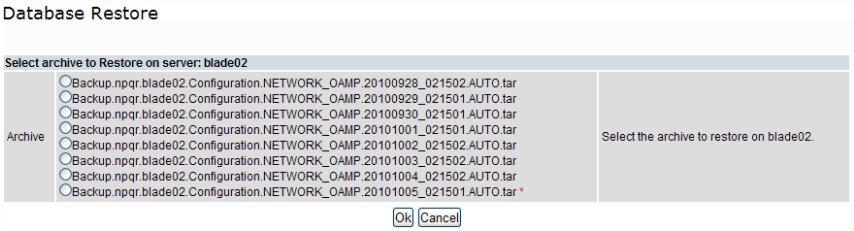
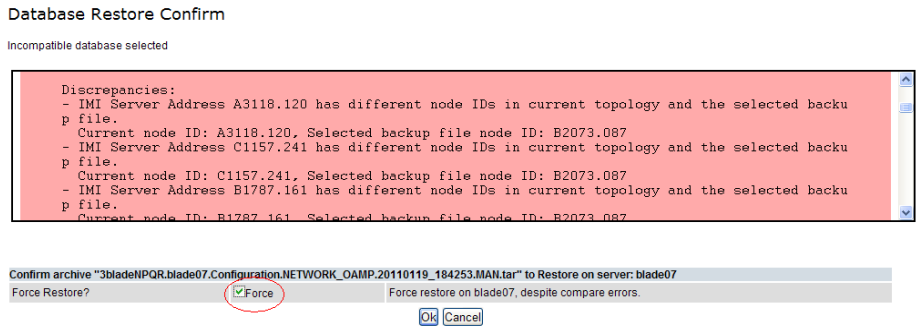
Procedure 2: Recovery Scenario 2

16. ☐	**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: 

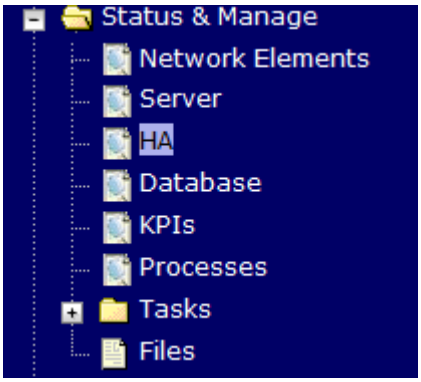
Procedure 2: Recovery Scenario 2

17. ☐	**Recovered SOAM GUI:** Verify the Archive Contents and Database Compatibility	Navigate to **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 15** of this procedure.  **Verify** that the output window matches the screen below. **Note:** You will get a database mismatch regarding the NodeIDs of the VMs. That is expected. If that is the only mismatch, proceed, otherwise stop and contact **Appendix E. My Oracle** Support (MOS)  **Note:** Archive Contents and Database Compatibilities must be the following: **Archive Contents:** Configuration data **Database Compatibility:** The databases are compatible. **Note:** The following is expected Output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. **Note:** We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility. If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.

Procedure 2: Recovery Scenario 2

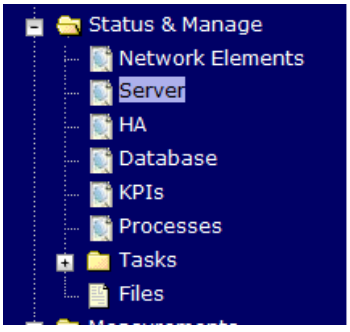
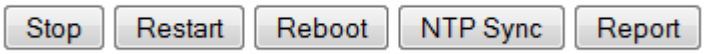
18. ☐	**Recovered SOAM GUI:** Restore the Database	Click on **Main Menu->Status & Manage->Database** Select the **Active SOAM** server, and click on **Restore** as shown below. The following screen will be displayed. Select the proper back up provisioning and configuration file.  Click **OK** Button. The following confirmation screen will be displayed. **Note:** You will get a database mismatch regarding the NodeIDs of the servers. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix E. My Oracle Support (MOS). Select the **Force** checkbox as shown above and Click **OK** to proceed with the DB restore.  **Note:** After the restore has started, the user will be logged out of XMI SOAM GUI since the restored Topology is old data.
19. ☐	**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 backup 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.

Procedure 2: Recovery Scenario 2

20. ☐	**NOAM VIP GUI:** Recover remaining SOAM Server **(OPTIONAL)** for Non-HA sites	**NOTE:** For **Non-HA** sites **SKIP** this step Install the SOAM servers by executing procedure from reference [1]: Procedure 12 “Configure the SOAM Servers”, steps 1, 3- 6 **NOTE:** Wait for server to reboot before continuing.
21.	**NOAM VIP GUI:** Set HA on SOAM Servers **(OPTIONAL)** for Non-HA sites	**NOTE:** For **Non-HA** sites **SKIP** this step Navigate to **Status & Manage -> HA**  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

22.	**Recovered Server:** Sync NTP	1) Perform the following to retrieve the remote NTP server:
		`$ sudo ntpq -np`
		Example output:
		`[admusr@NOAM-2 ~]$ ntpq -np`
		`remote refid st t when poll reach delay offset jitter`
		`==============================================================================`
		`*10.240.9.186 10.250.33.2 3 u 356 1024 377 1.409 0.113 2.434`
		2) Stop ntpd service:
		`$ sudo service ntpd stop`
		3) Sync the date to the ntp remote server:
		`$ sudo ntpdate <NTP remote server>`
		Note: The remote server below will be that of the one gathered in sub step 1.
		4) Start the ntp service:
		`$ sudo service ntpd start`

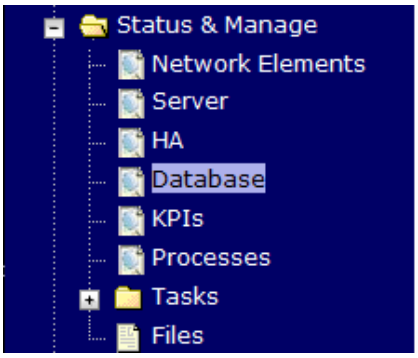
23.	**NOAM VIP GUI:** Restart DSR application **(OPTIONAL)** for Non-HA sites	**NOTE:** For **Non-HA** sites **SKIP** this step Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered server and click on **Restart**.  5)

Procedure 2: Recovery Scenario 2

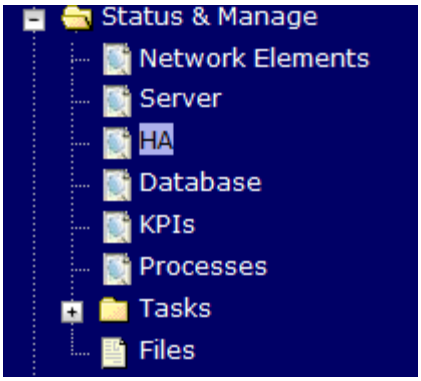
24. ☐	**NOAM VIP GUI:** Start Replication on working C-Level Servers	Un-Inhibit *(Start)* Replication to the **working** C-Level Servers which belong to the same site as of the failed SOAM servers. Execute **Appendix C**. Un-Inhibit A and B Level Replication on C-Level Servers Navigate to **Main Menu->Status & Manage->Database** 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)* • 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". 

25. ☐	**NOAM VIP GUI:** Recover the C-Level Server (DA-MP, SBRs, IPFE, SS7-MP)	Establish a SSH session to the C Level server being recovered, login as ***admusr.***
		
		Execute following command to set shared memory to unlimited:
		
		`$ sudo shl.set -m 0`
		
		Execute following command ONLY when the recovered C-Level server is of type IPFE:
		
		`$ sudo ipfeNetUpdate.sh`
		
		Execute the following procedures from [1] **FOR EACH** server that has been recovered:
		
		Procedure 15 "Configure the MP Virtual Machines", Steps 1, 4-11.

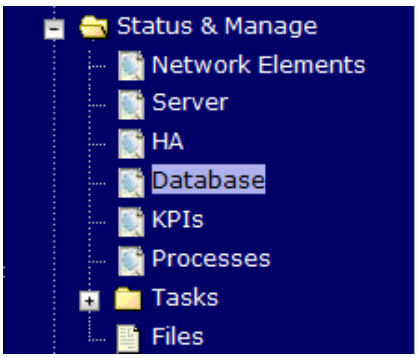
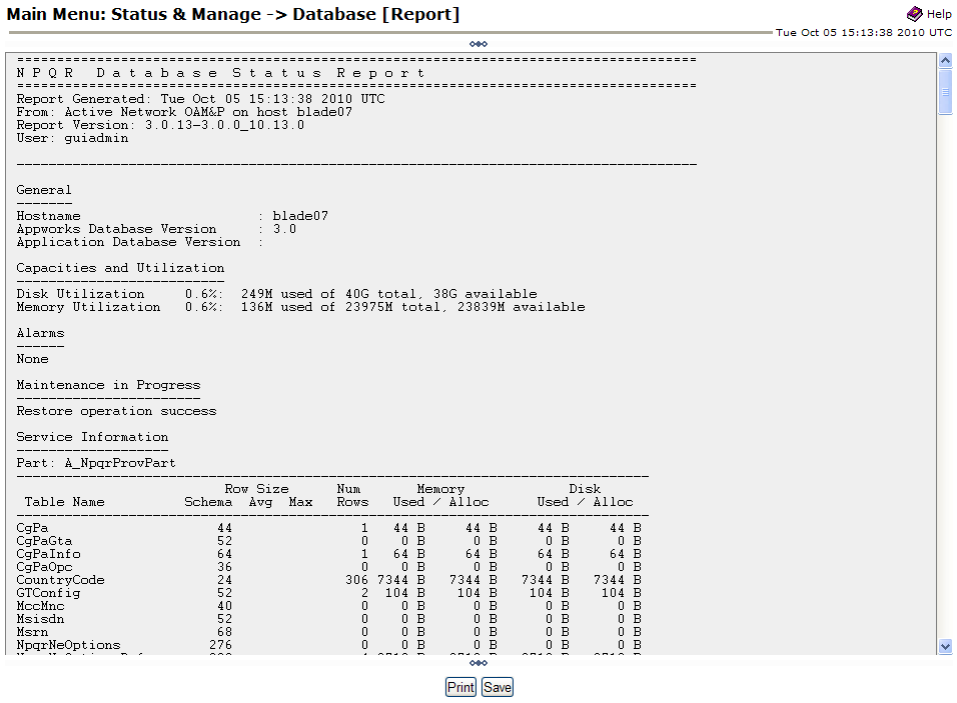
Procedure 2: Recovery Scenario 2

26. ☐	**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**  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)* • 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". 

Procedure 2: Recovery Scenario 2

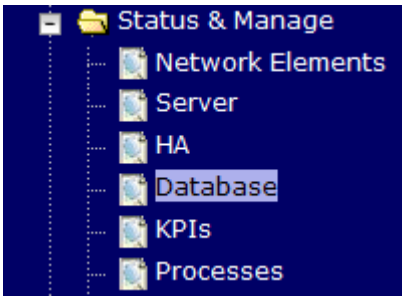
27. ☐	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen For each server whose Max Allowed HA Role is set to Standby, set it to **Active** Press **OK**
28. ☐	**Active SOAM:** Prepare recovered SOAM for optional feature activation	If DSR 7.1, skip this step Establish an SSH session to the Active SOAM, login as ***admusr.*** Execute the following command: `$ irem DsrApplication where "name in ('RBAR','FABR','PCA','MD-IWF','DM-IWF','CPA','GLA')"`
29. ☐	**Active SOAM:** Verify Preparation	If DSR 7.1, skip this step Execute the following command to verify preparation of optional feature activation: `$ iqt -z -h -p -fname DsrApplication where "name in ('RBAR','FABR','PCA','MD-IWF','DM-IWF','CPA','GLA')"` **Note:** There should be no output of this command, if there is, verify the correct entry of the command in **step 28**.
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>` **Note:** If an export server is configured, perform this step.

Procedure 2: Recovery Scenario 2

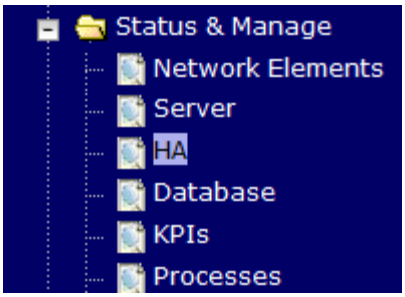
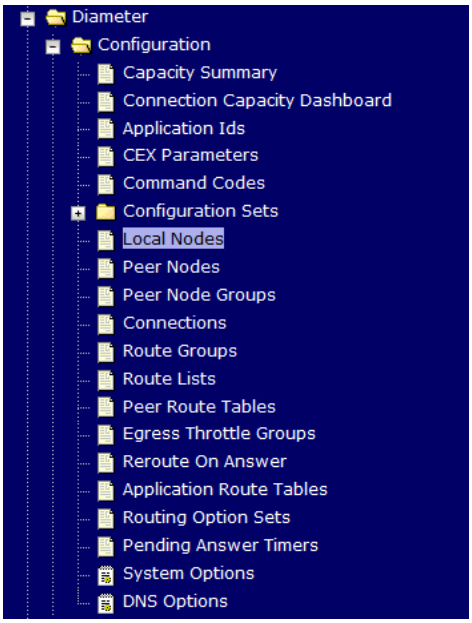
31. ☐	**ACTIVE NOAM:** Activate Optional Features	Establish an SSH session to the active NOAM, login as ***admusr.*** Refer to **section** 1.5 Optional Features to activate any features that were previously activated.
32. ☐	**NOAM VIP GUI:** Fetch and Store the database Report for the Newly Restored 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:  Click on **Save** and save the report to your local machine.

Procedure 2: Recovery Scenario 2

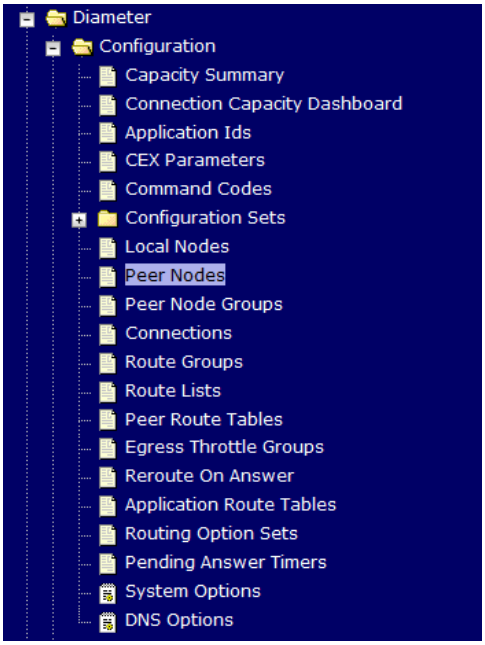
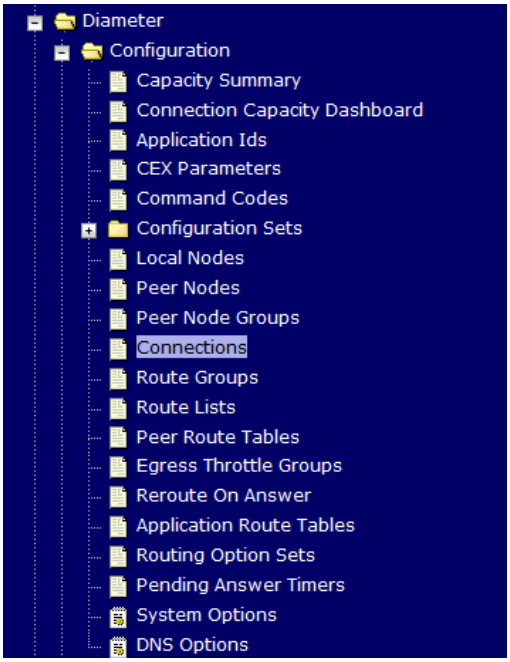
33. ☐	**ACTIVE NOAM:** Verify Replication Between Servers.	Login to the Active NOAM via SSH terminal as ***admusr*** user.
		Execute the following command:
		$ sudo irepstat –m
		Output like below shall be generated:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`RDU06-MP1 -- Stby`
		`BC From RDU06-SO1 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`
		Ctrl+c to exit the screen.

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

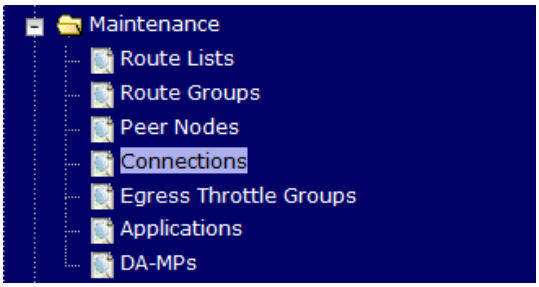
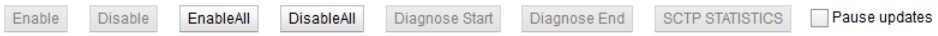
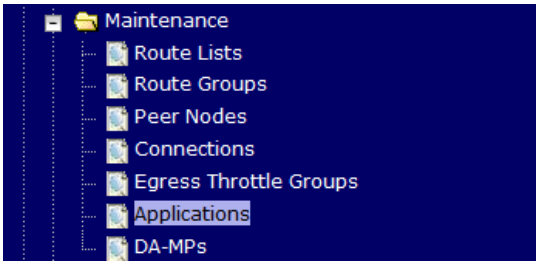
Procedure 2: Recovery Scenario 2

35. ☐	**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 "OAM 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 |
36. ☐	**SOAM VIP GUI:** Verify the Local Node Info	Navigate to **Main Menu->Diameter->Configuration->Local Node**  Verify that all the local nodes are shown.

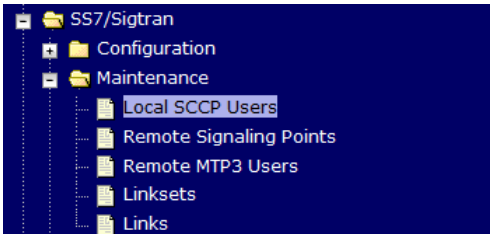
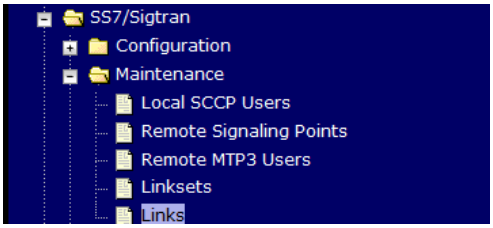
Procedure 2: Recovery Scenario 2

37. ☐	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.
38. ☐	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections**  Verify that all the connections are shown.

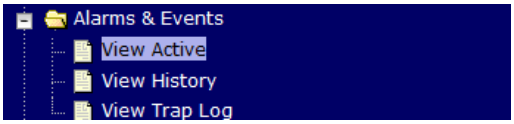
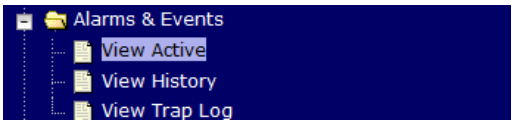
Procedure 2: Recovery Scenario 2

39.	**MP Servers:** Disable SCTP Auth Flag (DSR 7.1 Only)	For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [1]. Execute this procedure on all Failed MP Servers.
40. ☐	**SOAM VIP GUI:** Enable Connections if needed	Navigate to **Main Menu->Diameter->Maintenance->Connections**  Select each connection and click on the **Enable** button. Alternatively you can enable all the connections by selecting the **EnableAll** button.  Verify that the Operational State is Available.
41. ☐	**SOAM VIP GUI:** Enable Optional Features	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Select the optional feature application configured in **step 31**. Click the **Enable** button. 

Procedure 2: Recovery Scenario 2

42.	**SOAM VIP GUI:** Re-enable Transports if Needed	Navigate to **Main Menu->Transport Manager -> 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**  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**  Click on **Enable** button for each link.  Verify that the Operational Status for each link is Up.

Procedure 2: Recovery Scenario 2

45. ☐	**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 E. My Oracle** Support (MOS).
46. ☐	**NOAM VIP GUI:** Examine All Alarms	Login to the NOAM VIP if not already logged in. Navigate to **Main Menu->Alarms & Events->View Active**  Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix E. My Oracle** Support (MOS).
47. ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**. DSR Database Backup to back up the Configuration databases:

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

For a partial server outage with an SOAM server intact and available; NOAM servers are recovered using recovery procedures for 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. All other servers are recovered using recovery procedures for 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 software and the database.

- Recover the software.
- Recover the database

Recover **Standby NOAM servers** by recovering software.

- Recover the software.

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

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

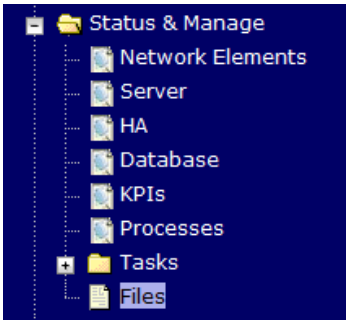
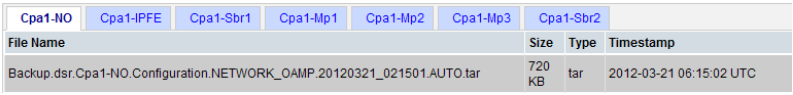
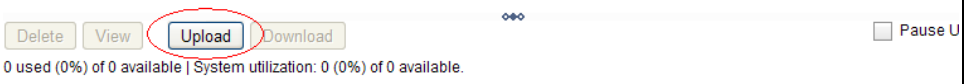
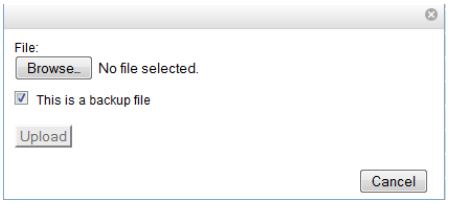
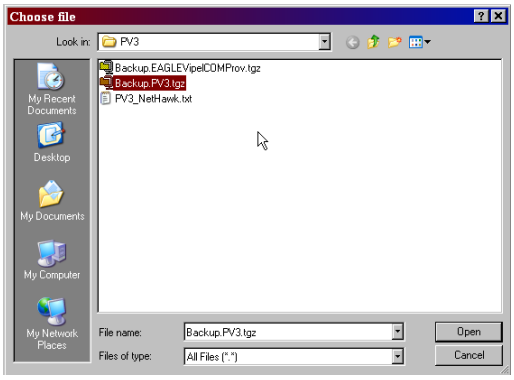
Procedure 3: Recovery Scenario 3

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 E. My Oracle Support (MOS), and ask for assistance.	
1. ☐	**Workarounds**	Refer to **Appendix D**. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
1. ☐	**Gather Required Materials**	Gather the documents and required materials listed in **Section 3.1** Required Materials
2. ☐	**Recover the Failed Software**	For VMWare based deployments: 1. For NOAM execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA b. Procedure 2 (VMWare Only). Configure NOAM guests role based on resource profile 2. For SOAM execute the following procedures from reference [1]: c. Procedure 1 (VMWare). Import DSR OVA d. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile 3. For failed MPs execute the following procedures from reference [1]: e. Procedure 1 (VMWare). Import DSR OVA f. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile For KVM/Openstack based deployments: 1. For NOAM execute the following procedures from reference [1]: a. Procedure 4 (KVM/Openstack). "Import DSR OVA" b. Procedure 5 (KVM/Openstack). "Configure NOAM guests role based on resource profile" 2. For SOAM execute the following procedures from reference [1]: c. Procedure 4 (KVM/Openstack). "Import DSR OVA" d. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests role based on resource profile" 3. For failed MPs execute the following procedures from reference [1]: e. Procedure 4 (KVM/Openstack). "Import DSR OVA" f. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests role based on resource profile"

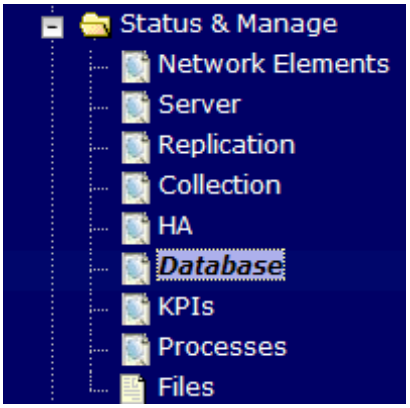
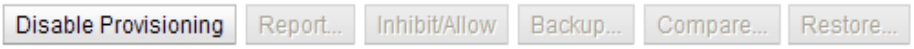
Procedure 3: Recovery Scenario 3

3. ☐	**Obtain Latest Database Backup and Network Configuration Data.**	Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. From required materials list in **Section 3.1** `Required Materials`; use site survey documents and Network Element report (if available), to determine network configuration data.
4. ☐	**Execute DSR Installation Procedure for the First NOAM**	Verify the networking data for Network Elements **Note:** Use the backup copy of network configuration data and site surveys (Step 2) **Execute** installation procedures for the first NOAM server from reference [1]: Procedure 7 “Configure the First NOAM NE and Server” and Procedure 8 “Configure the NOAM Server Group”.
5. ☐	**NOAM GUI:** Login	Login to the NOAM GUI as the ***guiadmin*** user: 

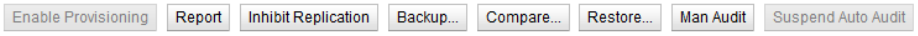
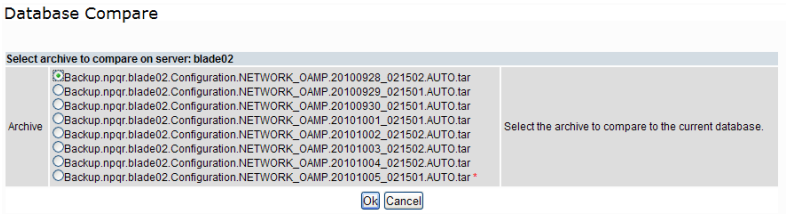
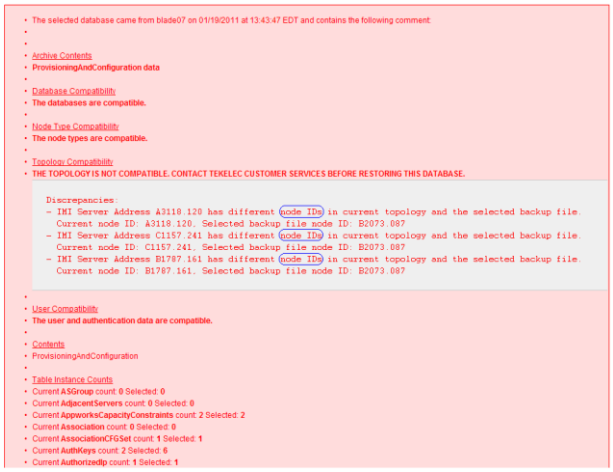
Procedure 3: Recovery Scenario 3

6. ☐	**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:  Click on **Upload** as shown below and select the file *"NO Provisioning and Configuration:"* file backed up after initial installation and provisioning.  1. Click on **Browse** and locate the backup file 2. Check **This is a backup file** Box 3. Click on Open as shown below.   Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.

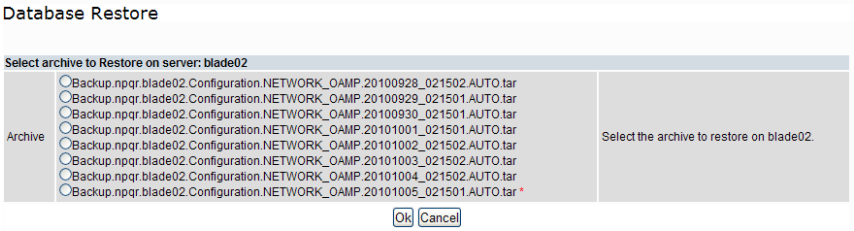
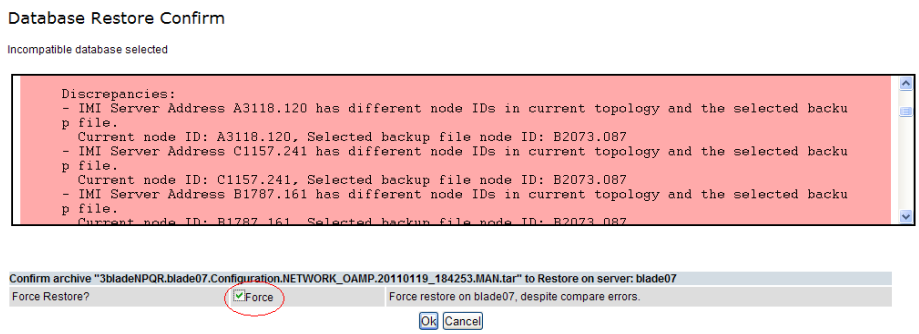
Procedure 3: Recovery Scenario 3

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

Procedure 3: Recovery Scenario 3

8. ☐	**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 6** of this procedure.  **Verify** that the output window matches the screen below. **Note:** You will get a database mismatch regarding the NodeIDs of the VMs. That is expected. If that is the only mismatch, proceed, otherwise stop and contact **Appendix E. My Oracle** Support (MOS)  **Note:** Archive Contents and Database Compatibilities must be the following: **Archive Contents:** Configuration data **Database Compatibility:** The databases are compatible. **Note:** The following is expected Output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one NOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. **Note:** We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility. If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.

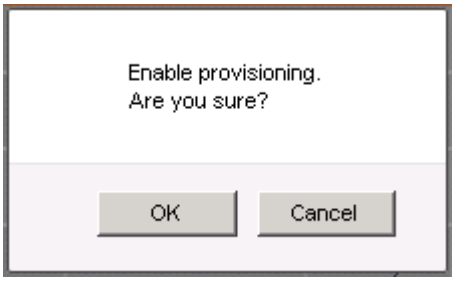
Procedure 3: Recovery Scenario 3

9. ☐	**ACTIVE NOAM:** Restore the Database	Click on **Main Menu->Status & Manage->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.  Click **OK** Button. The following confirmation screen will be displayed. **Note:** You will get a database mismatch regarding the NodeIDs of the servers. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix E. My Oracle Support (MOS). Select the **Force** checkbox as shown above and Click **OK** to proceed with the DB restore.  **Note:** After the restore has started, the user will be logged out of XMI NO GUI since the restored Topology is old data.

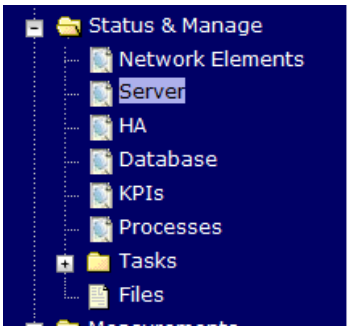
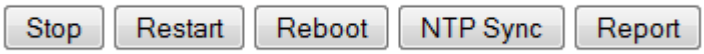
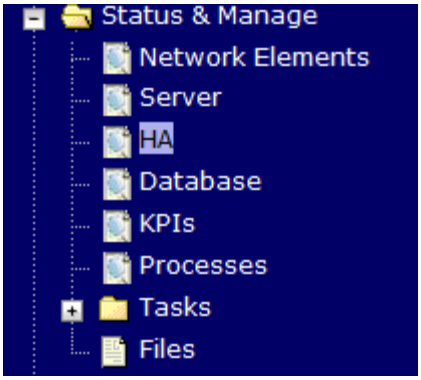
Procedure 3: Recovery Scenario 3

10. ☐	**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: 
11. ☐	**NOAM VIP GUI:** Monitor and Confirm database restoral	Wait for **5-10 minutes** for the System to stabilize with the new topology: Monitor the Info tab for **"Success"**. This will indicate that the backup is complete and the system is stabilized. Following alarms **must** be ignored for NOAM and MP Servers until all the Servers are configured: Alarms with Type Column as **"REPL"** , **"COLL", "HA"** (with mate NOAM), **"DB"** (about Provisioning Manually Disabled) **Note:** Do not pay attention to alarms until all the servers in the system are completely restored. **Note:** The Configuration and Maintenance information will be in the same state it was backed up during initial backup.
12. ☐	**ACTIVE NOAM:** Login	Login to the recovered Active NOAM via SSH terminal as ***admusr*** user.

Procedure 3: Recovery Scenario 3

13. ☐	**ACTIVE NOAM:** Restore /etc/hosts/ File of the Active NOAM	**IF DSR 7.1 or later, SKIP THIS STEP** Execute the following command: `$ sudo AppWorks AppWorks_AppWorks updateServerAliases <NOAM Host Name>`
14. ☐	**NOAM VIP GUI:** Re-enable Provisioning	Navigate to **Main Menu->Status & Manage->Database**  Click on the **Enable Provisioning**. A pop-up window will appear to confirm as shown below, press **OK**. 
15. ☐	**NOAM VIP GUI:** Recover Standby NOAM	Install the second NOAM server by executing procedures from reference [1]: Procedure 9 “Configure the Second NOAM Server” steps 1, 3-7 Procedure 10 “Complete Configuring the NOAM Server Group” Step 5 **Note**: If Topology or nodeId alarms are persistent after the database restore, refer to Appendix D. Workarounds for Issues not fixed in this Releaseor the next step below.
16. ☐	**NOAM VIP GUI:** Recover remaining failed SOAM Servers	Recover the **remaining** SOAM servers (**standby, spare**) by repeating the **following steps** for each SOAM server: 1. Install the remaining SOAM servers by executing Procedure 12 “Configure the SOAM Servers”, steps 1, 3- 7 from reference [1]. **NOTE:** Wait for server to reboot before continuing.

Procedure 3: Recovery Scenario 3

17. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered server and click on **Restart**. 
18. ☐	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**  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**
19.	**Recovered Server:** Login	Establish an SSH to the recovered server's XMI address:

Procedure 3: Recovery Scenario 3

<table>
<tr>
<td>20.</td>
<td>Recovered Server: Sync NTP</td>
<td>1) Perform the following to retrieve the remote NTP server:

$ sudo ntpq –np

Example output:

[admusr@NOAM-2 ~]$ ntpq -np
remote refid st t when poll reach delay offset jitter
==
*10.240.9.186 10.250.33.2 3 u 356 1024 377 1.409 0.113 2.434

2) Stop ntpd service:

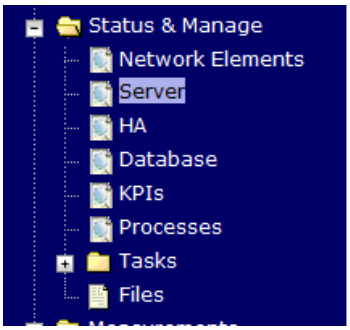
$ sudo service ntpd stop

3) Sync the date to the ntp remote server:

$ sudo ntpdate <NTP remote server>

Note: The remote server below will be that of the one gathered in sub step 1.

4) Start the ntp service:

$ sudo service ntpd start</td>
</tr>
<tr>
<td>21.</td>
<td>NOAM VIP GUI: Restart DSR application</td>
<td>Navigate to Main Menu->Status & Manage->Server,
 

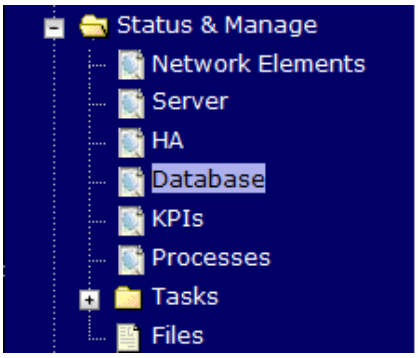
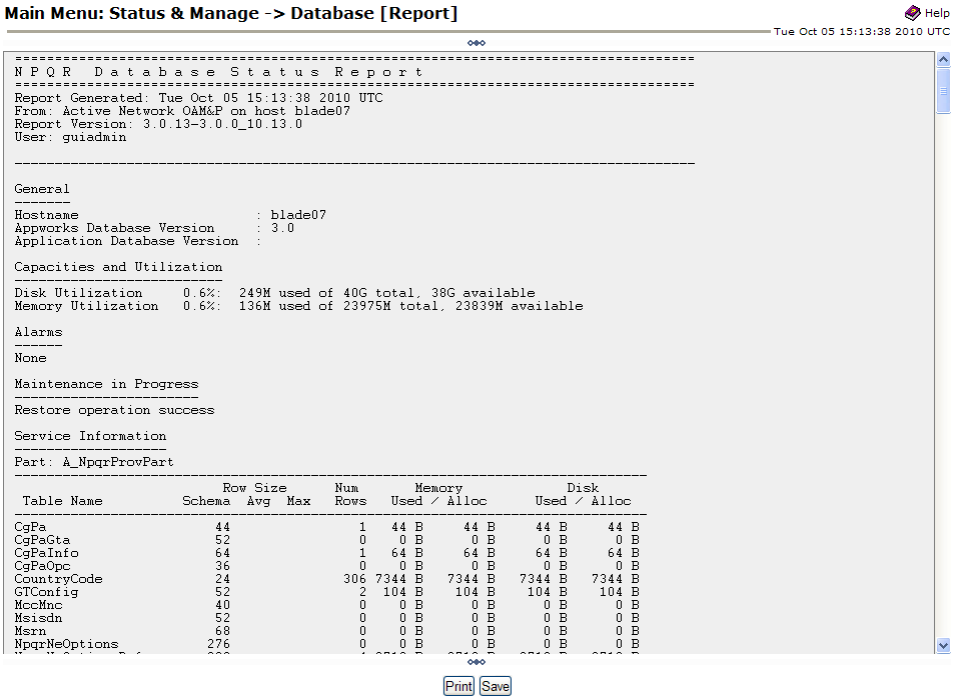
Select each recovered server and click on Restart.

Stop Restart Reboot NTP Sync Report</td>
</tr>
</table>

Procedure 3: Recovery Scenario 3

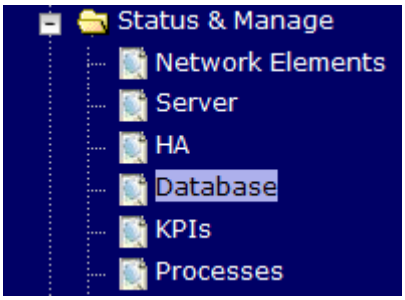
22. ☐	**Active SOAM:** Prepare recovered SOAM for optional feature activation	If DSR 7.1, skip this step. Establish an SSH session to the Active SOAM, login as ***admusr.*** Execute the following command: `$ irem DsrApplication where "name in ('RBAR','FABR','PCA','MD-IWF','DM-IWF','CPA','GLA')"`
23. ☐	**Active SOAM:** Verify Preparation	If DSR 7.1, skip this step Execute the following command to verify preparation of optional feature activation: `$ iqt -z -h -p -fname DsrApplication where "name in ('RBAR','FABR','PCA','MD-IWF','DM-IWF','CPA','GLA')"` **Note:** There should be no output of this command, if there is, verify the correct entry of the command in **step 24**.
24. ☐	**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.
25. ☐	**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 3: Recovery Scenario 3

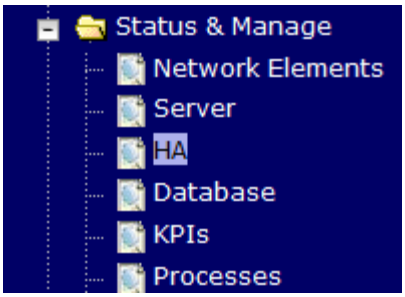
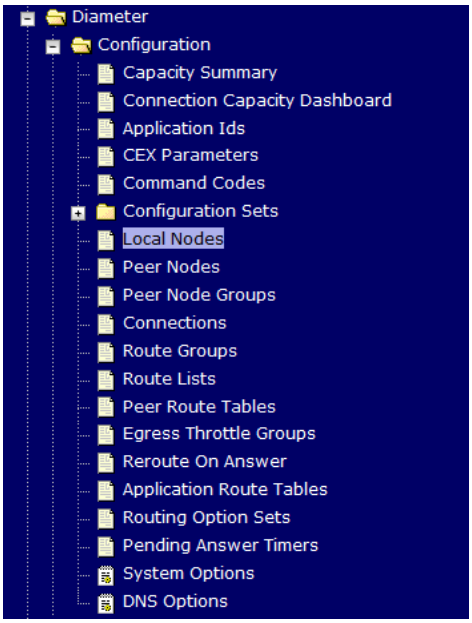
26. ☐	**NOAM VIP GUI:** Fetch and Store the database Report for the Newly Restored Data and Save it	Navigate to **Main Menu->Status & Manage->Database**  Select the **active** NOAM server and click on the **Report** button at the bottom of the page. The following screen is displayed:  Click on **Save** and save the report to your local machine.

Procedure 3: Recovery Scenario 3

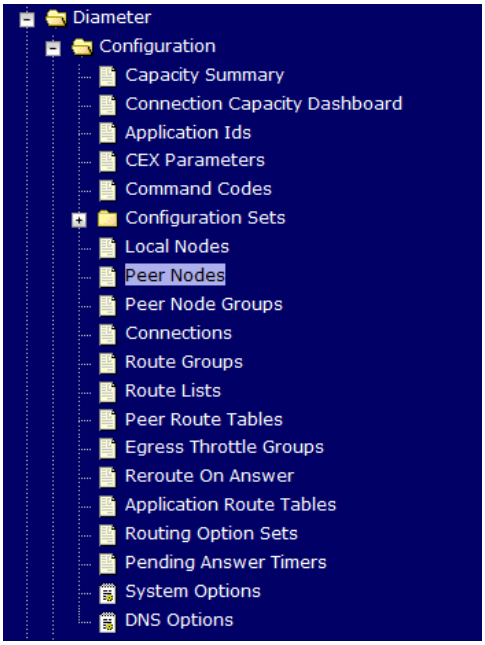
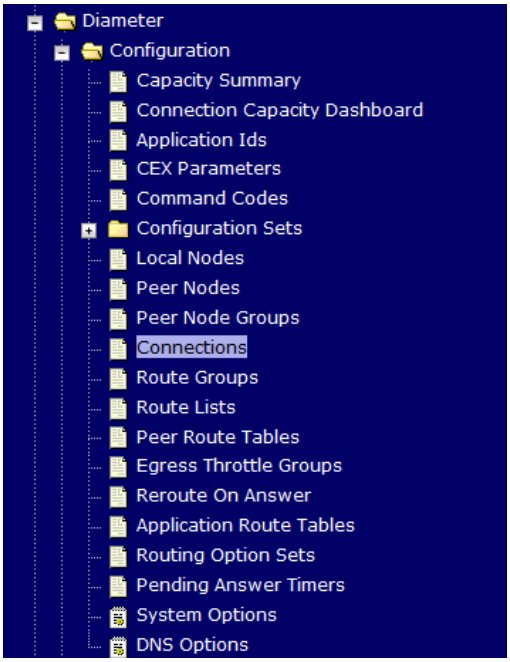
27. ☐	**ACTIVE NOAM:** Verify Replication Between Servers.	Login to the Active NOAM via SSH terminal as ***admusr*** user.
		Execute the following command:
		$ sudo irepstat –m
		Output like below shall be generated:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`RDU06-MP1 -- Stby`
		`BC From RDU06-SO1 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`
		Ctrl+c to exit the screen.

28. ☐	**NOAM VIP GUI:** Verify the Database states	Click on **Main Menu->Status and Manager->Database**  Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below: Network Element | Server | Role | OAM Max HA Role | Application Max HA Role | Status | DB Level | OAM Repl Status | SIG Repl Status | Repl Status | Repl Audit Status NO_10303 | NO2 | Network OAM&P | Active | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg SO_10303 | PSBR | MP | Active | Active | Normal | 0 | Normal | Normal | Allowed | AutoInProg SO_10303 | MP2 | MP | Active | Active | Normal | 0 | Normal | Normal | Allowed | AutoInProg SO_10303 | SO1 | System OAM | Standby | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg NO_10303 | NO1 | Network OAM&P | Standby | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg SO_10303 | IPFE | MP | Active | OOS | Normal | 0 | Normal | Normal | Allowed | AutoInProg SO_10303 | SO2 | System OAM | Active | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg

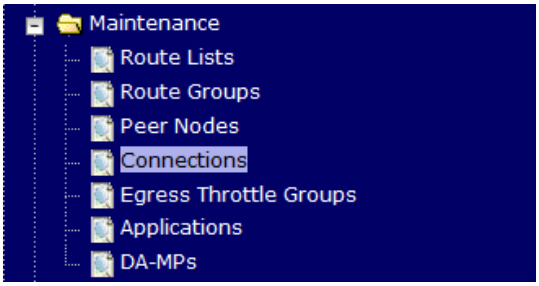
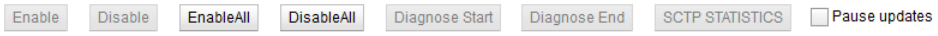
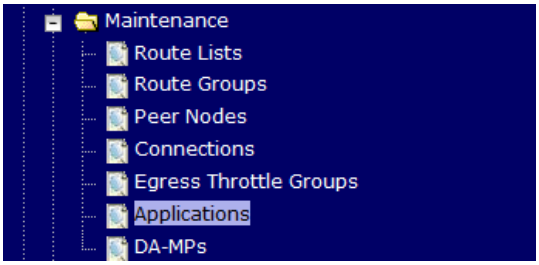
Procedure 3: Recovery Scenario 3

29. ☐	**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 "OAM 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 |
30. ☐	**SOAM VIP GUI:** Verify the Local Node Info	Navigate to **Main Menu->Diameter->Configuration->Local Node**  Verify that all the local nodes are shown.

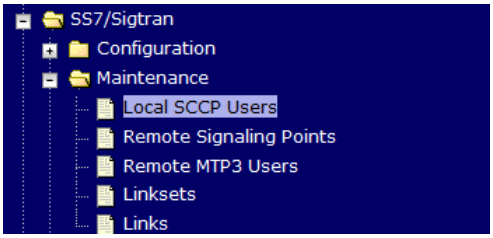
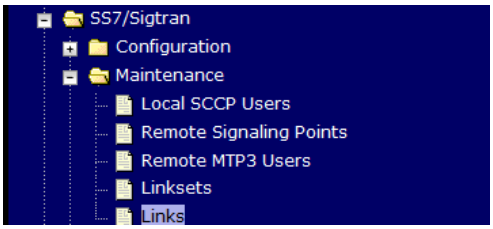
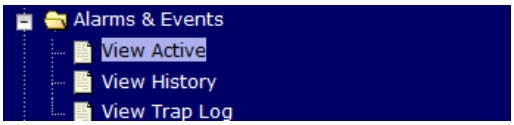
Procedure 3: Recovery Scenario 3

31. ☐	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.
32. ☐	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections**  Verify that all the connections are shown.

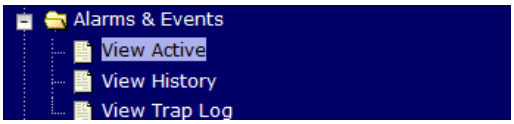
Procedure 3: Recovery Scenario 3

33. ☐	**SOAM VIP GUI:** Enable Connections if needed	Navigate to **Main Menu->Diameter->Maintenance->Connections**  Select each connection and click on the **Enable** button. Alternatively you can enable all the connections by selecting the **EnableAll** button.  Verify that the Operational State is Available.
34. ☐	**SOAM VIP GUI:** Enable Optional Features	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Select the optional feature application configured in **step 31**. Click the **Enable** button. 
35.	**SOAM VIP GUI:** Re-enable Transports if Needed	Navigate to **Main Menu->Transport Manager -> Maintenance -> Transport**  Select each transport and click on the Enable button  Verify that the Operational Status for each transport is Up.

Procedure 3: Recovery Scenario 3

36.	**SOAM VIP GUI:** Re-enable MAPIWF application if needed	Navigate to **Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users**  Click on the **Enable** button corresponding to MAPIWF Application Name.  Verify that the SSN Status is Enabled.
37.	**SOAM VIP GUI:** Re-enable links if needed	Navigate to **Main Menu->SS7/Sigtran->Maintenance->Links**  Click on **Enable** button for each link.  Verify that the Operational Status for each link is Up.
38. ☐	**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 E. My Oracle** Support (MOS).

Procedure 3: Recovery Scenario 3

39. ☐	**NOAM VIP GUI:** Examine All Alarms	Login to the NOAM VIP if not already logged in. Navigate to **Main Menu->Alarms & Events->View Active**  Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix E. My Oracle** Support (MOS).
40. ☐	**Restore GUI Usernames and Passwords**	If applicable, Execute steps in **Section 6.0** to recover the user and group information restored.
41. ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**. DSR Database Backup to back up the Configuration databases:

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

For a partial outage with an NOAM server and an SOAM server intact and available, only base recovery of 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 software.

- 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 software.
- Recover the software.

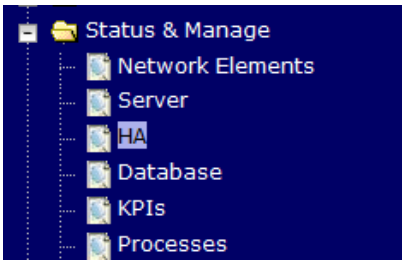
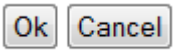
The database in intact at the active NOAM server and does not require restoration at the SO and MP servers.

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

Procedure 4: Recovery Scenario 4

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 E. My Oracle Support (MOS), and ask for assistance.	
1. ☐	**Workarounds**	Refer to **Appendix D**. Workarounds for Issues not fixed in this Releaseto 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: 

Procedure 4: Recovery Scenario 4

4. ☐	**Active NOAM:** Set Failed Servers to Standby	Navigate to **Main Menu -> Status & Manage -> HA**  Select **Edit** Set the Max Allowed HA Role drop down box to **Standby** for the failed servers. Select **Ok** 

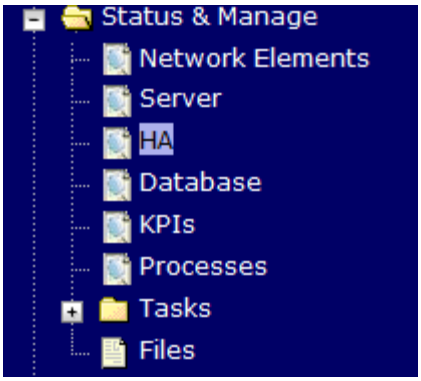
Procedure 4: Recovery Scenario 4

5. ☐	**Recover the Failed Software**	For VMWare based deployments: 1. For NOAM execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA b. Procedure 2 (VMWare Only). Configure NOAM guests role based on resource profile 2. For SOAM execute the following procedures from reference [1]: c. Procedure 1 (VMWare). Import DSR OVA d. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile 3. For failed MPs execute the following procedures from reference [1]: e. Procedure 1 (VMWare). Import DSR OVA f. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile For KVM/Openstack based deployments: 1. For NOAM execute the following procedures from reference [1]: a. Procedure 4 (KVM/Openstack). "Import DSR OVA" b. Procedure 5 (KVM/Openstack). "Configure NOAM guests role based on resource profile" 2. For SOAM execute the following procedures from reference [1]: c. Procedure 4 (KVM/Openstack). "Import DSR OVA" d. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests role based on resource profile" 3. For failed MPs execute the following procedures from reference [1]: e. Procedure 4 (KVM/Openstack). "Import DSR OVA" f. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests role based on resource profile"
6. ☐	**Repeat for Remaining Failed Servers**	If necessary, repeat **5** for all remaining failed servers.

Procedure 4: Recovery Scenario 4

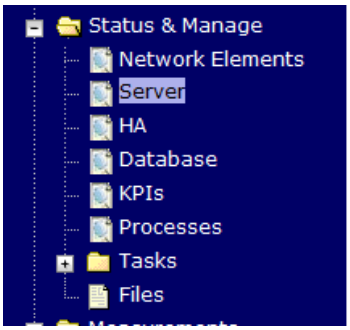
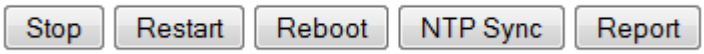
7. ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 
8. ☐	**NOAM VIP GUI:** Recover Standby NOAM if needed	Install the second NOAM server by executing procedures from reference [1]: Procedure 9 “Configure the Second NOAM Server” steps 1, 3-7 Procedure 10 “Complete Configuring the NOAM Server Group” Step 5 **Note:** If Topology or nodeId alarms are persistent after the database restore, refer to Appendix D. Workarounds for Issues not fixed in this Release, or the next step below.
9. ☐	**(OPTIONAL) NOAM VIP GUI:** Recover the Failed SOAM Servers if needed	If the failed server is an SOAM, recover the **remaining** SOAM servers (**standby, spare**) by repeating the **following steps** for each SOAM server: 1. Install the remaining SOAM servers by executing Procedure 12 “Configure the SOAM Servers”, steps 1, 3- 7 from reference [1]. **NOTE:** Wait for server to reboot before continuing.

Procedure 4: Recovery Scenario 4

10. ☐	**(OPTIONAL) NOAM VIP GUI:** Set HA on Recovered Servers	Navigate to **Status & Manage -> HA**  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**
11.	**Recovered Server:** Login	Establish an SSH to the recovered server's XMI address:

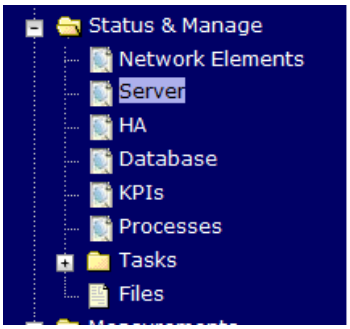
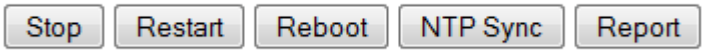
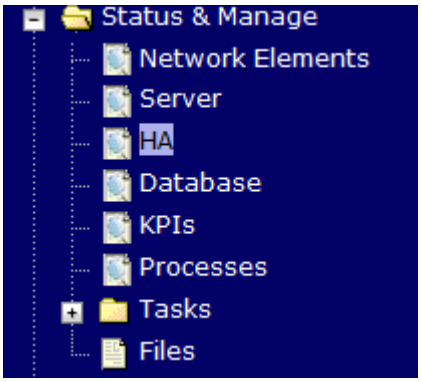
12.	**Recovered Server:** Sync NTP	1) Perform the following to retrieve the remote NTP server:
		`$ sudo ntpq –np`
		Example output:
		`[admusr@NOAM-2 ~]$ ntpq -np`
		`remote refid st t when poll reach delay offset jitter`
		`*10.240.9.186 10.250.33.2 3 u 356 1024 377 1.409 0.113 2.434`
		2) Stop ntpd service:
		`$ sudo service ntpd stop`
		3) Sync the date to the ntp remote server:
		`$ sudo ntpdate <NTP remote server>`
		Note: The remote server below will be that of the one gathered in sub step 1.
		4) Start the ntp service:
		`$ sudo service ntpd start`

Procedure 4: Recovery Scenario 4

13.	**(OPTIONAL) NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered server and click on **Restart**. 

14. ☐	**NOAM VIP GUI:** Recover the C-Level Server (DA-MP, SBRs, IPFE, SS7-MP)	Establish a SSH session to the C Level server being recovered, login as ***admusr.***
		
		Execute following command to set shared memory to unlimited:
		`$ sudo shl.set -m 0`
		
		Execute following command ONLY when the recovered C-Level server is of type IPFE:
		`$ sudo ipfeNetUpdate.sh`
		
		Execute the following procedures from [1] **FOR EACH** server that has been recovered:
		
		Procedure 15 “Configure the MP Virtual Machines”, Steps 1, 4-11.

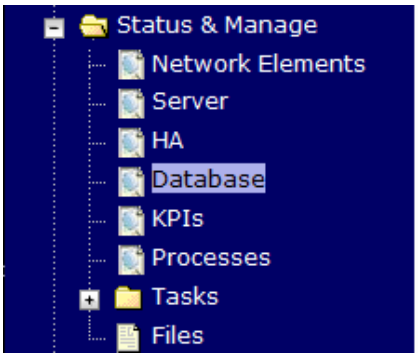
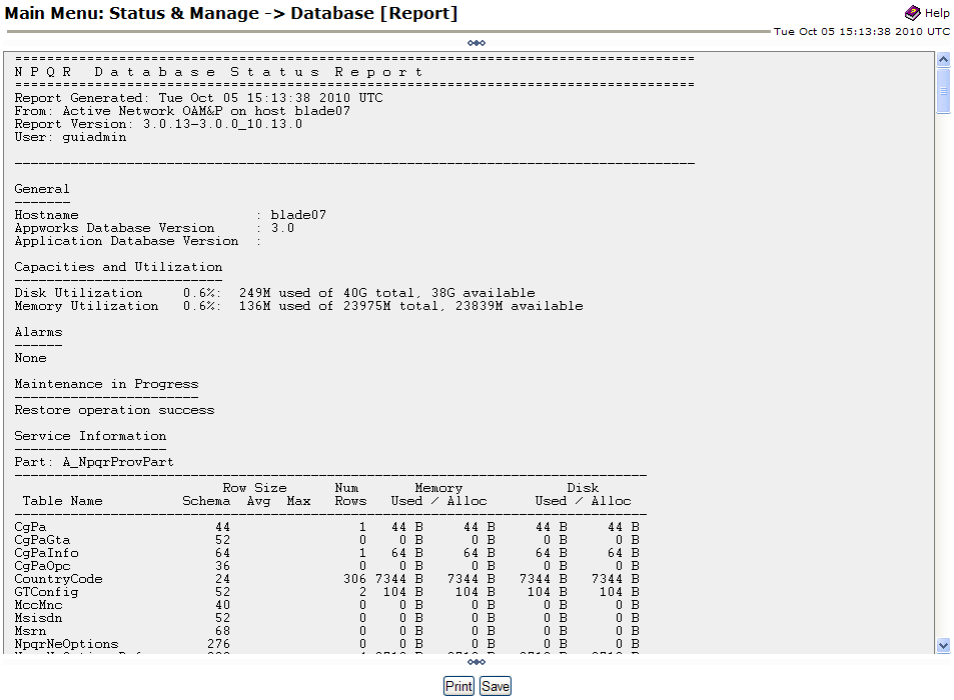
Procedure 4: Recovery Scenario 4

15. ☐	**NOAM VIP GUI:** Restart DSR Application on recovered C-Level Servers.	Navigate to **Main Menu->Status & Manage->Server**  Select the recovered servers and click on **Restart**. 
16. ☐	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**  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**
17. ☐	**ACTIVE NOAM:** Login	Login to the recovered Active NOAM via SSH terminal as ***admusr*** user.
18. ☐	**Active SOAM:** Prepare recovered SOAM for optional feature activation	If DSR 7.1, skip this step Establish an SSH session to the Active SOAM, login as ***admusr.*** Execute the following command: `$ irem DsrApplication where "name in ('RBAR','FABR','PCA','MD-IWF','DM-IWF','CPA','GLA')"`

Procedure 4: Recovery Scenario 4

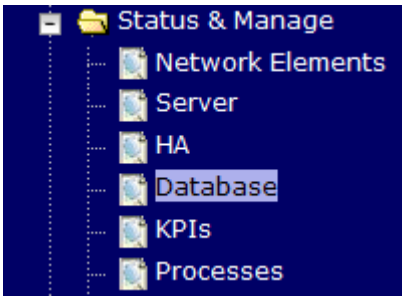
19. ☐	**Active SOAM:** Verify Preparation	If DSR 7.1, skip this step. Execute the following command to verify preparation of optional feature activation: `$ iqt -z -h -p -fname DsrApplication where "name in ('RBAR','FABR','PCA','MD-IWF','DM-IWF','CPA','GLA')"` **Note:** There should be no output of this command, if there is, verify the correct entry of the command in **step 18**.
20. ☐	**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>`
21. ☐	**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 4: Recovery Scenario 4

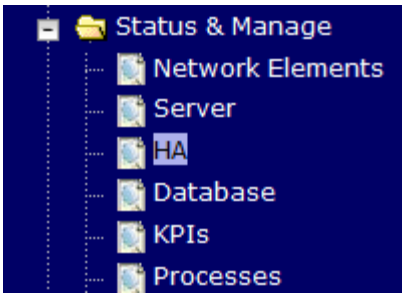
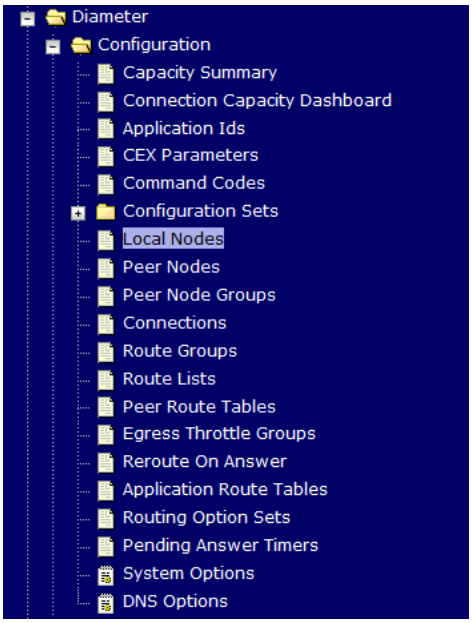
22. ☐	**NOAM VIP GUI:** Fetch and Store the database Report for the Newly Restored Data and Save it	Navigate to **Main Menu->Status & Manage->Database**  Select the **active** NOAM server and click on the **Report** button at the bottom of the page. The following screen is displayed:  Click on **Save** and save the report to your local machine.

Procedure 4: Recovery Scenario 4

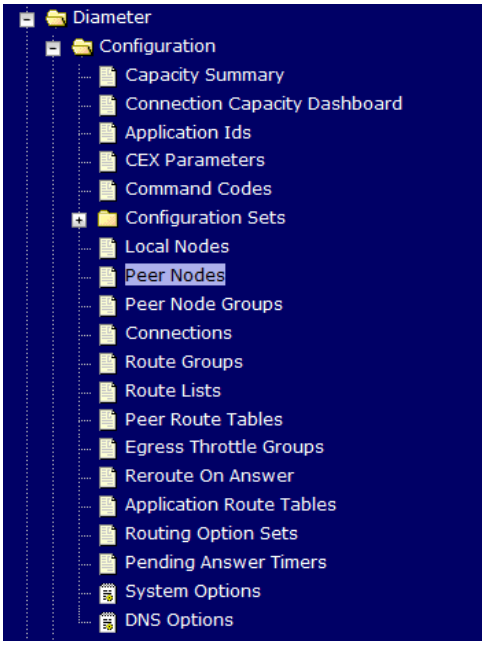
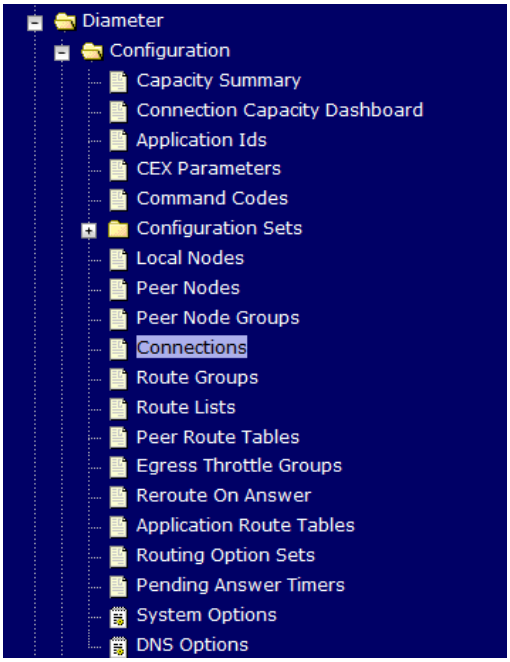
23. ☐	**ACTIVE NOAM:** Verify Replication Between Servers.	Login to the Active NOAM via SSH terminal as ***admusr*** user.
		Execute the following command:
		$ sudo irepstat –m
		Output like below shall be generated:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`RDU06-MP1 -- Stby`
		`BC From RDU06-SO1 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`
		Ctrl+c to exit the screen.

24. ☐	**NOAM VIP GUI:** Verify the Database states	Click on **Main Menu->Status and Manager->Database**  Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below: Network Element | Server | Role | OAM Max HA Role | Application Max HA Role | Status | DB Level | OAM Repl Status | SIG Repl Status | Repl Status | Repl Audit Status NO_10303 | NO2 | Network OAM&P | Active | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg SO_10303 | PSBR | MP | Active | Active | Normal | 0 | Normal | Normal | Allowed | AutoInProg SO_10303 | MP2 | MP | Active | Active | Normal | 0 | Normal | Normal | Allowed | AutoInProg SO_10303 | SO1 | System OAM | Standby | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg NO_10303 | NO1 | Network OAM&P | Standby | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg SO_10303 | IPFE | MP | Active | OOS | Normal | 0 | Normal | Normal | Allowed | AutoInProg SO_10303 | SO2 | System OAM | Active | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg

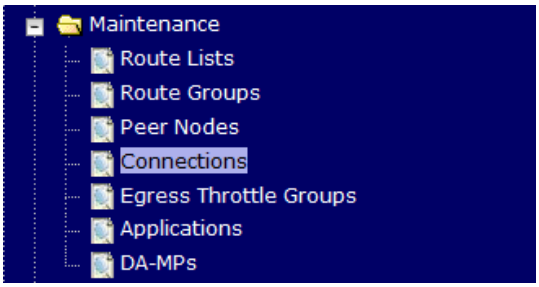
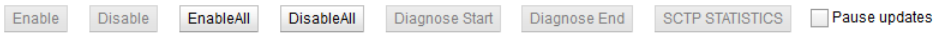
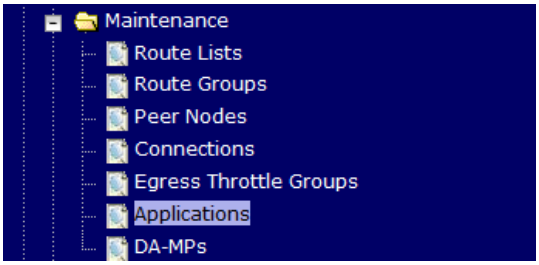
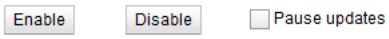
Procedure 4: Recovery Scenario 4

25. ☐	**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 "OAM 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 |
26. ☐	**SOAM VIP GUI:** Verify the Local Node Info	Navigate to **Main Menu->Diameter->Configuration->Local Node**  Verify that all the local nodes are shown.

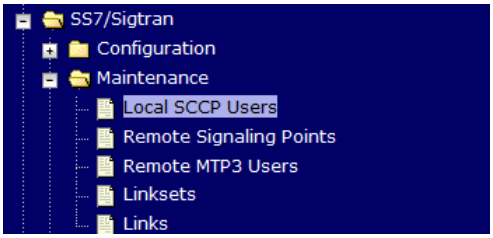
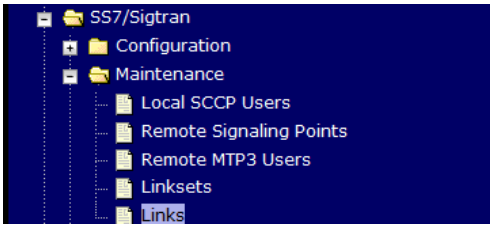
Procedure 4: Recovery Scenario 4

27. ☐	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.
28. ☐	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections**  Verify that all the connections are shown.

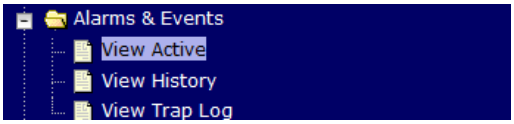
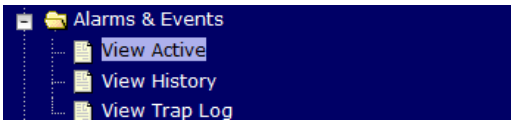
Procedure 4: Recovery Scenario 4

29.	**MP Servers:** Disable SCTP Auth Flag (DSR 7.1 Only)	For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [1]. Execute this procedure on all Failed MP Servers.
30. ☐	**SOAM VIP GUI:** Enable Connections if needed	Navigate to **Main Menu->Diameter->Maintenance->Connections**  Select each connection and click on the **Enable** button. Alternatively you can enable all the connections by selecting the **EnableAll** button.  Verify that the Operational State is Available.
31. ☐	**SOAM VIP GUI:** Enable Optional Features	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Select the optional feature application configured in **step 21**. Click the **Enable** button. 

Procedure 4: Recovery Scenario 4

32. ☐	**SOAM VIP GUI:** Re-enable Transports if Needed	Navigate to **Main Menu->Transport Manager -> Maintenance -> Transport**  Select each transport and click on the **Enable** button  Verify that the Operational Status for each transport is Up.
33. ☐	**SOAM VIP GUI:** Re-enable MAPIWF application if needed	Navigate to **Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users**  Click on the **Enable** button corresponding to MAPIWF Application Name.  Verify that the SSN Status is Enabled.
34. ☐	**SOAM VIP GUI:** Re-enable links if needed	Navigate to **Main Menu->SS7/Sigtran->Maintenance->Links**  Click on **Enable** button for each link.  Verify that the Operational Status for each link is Up.

Procedure 4: Recovery Scenario 4

35. ☐	**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 E. My Oracle** Support (MOS).
36. ☐	**NOAM VIP GUI:** Examine All Alarms	Login to the NOAM VIP if not already logged in. Navigate to **Main Menu->Alarms & Events->View Active**  Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix E. My Oracle** Support (MOS).

37. ☐	**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`

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

5.1.5 Recovery Scenario 5 (Database Recovery)

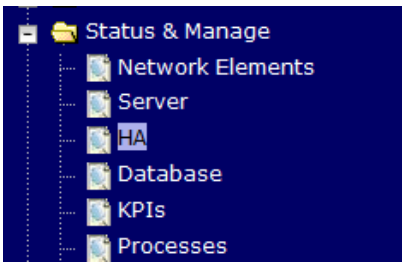
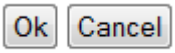
5.1.5.1 Recovery Scenario 5: Case 1

For a partial outage with

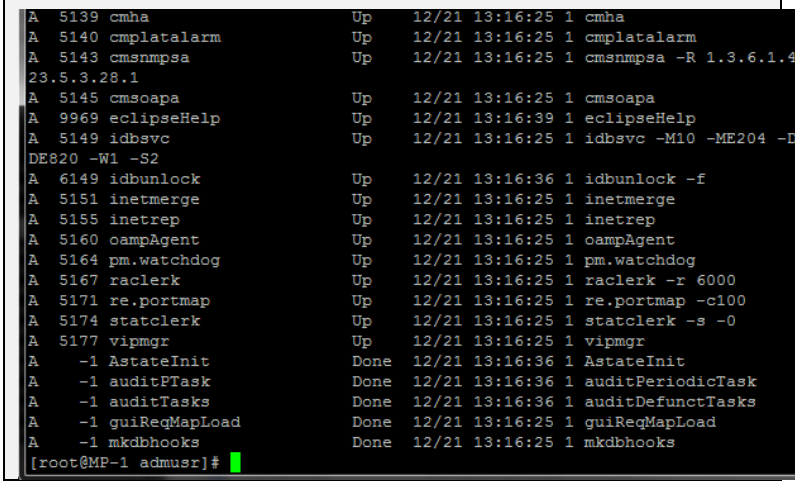
- Server having a corrupted database
- Replication channel from parent is inhibited because of upgrade activity or
- Server is in a different release then that of its Active parent because of upgrade activity.
- Verify that the Server Runtime backup files, performed at the start of the upgrade, are present 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 5: Recovery Scenario 5 (Case 1)

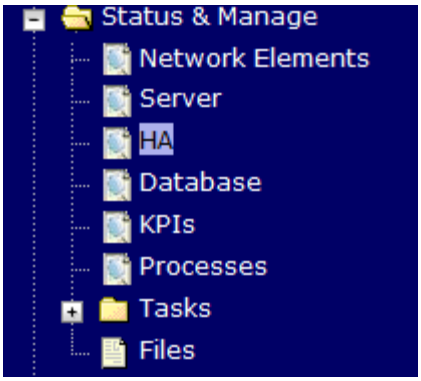
S T E P #		
	This procedure performs recovery if database is corrupted in the system Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix E. My Oracle Support (MOS), and ask for assistance.	
1. ☐	**Workarounds**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

Procedure 5: Recovery Scenario 5 (Case 1)

3. ☐	**Server in Question:** Login	Establish an SSH session to the server in question. Login as ***admusr*** user.
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`
7. ☐	**Server in Question:** Verify the server	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
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 -D
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]#
```

Procedure 5: Recovery Scenario 5 (Case 1)

8.	**NOAM VIP GUI:** Set Failed Servers to Active	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**
9. ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**. DSR Database Backup to back up the Configuration databases:

5.1.5.2 Recovery Scenario 5: Case 2

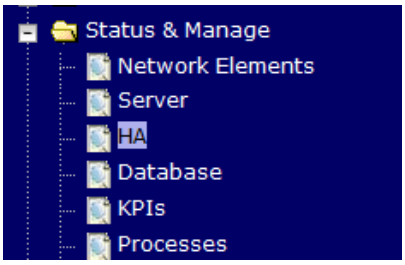
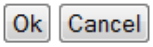
For a partial outage with

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

Procedure 6: Recovery Scenario 5 (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 E. My Oracle Support (MOS), and ask for assistance.	
1. ☐	**Workarounds**	Refer to **Appendix D**. Workarounds for Issues not fixed in this Releaseto understand any workarounds required during this procedure.

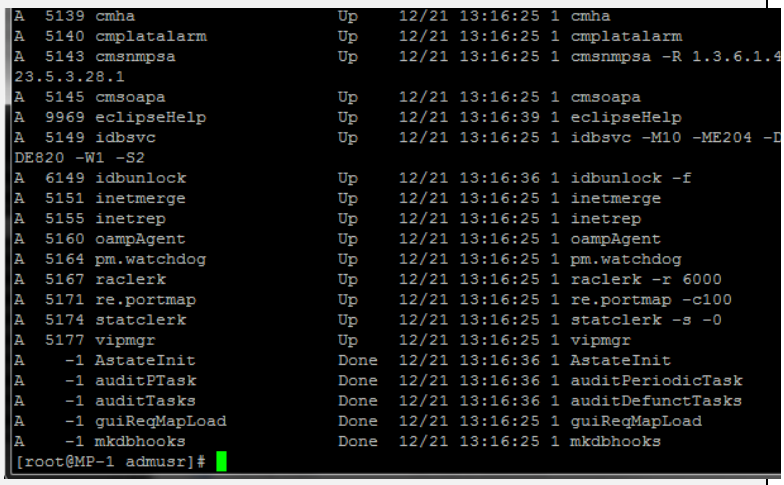
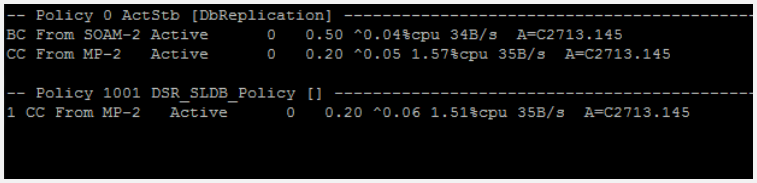
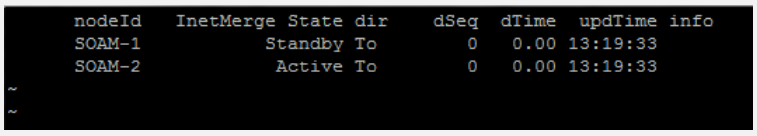
Procedure 6: Recovery Scenario 5 (Case 2)

2.	**NOAM VIP GUI:** Set Failed Servers to Standby	Navigate to **Main Menu -> Status & Manage -> HA**  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*** user.

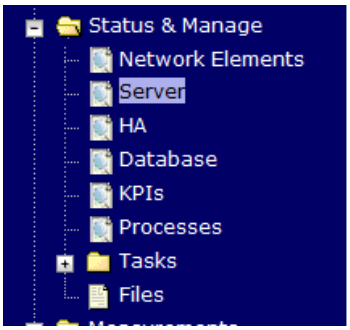
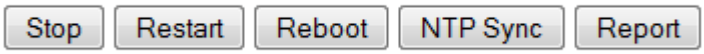
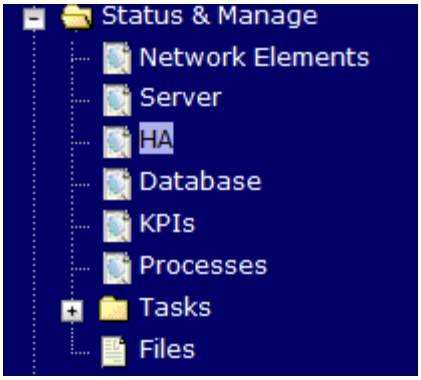
4. ☐	**Server in Question:** Take Server out of Service	Execute the following command to take the server out of service.
		`$ sudo bash -l`
		`# prod.clobber`

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`

Procedure 6: Recovery Scenario 5 (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:  Execute the following command to verify if replication channels are up and running: **$ sudo irepstat** Example Output:  Execute the following command to verify if merging channels are up and running: **$ sudo inetmstat** Example Output: 

Procedure 6: Recovery Scenario 5 (Case 2)

7.	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select each recovered server and click on **Restart**. 
8.	**NOAM VIP GUI:** Set Failed Servers to Active	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**
9. ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**. DSR Database Backup to back up the Configuration databases:

6.0 Resolving User Credential Issues after Database Restore

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

6.1 Restoring a Deleted User

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

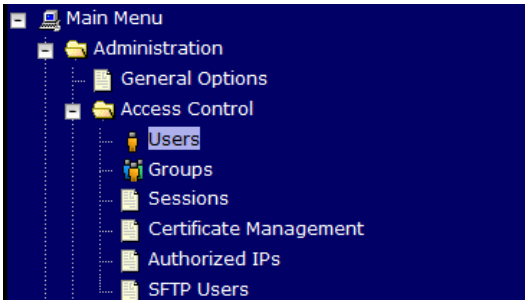
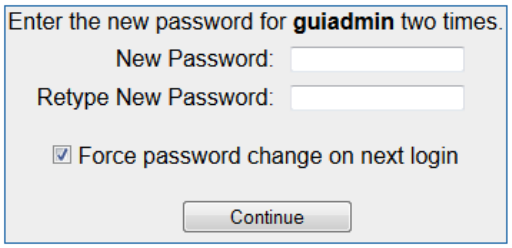
These users were removed prior to creation of the backup and archive file. They will be reintroduced by system restoration of that file.

6.2 Keeping a Restored user

Procedure 7: 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 E. 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: 

Procedure 7: Keep Restored User

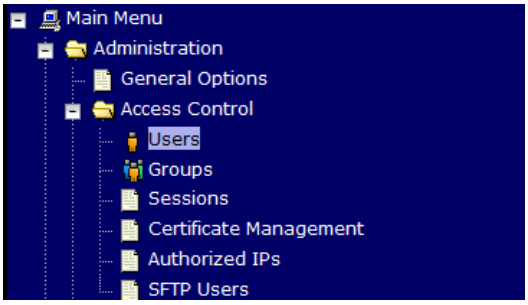
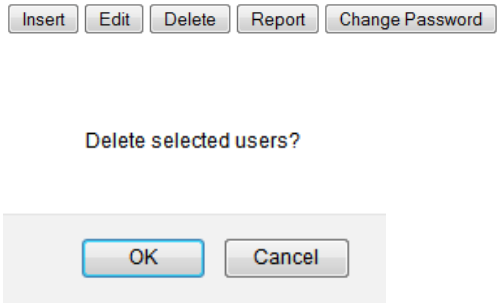
3. ☐	**After Restoration:** Reset User Passwords	Navigate to **Administration -> Access Control -> Users**  Select the user Click the **Change Password** button  Enter a new password  Click the **Continue** button

6.3 Removing a Restored User

Procedure 8: 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 E. 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: 

Procedure 8: Remove the Restored User

2. ☐	**After Restoration:** Reset User Passwords	Navigate to **Administration -> Access Control -> Users**  Select the user Click the **Delete** button  Click the **OK** button to confirm.

6.4 Restoring a Modified User

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

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

Before Restoration:

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

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

After Restoration:

Log in and reset the passwords for all users in this category. See the steps in Appendix E. My Oracle Support (MOS) 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.

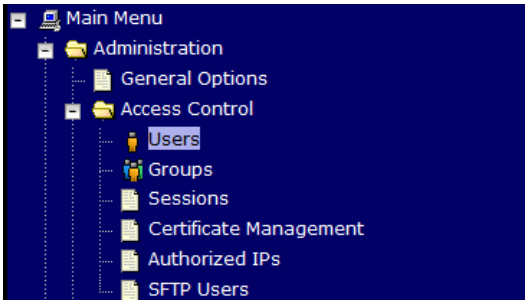
```
- User 'testuser' exists in current database but not in the selected backup
file.
```

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

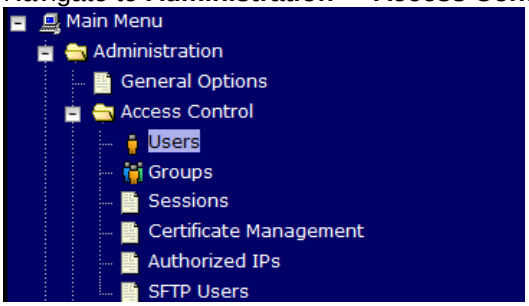
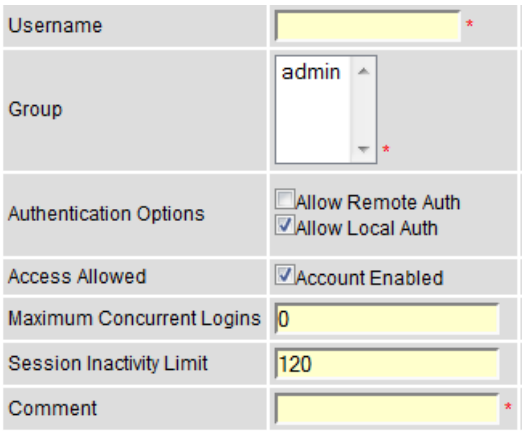
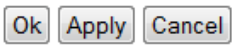
Procedure 9: Restoring an Archive that does not Contain a Current User

S T E P #		
	Perform this procedure to remove users that will be restored by system restoration Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix E. 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: 

Procedure 9: Restoring an Archive that does not Contain a Current User

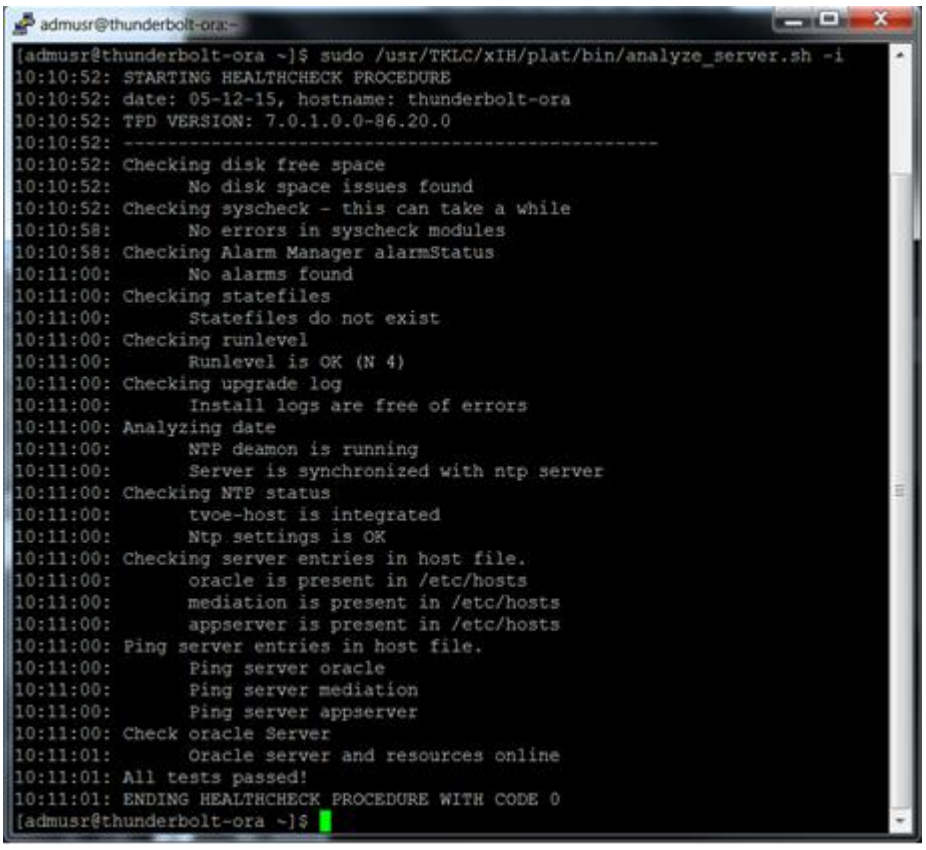
3. ☐	**Before Restoration:** Record user settings	Navigate to **Administration -> Access Control -> Users**  Under each affected user, record the following: • Username, • Account status • Remote Auth • Local Auth • Concurrent Logins Allowed • Inactivity Limit • Comment • Groups
4. ☐	**After Restoration:** 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: 

Procedure 9: Restoring an Archive that does not Contain a Current User

5. ☐	**After Restoration:** Recreate affected user	Navigate to **Administration -> Access Control -> Users**  Click **Insert**  Recreate the user using the data collected in **Step 3.**  Click **Ok** 
6. ☐	**After Restoration:** Repeat for Additional Users	Repeat **Step 5** to recreate additional users.
7. ☐	**After Restoration:** Reset the Passwords	See Appendix E. My Oracle Support (MOS) for resetting passwords for a user.

7.0 IDIH Disaster Recovery

Procedure 10: 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 E. My Oracle Support (MOS), and ask for assistance.	
1. ☐	**Oracle Guest:** Login	Establish an SSH session to the Oracle guest, login as ***admusr***.
2. ☐	**Oracle Guest:** Perform Database Health check	Execute the following command to perform a database health check: `$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i` Output:  **NOTE:** if this step fails a re-installation is necessary by following procedure 23,25 - 30 for VMWare and / or procedure 24 –30for KVM / Openstack from reference [1]

Procedure 11: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

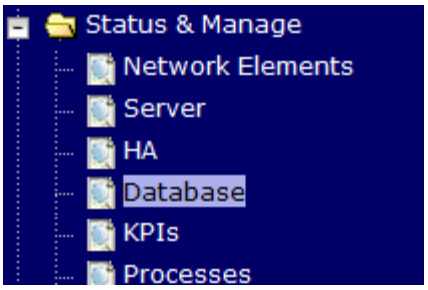
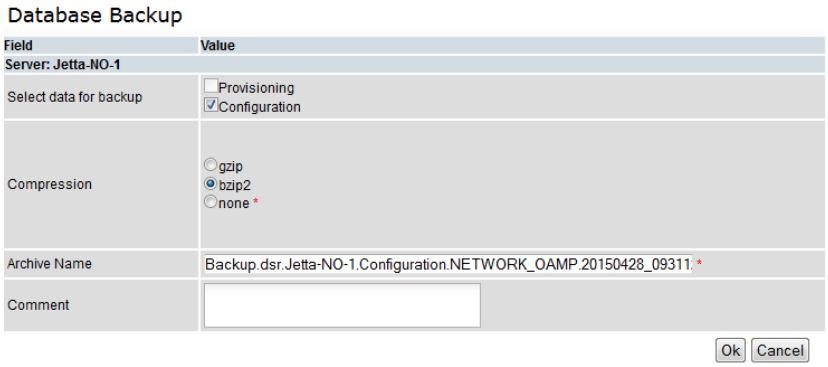
S T E P #	This procedure performs disaster recovery for the IDIH by re-installing the mediation and application servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix E. My Oracle Support (MOS), and ask for assistance.	
1. ☐	**Create iDIH Application & Mediation VMs**	Execute the following procedure from [1] to recover the Application and Mediation VMs: For VMWare based deployments: Procedure 23 "(VMware only) Create iDIH Oracle, Mediation and Application VMs" For KVM / Openstack based deployments: Procedure 24. (KVM/OpenStack only) Create iDIH Oracle, Mediation and Application VMs (Optional)
2. ☐	**Configure iDIH VM Networks**	Execute the following procedure from [1] to configure the VM networks on the Application and Mediation VMs only: Procedure 25 "Configure iDIH VM Networks"
3. ☐	**Configure VMs**	Execute the following procedure from [1]: Procedure 26"Run Post Installation scripts on iDIH VMs", steps 3 - 9
4. ☐	**Integrate into DSR (Optional)**	If integration is needed execute the following procedure from [1]: Procedure 29. Integrate iDIH into DSR
5. ☐	**iDIH Application Final configuration**	Execute the following procedure from [1]: Procedure 30. iDIH Application final configuration

Appendix A. DSR Database Backup

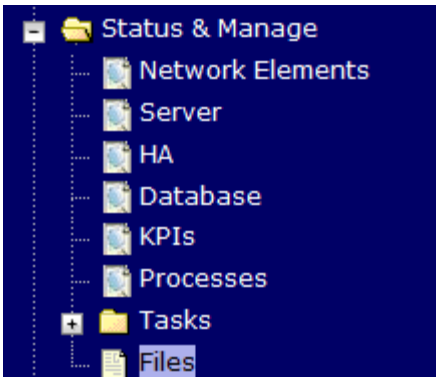
Procedure 12: Restoring an Archive that does not Contain a Current User

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 E. 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: 

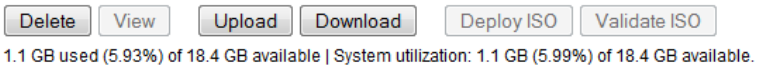
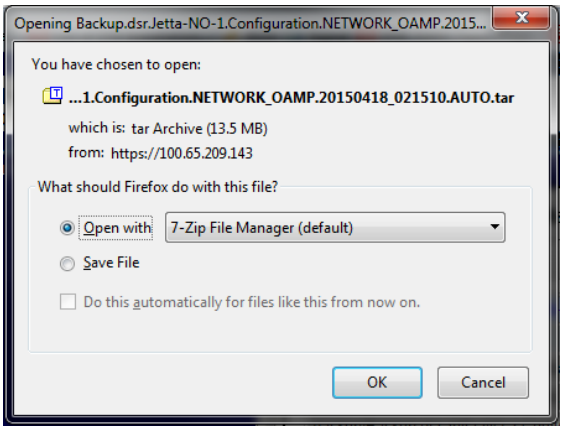
Procedure 12: Restoring an Archive that does not Contain a Current User

2. ☐	**NOAM/SOAM VIP:** Backup Configuration Data for the System	Navigate to **Main Menu -> Status & Manage -> Database**  Select the Active NOAM Server and Click on **Backup** button  Make sure that the checkboxes next to “Configuration” is checked.  Enter a filename for the backup and press **OK**

Procedure 12: Restoring an Archive that does not Contain a Current User

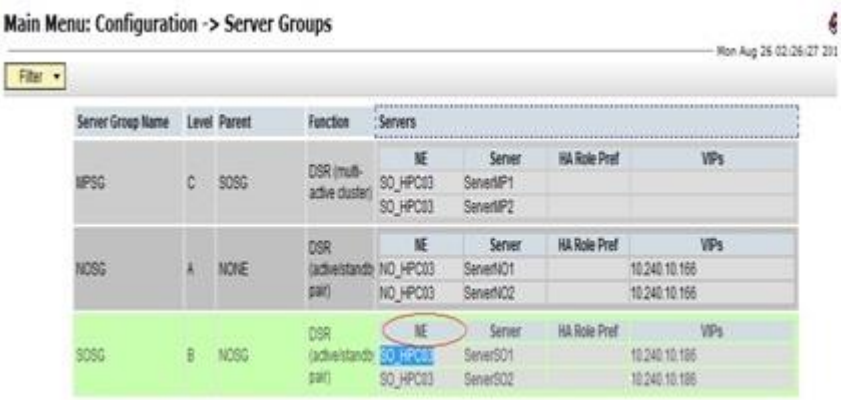
3. ☐	**NOAM/SOAM VIP:** Verify the backup file existence.	Navigate to **Main Menu -> Status & Manage -> Files**  **Main Menu: Status & Manage -> Files** Filter Tasks Jetta-NO-1 | Jetta-NO-2 | Jetta-SO-1 | Jetta-SO-2 | Jetta-DAMP-1 | Jetta-DAMP-2 File Name Backup.DSR.Jetta-NO-1.FullDBParts.NETWORK_OAMP.20150421_143846.UPG.tar.bz2 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 12: Restoring an Archive that does not Contain a Current User

4. ☐	**NOAM/SOAM VIP:** Download the file to a local machine.	From the previous step, choose the backup file. Select the **Download** button  Select **OK** to confirm the download. 
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

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

Procedure 13: Inhibit A and B Level Replication on C-Level Servers

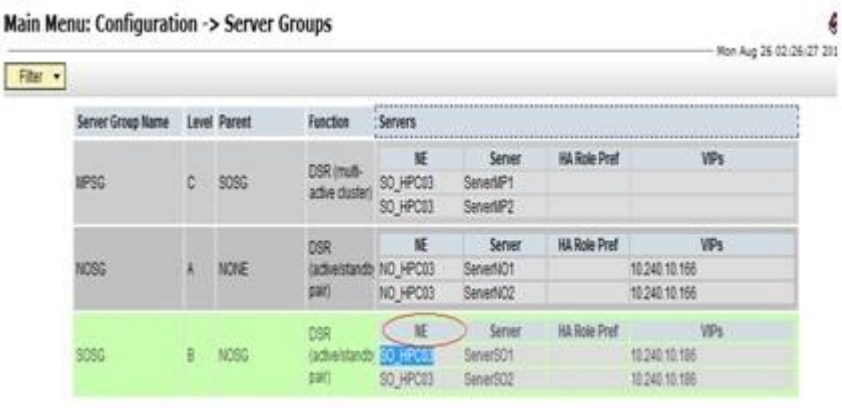
S T E P #		
	The intent of this procedure is to inhibit A and B level replication on all C Level servers of this site Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix E. My Oracle Support (MOS), and 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 $(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<NE name of the site>'"); do iset -finhibitRepPlans='A B' NodeInfo where "nodeName='$i'"; done` **Note:** 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. 

Procedure 13: 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: **$ 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 A B SO_HPC03 C2254.233 MP1 MP1 Active A B SO_HPC03

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

Procedure 14: Un-Inhibit A and B Level Replication on C-Level Servers

S T E P #		
	The intent of this procedure is to Un-inhibit A and B level replication on all C Level servers of this site Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix E. 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:** Un-Inhibit replication on all C level Servers	Execute the following command: `$ for i in $(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<NE name of the site>'"); do iset -finhibitRepPlans='' NodeInfo where "nodeName='$i'"; done` **Note:** 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. 

Procedure 14: 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 D. Workarounds for Issues not fixed in this Release

<table>
<tr><th>Issue</th><th>Associated PR</th><th>Workaround</th></tr>
<tr><td>Inetmerge alarm after force restore</td><td rowspan="2">Bug 19095635</td><td rowspan="2">Get the clusterID of the NO using the following command:
$ top.myrole
myNodeId=A3603.215
myMasterCapable=true

Then update the clusterId field in RecognizedAuthority table to have the same clusterid:
$ ivi RecognizedAuthority
e.g.
iload -ha -xU -frecNum -fclusterId -ftimestamp RecognizedAuthority \
<<'!!!!'
0|A1878|1436913769646
!!!!</td></tr>
<tr><td>Incorrect NodeID</td></tr>
<tr><td>Inetsync alarms after performing disaster recovery</td><td>Bug 19095639</td><td>Restart the Inetsync service on all affected servers using the following commands:
$ pm.set off inetsync
$ pm.set on inetsync</td></tr>
<tr><td>Active NO /etc/hosts file does not contain server aliases after force restore done.</td><td rowspan="2">222829,234357</td><td rowspan="2">Release 7.0.1:

From the recovered NOAM server command line, execute:
$ AppWorks AppWorks_AppWorks updateServerAliases <NO Host Name></td></tr>
<tr><td>Active NO cannot communicate with other Servers</td></tr>
</table>

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

Appendix E. 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.