Oracle® Communications

Diameter Signaling Router

Cloud Disaster Recovery Guide

Release 8.4

F12351-01

April 2019

ORACLE®

Oracle Communications Diameter Signaling Router, DSR Cloud Disaster Recovery Guide

CAUTION: Use only the DR procedures included in the Disaster Recovery Kit.

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

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

Table of Contents 3
List of Procedures 5
List of Tables 5
List of Figures 5
1.0 Introduction 6
1.1 Purpose and Scope 6
1.2 References 6
1.3 Acronyms 7
1.4 Terminology 8
1.5 Optional Features 8
2.0 General Description 9
2.1 Complete Server Outage (All Servers) - Recovery Scenario 5.1.1 10
2.2 Partial server outage with one NOAM server intact and both SOAMs failed- Recovery Scenario 5.1.2 10
2.3 Partial server outage with both NOAM servers failed and one SOAM server intact- Recovery Scenario 5.1.3 10
2.4 Partial server outage with NOAM and one SOAM server intact- Recovery Scenario 5.1.4 10
2.5 Partial server outage with both NOAM servers failed with DR-NOAM available- Recovery Scenario 5.1.5 11
2.6 Partial Service outage with corrupt database 11
3.0 Procedure Overview 12
3.1 Required Materials 12
3.2 Disaster Recovery Strategy 13
4.0 Procedure Preparation 15
5.0 Disaster Recovery Procedure 16
5.1 Recovering and Restoring System Configuration 17
5.1.1 Recovery Scenario 1 (Complete Server Outage) 17
5.1.2 Recovery Scenario 2 (Partial Server Outage with one NOAM server intact and both SOAMs failed) 49
5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact) 76
5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact) 96
5.1.5 Recovery Scenario 5 (Partial Server Outage with all NOAM servers failed with DR-NOAM available) 112
5.1.6 Recovery Scenario 6 (Database Recovery) 119

6.0 Resolving User Credential Issues after Database Restore 125
6.1 Restoring a Deleted User 125
6.2 Keeping a Restored user 126
6.3 Removing a Restored User 128
6.4 Restoring a Modified User 130
6.5 Restoring an Archive that does not contain a Current User 131
7.0 IDIH Disaster Recovery 135
Appendix A. DSR Database Backup 138
Appendix B. Inhibit A and B Level Replication on C-Level Servers 142
Appendix C. Un-Inhibit A and B Level Replication on C-Level Servers 144
Appendix D. Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost) 146
Appendix E. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost) 149
Appendix F. Workarounds for Issues not fixed in this Release 152
Appendix G. My Oracle Support (MOS) 154
Appendix H. Emergency Response 155
Appendix I. Locate Product Documentation on the Oracle Help Center 156

List of Procedures

Procedure 1. Table 1: Acronyms 7
Procedure 2. Table 2: Terminology 8
Procedure 3. Table 3: Optional Features 8
Procedure 4. Table 4: Recovery Scenarios 15
Procedure 5. Recovery Scenario 1 18
Procedure 6. Recovery Scenario 2 49
Procedure 7. Recovery Scenario 3 76
Procedure 8. Recovery Scenario 4 96
Procedure 9. Recovery Scenario 5 112
Procedure 10. Recovery Scenario 6 (Case 1) 120
Procedure 11. Recovery Scenario 6 (Case 2) 122
Procedure 12. Keep Restored User 126
Procedure 13. Remove the Restored User 128
Procedure 14. Restoring an Archive that does not Contain a Current User 131
Procedure 15. IDIH Disaster Recovery Preparation 135
Procedure 16. IDIH Disaster Recovery (Re-Install Mediation and Application Servers) 137
Procedure 17. Back up the provision and configuration data 138
Procedure 18. Inhibit A and B Level Replication on C-Level Servers 142
Procedure 19. Un-Inhibit A and B Level Replication on C-Level Servers 144
Procedure 20. Inhibit A and B Level Replication on C-Level Servers 146
Procedure 21. Un-Inhibit A and B Level Replication on C-Level Servers 149
Procedure 22. Backup directory 152

List of Tables

Procedure 1. Table 1: Acronyms 7
Procedure 2. Table 2: Terminology 8
Procedure 3. Table 3: Optional Features 8
Procedure 4. Table 4: Recovery Scenarios 15

List of Figures

Figure 1. Determining Recovery Scenario 14

1.0 Introduction

1.1 Purpose and Scope

This document is a guide to describe procedures used to execute disaster recovery for DSR (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. 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.

Note: Please note that failures can happen from the host or Infrastructure level too. Different infrastructures have different approaches to recover VMs which is not covered in this document. For example, VMWare has a vMotion feature which can migrate VM from one host to another. Any such Infrastructure/Hypervisor related migrations/disaster recovery scenarios are out of scope of this document. This document covers the DR scenarios within the DSR application.

1.2 References

[1] DSR Cloud Installation Guide
[2] DSR / SDS NOAM Failover User's Guide
[3] DSR PCA Activation Guide
[4] DSR MAP-Diameter IWF Feature Activation Procedure

1.3 Acronyms

Procedure 1. 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
NOAM	Network Operations, Administration & Maintenance
OS	Operating System
OVA	Open Virtualization Appliance
OVM-M	Oracle Virtual Machine Manager
OVM-S	Oracle Virtual Machine Server
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
SOAM	Systems Operations, Administration & Maintenance
TPD	Tekelec Platform Distribution
VM	Virtual Machine
vSTP	Virtual Signaling Transfer Point

1.4 Terminology

Procedure 2. Table 2: Terminology

Base software	Base software includes deploying the VM image.
Failed server	A failed server in disaster recovery context refers to a VM 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

Procedure 3. Table 3: Optional Features

Feature	Document
Diameter Mediation	DSR Meta Administration Feature Activation Procedure
Full Address Based Resolution (FABR)	DSR FABR Feature Activation Procedure
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation Procedure
Map-Diameter Interworking (MAP-IWF) –	DSR MAP-Diameter IWF Feature Activation Procedure
Policy and Charging Application (PCA)	DSR PCA Activation Procedure
Host Intrusion Detection System (HIDS)	DSR Security Guide, Section 3.2

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 [*5.1.1 Recovery Scenario 1 (Complete Server 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 [*5.1.2 Recovery Scenario 2 (Partial Server Outage with one NOAM server intact and both SOAMs failed)*]	• 1 or more NOAM servers intact • All SOAM servers or MP servers failed
Recovery of the NOAM pair with one or more SOAM servers intact [*5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server 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. [*5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)*]	• 1 or more NOAM servers intact • 1 or more SOAM servers intact • 1 or more MP servers failed
Recovery of the NOAM pair with DR-NOAM available and one or more SOAM servers intact [*5.1.5 Recovery Scenario 5 (Partial Server Outage with all NOAM servers failed with DR-NOAM available*)]	• All NOAM servers failed • 1 or more SOAM servers intact • DR-NOAM available
Recovery of one or more server with corrupt databases that cannot be restored via replication from the active parent node. *[5.1.6 Recovery Scenario 6 (Database Recovery)]*	• Server having a corrupted database

2.1 Complete Server Outage (All Servers) - Recovery Scenario 5.1.1

Scenario:

- All NOAM servers failed
- All SOAM servers failed
- 1 or more MP servers failed

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- Recovery Scenario 5.1.2

Scenario:

- 1 or more NOAM servers intact
- All SOAM servers failed
- 1 or more MP servers 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- Recovery Scenario 5.1.3

Scenario:

- All NOAM servers failed
- 1 or more SOAM servers 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- Recovery Scenario 5.1.4

Scenario:

- 1 or more NOAM servers intact

- 1 or more SOAM servers intact
- 1 or more MP servers failed

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 server outage with both NOAM servers failed with DR-NOAM available- Recovery Scenario 5.1.5

Scenario:

- All NOAM servers failed
- 1 or more SOAM servers intact
- DR-NOAM available

This case assumes that a partial outage with both NOAM servers failed but a DR NOAM available. The DR NOAM is switched from secondary to primary then recovers the failed NOAM servers

2.6 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 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.

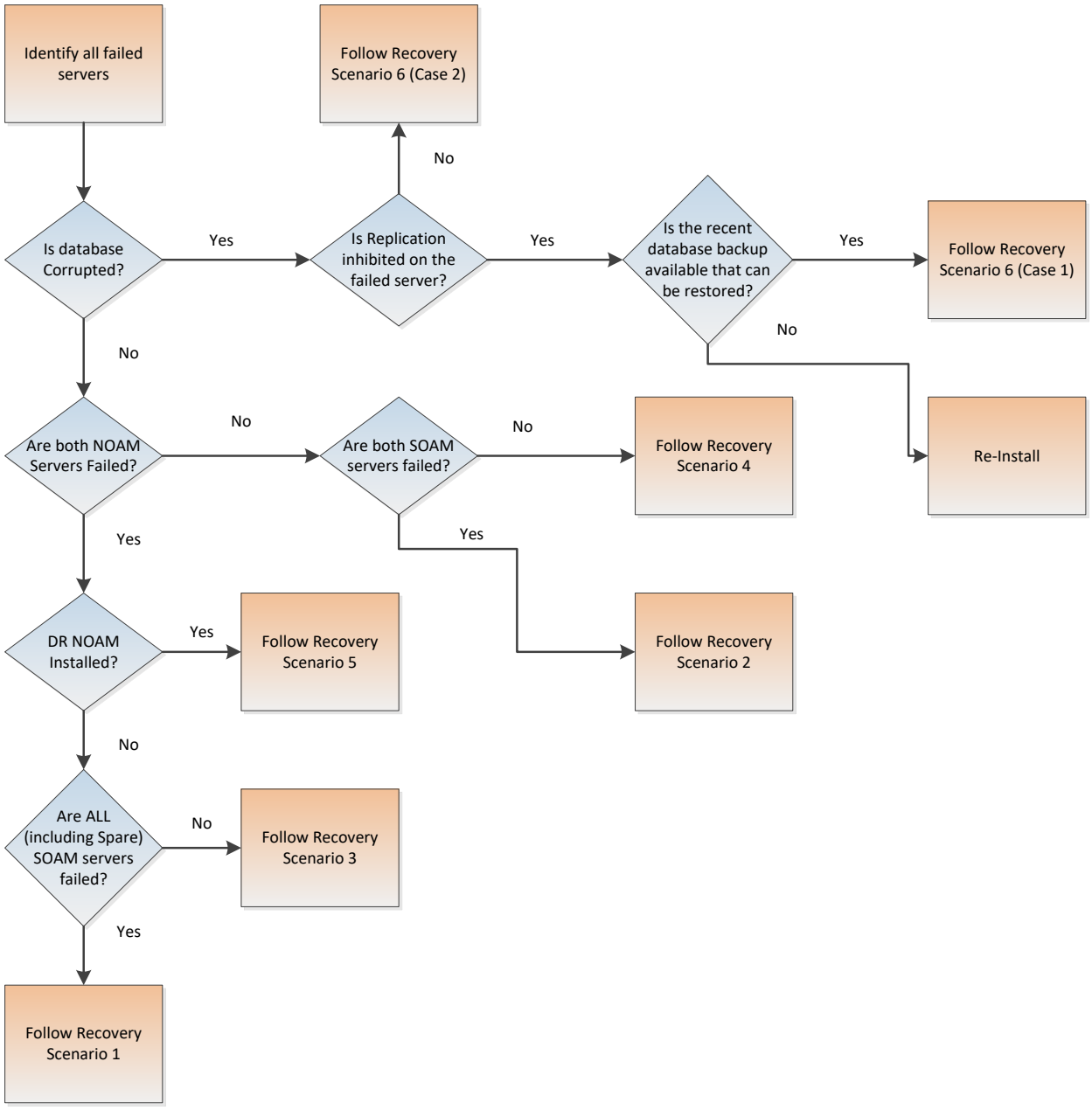
Note: For all Disaster Recovery scenarios, we assume that the NOAM Database backup and the SOAM database backup were performed around the same time, and that no synchronization issues exist among them.

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.

Procedure 4. 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, and 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, and Spare is intact and available. • 1 or more MP servers have failed.	Section 5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)
5	• Both NOAM servers failed in Primary site • At least 1 SOAM server out of Active, StandBy, and Spare is intact and available. • DR-NOAM is available	Section 5.1.5 Recovery Scenario 5 (Partial Server Outage with all NOAM servers failed with DR-NOAM available)
6: Case 1	• Server is intact • Database gets corrupted on the server • Replication is occurring to the server with corrupted database	Section 5.1.6.1 Recovery Scenario 6: Case 1

6: Case 2	• Server is intact • Database gets corrupted on the server • Latest Database backup of the corrupt server is NOT present • Replication is inhibited (either manually or because of comcol upgrade barrier)	Section 5.1.6.2 Recovery Scenario 6: Case 2

5.0 Disaster Recovery Procedure

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

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

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

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

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

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 8 distinct procedures to choose from depending on the type of recovery needed. Only one of these should be followed (not all).


!!WARNING!!

Whenever there is need to restore the database backup for NOAM and SOAM servers in any of below Recovery Scenarios, the backup directory may not be there in the system as system will be DRed.

In this case, please refer to Workarounds for Issues not fixed in this Release, this will provide steps to check and create the backup directory.

File format for recovery will be when back was taken. Generally back file is in format below.
For example:-
Backup.DSR.HPC02-NO2.FullDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2

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 Procedure 1. 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

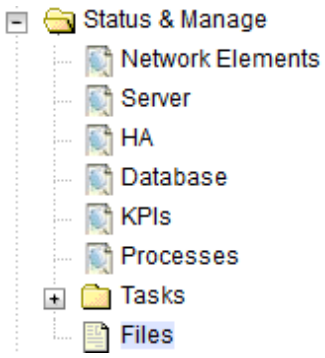
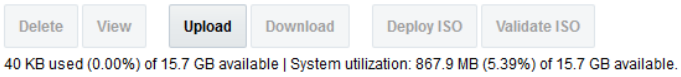
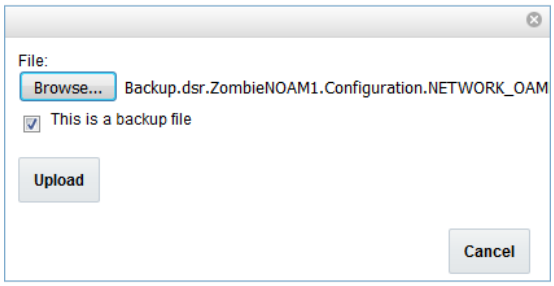
Note: Any other applications DR recovery actions (SDS and IDIH) may occur in parallel. These actions can/should be worked simultaneously; doing so would allow faster recovery of the complete solution (i.e. stale DB on DP servers will not receive updates until SDS-SOAM servers are recovered.

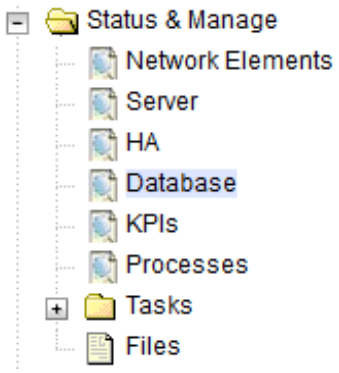
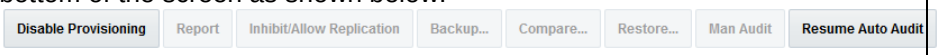
Procedure 5. Recovery Scenario 1

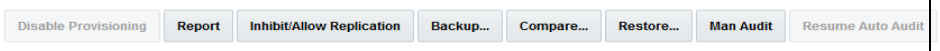
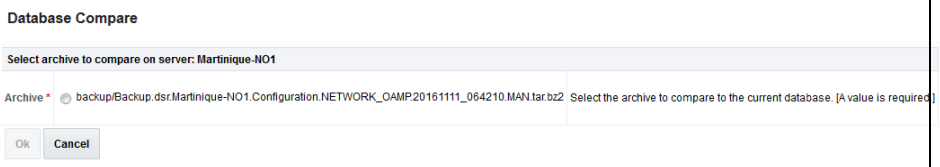
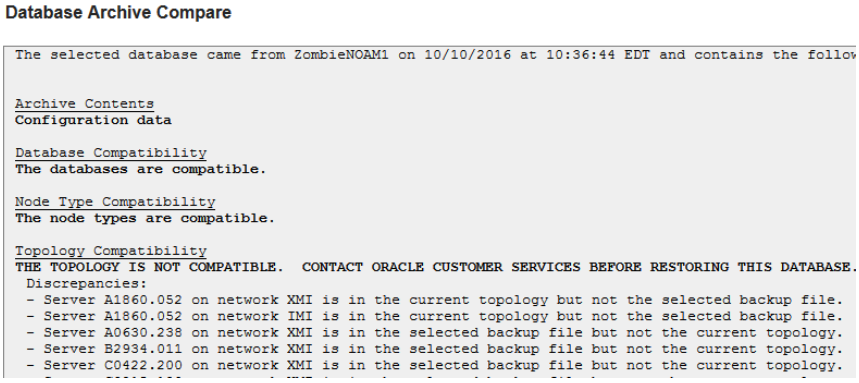
STEP #	Procedure	Description
This procedure performs recovery if both NOAM servers are failed and all SOAM servers are failed. This procedure also covers the C-Level Sever failure Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	**Workarounds**	Refer to **Workarounds for** Issues not fixed in this Release to understand/apply 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 NOAMs execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 2 (VMWare Only). Configure NOAM guests based on resource profile 2. For SOAMs execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile 3. For failed MPs execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile For KVM / Openstack based deployments: 1. For NOAMs execute the following procedures from reference [1]: a. Procedure 4 (KVM / Openstack). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 5 (KVM / Openstack Only). Configure NOAM guests based on resource profile

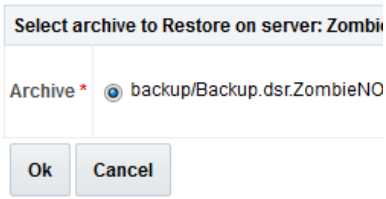
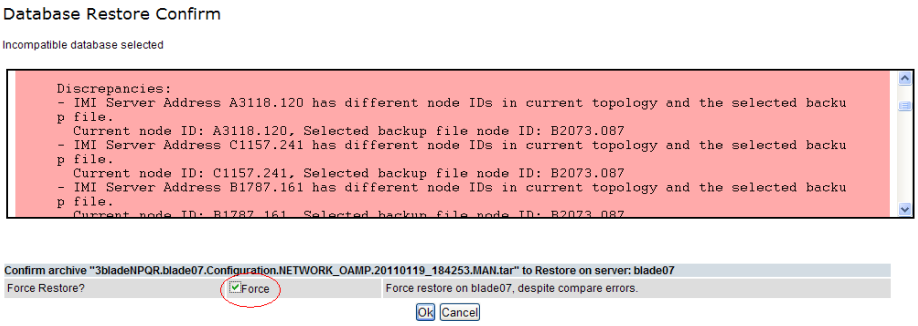
STEP #	Procedure	Description
		2. For SOAMs execute the following procedures from reference [1]: a. Procedure 4 (KVM / Openstack). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 6 (KVM / Openstack Only). Configure Remaining DSR guests based on resource profile 3. For failed MPs execute the following procedures from reference [1]: a. Procedure 4 (KVM / Openstack). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 6 (KVM / Openstack Only). Configure Remaining DSR guests based on resource profile For OVM-S / OVM-M based deployments: Execute the following procedures from reference [1]: a. Procedure 7 (OVM-S/OVM-M). Import DSR OVA and prepare for VM creation b. Procedure 8 (OVM-S/OVM-M). Configure each DSR VM ***Note***: While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs)
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 9 “Configure the First NOAM NE and Server” and Procedure 10 “Configure the NOAM Server Group”.

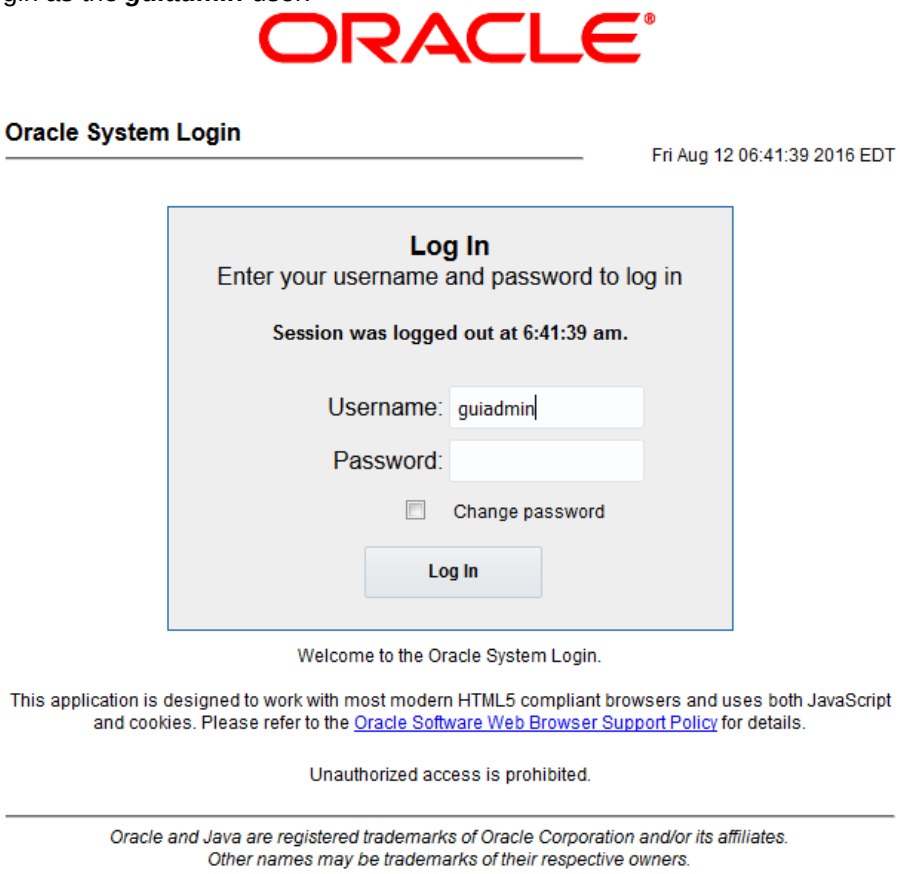
STEP #	Procedure	Description
6. ☐	**NOAM GUI:** Login	Login to the NOAM GUI as the ***guiadmin*** user: 

STEP #	Procedure	Description
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: **Main Menu: Status & Manage -> Files**  Click on **Upload** as shown below and select the file *"NO Provisioning and Configuration:"* file backed up after initial installation and provisioning.  1. 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.

STEP #	Procedure	Description
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.

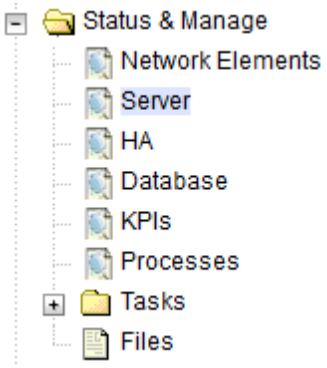
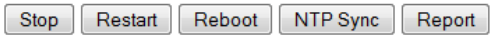
STEP #	Procedure	Description
9. ☐	**NOAM GUI:** Verify the Archive Contents and Database Compatibility	Select the **Active NOAM** server and click on the **Compare**.  The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 13** of this 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 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.

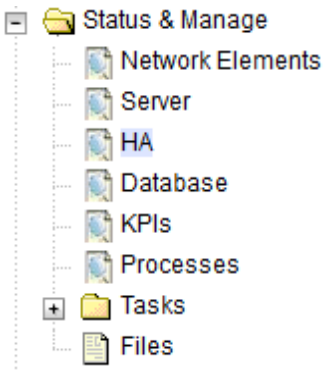
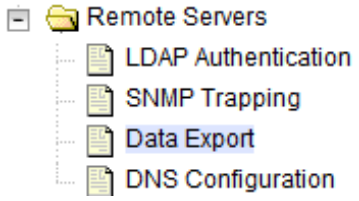
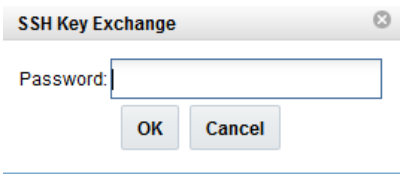
STEP #	Procedure	Description
10. ☐	**ACTIVE NOAM:** Restore the Database	Click on **Main Menu->Status & Manage->Database** Select the **Active NOAM** server, and click on **Restore** as shown below. The following screen will be displayed. Select the proper back up provisioning and configuration file.  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 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.

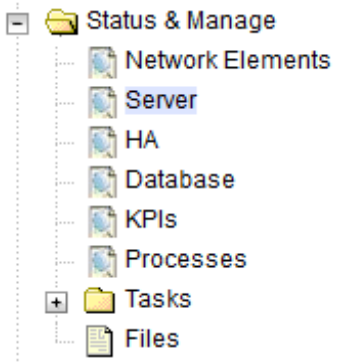
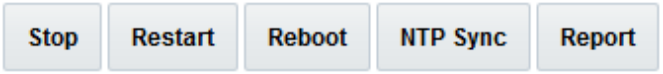
STEP #	Procedure	Description
11. ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 
12. ☐	**NOAM VIP GUI:** Monitor and 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.

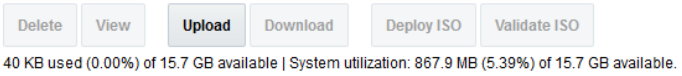
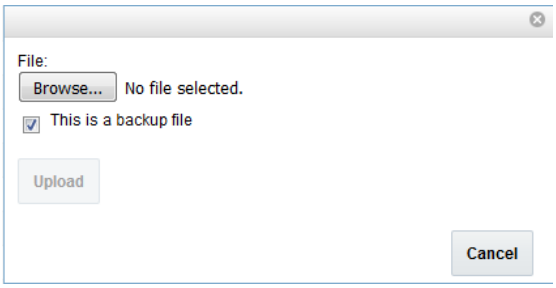
STEP #	Procedure	Description
13. ☐	**ACTIVE NOAM:** Login	Login to the recovered Active NOAM via SSH terminal as ***admusr*** user.
14. ☐	**NOAM VIP GUI:** Recover Standby NOAM	Install the second NOAM server by executing procedures from reference [1] Procedure 15 “Configure the Second NOAM Server” steps 1, 3-7 Procedure 16 “Complete Configuring the NOAM Server Group” Step 4

15. ☐	**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>`

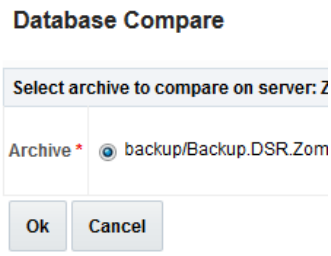
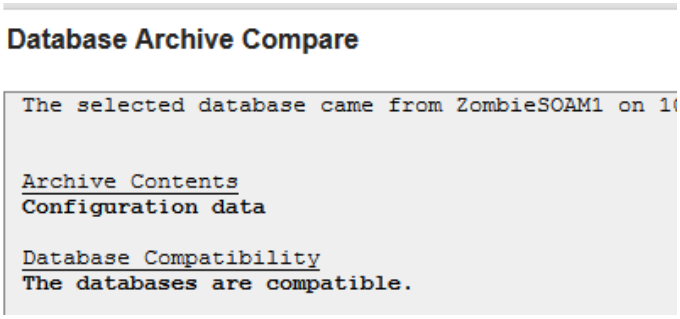
16. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered standby NOAM server and click on **Restart**. 

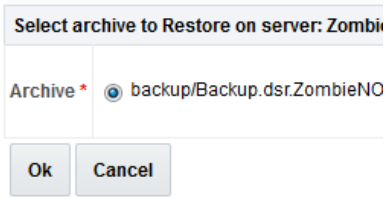
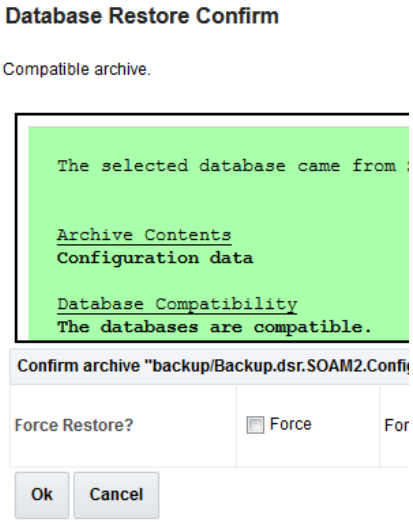
STEP #	Procedure	Description
17. ☐	**NOAM VIP GUI:** Set HA on Standby NOAM	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Select the standby NOAM server, set it to **Active** Press **OK**
18. ☐	**NOAM VIP GUI:** Perform Key exchange with Export Server	Navigate to **Main Menu -> Administration -> Remote Servers -> Data Export**  Click on **SSH Key Exchange** at the bottom of the screen Enter the Password and press **OK** 

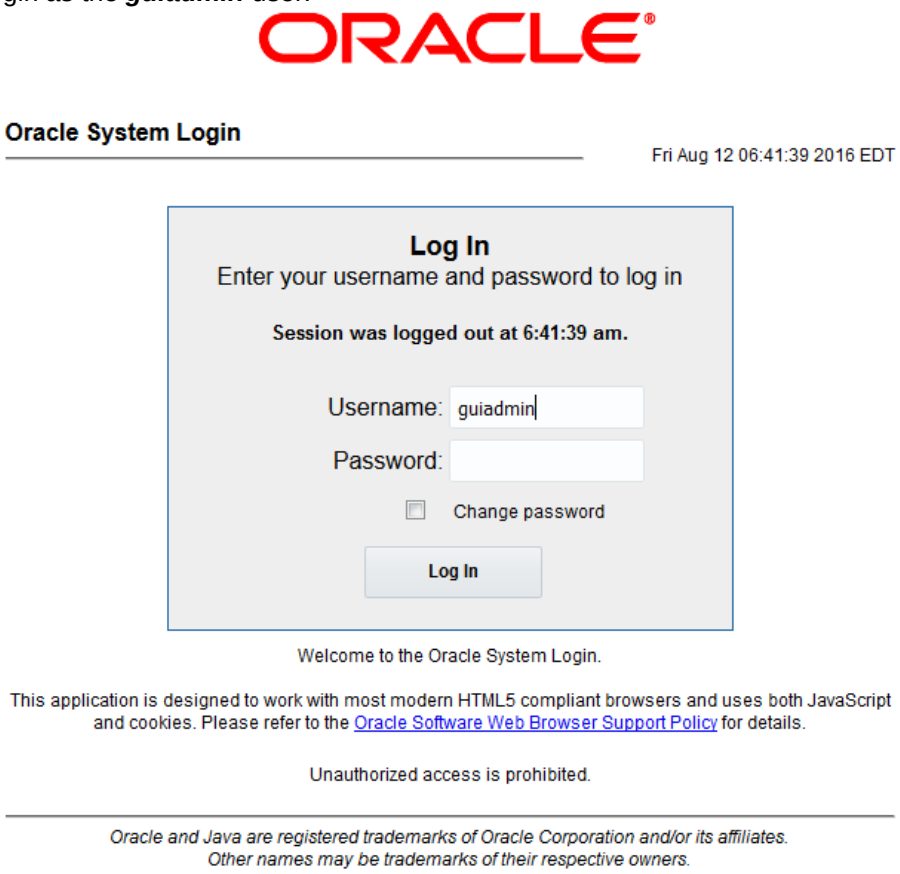
STEP #	Procedure	Description
19. ☐	**NOAM VIP GUI:** Stop Replication to the C-Level Servers of this Site.	Inhibit Replication to the working C Level Servers which belong to the **same site** as of the failed SOAM servers, as the recovery of Active SOAM will cause the database wipeout in the C level servers because of the replication  **If the spare SOAM is also present in the site and lost**: Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost) **If the spare SOAM is NOT deployed in the site:** Execute **Inhibit A** and B Level Replication on C-Level Servers 
20. ☐	**NOAM VIP GUI:** Recover Active SOAM Server	Install the SOAM servers by executing procedures from reference [1] Procedure 22 “Configure the SOAM Servers”, steps 1, 3- 7 **NOTE:** Wait for server to reboot before continuing.
21. ☐	**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**. 

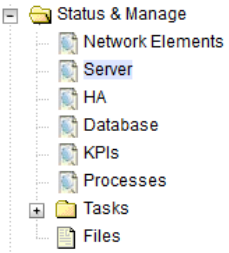
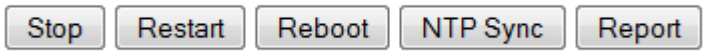
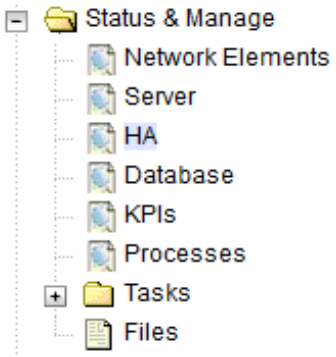
STEP #	Procedure	Description
22. ☐	**NOAM VIP GUI:** Upload the backed up SOAM Database file	Navigate to **Main Menu->Status & Manage->Files** Select the **Active SOAM server**. The following screen will appear. Click on Upload as shown below and select the file *"SO Provisioning and Configuration:"* 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.

STEP #	Procedure	Description
23. ☐	**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: 

STEP #	Procedure	Description
24. ☐	**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 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.

STEP #	Procedure	Description
25. ☐	**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.
26. ☐	**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.

STEP #	Procedure	Description
27. ☐	**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: 
28. ☐	**NOAM VIP GUI:** Recover remaining SOAM Server	Install the SOAM servers by executing procedure from reference [1] Procedure 22 “Configure the SOAM Servers”, steps 1, 3- 6 **NOTE:** Wait for server to reboot before continuing.

STEP #	Procedure	Description
29. ☐	**NOAM VIP GUI:** Restart DSR application on remaining SOAM Server(s)	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered server and click on **Restart**. 
30. ☐	**NOAM VIP GUI:** Set HA on Recovered Standby SOAM Server	**NOAM VIP GUI:** Set HA on Recovered Standby SOAM Server Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Set Max Allowed HA Role to **Active** Press **OK**

<table>
<tr><th>STEP #</th><th>Procedure</th><th>Description</th></tr>
<tr><td>31.
☐</td><td>NOAM VIP GUI: Start Replication on Working C-Level Servers</td><td>Un-Inhibit (Start) Replication to the working C-Level Servers which belong to the same site as of the failed SOAM servers.

<u>If the spare SOAM is also present in the site and lost</u>: Execute Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)

<u>If the spare SOAM is NOT deployed in the site</u>: Execute 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
• 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 examining the Repl Status table as seen below:

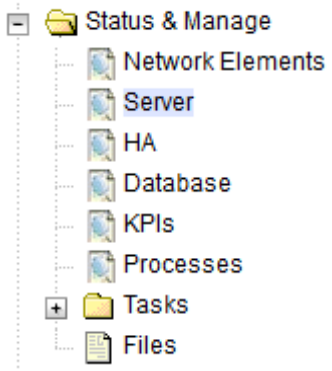
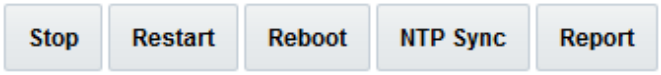
<table>
<tr><th>OAM Repl Status</th><th>SIG Repl Status</th><th>Repl Status</th><th>Repl Audit Status</th></tr>
<tr><td>NotApplicable</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
</table>
</td></tr>
<tr><td>32.
☐</td><td>NOAM VIP GUI: Recover the C-Level Server (DA-MP, SBRs, IPFE,vSTP-MP)</td><td>Establish a SSH session to the C Level server being recovered, login as admusr.

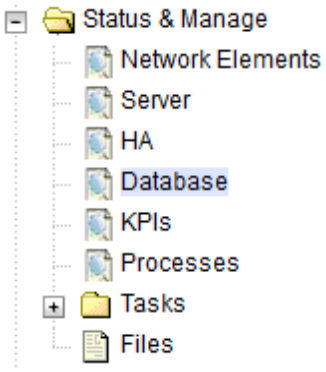
Execute following command to set shared memory to unlimited:

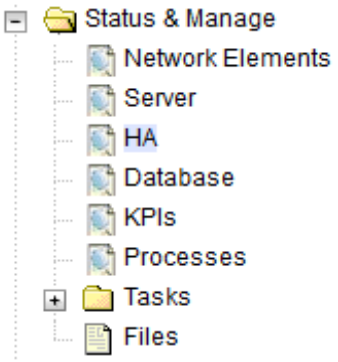
<code>$ sudo shl.set –m 0</code>

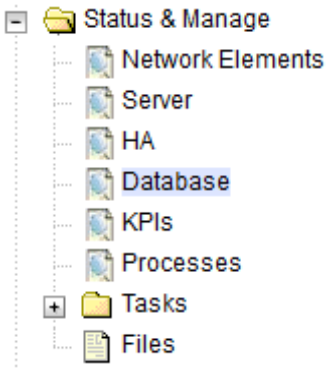
Execute the following procedures from [1] FOR EACH server that has been recovered:

Procedure 25 “Configure the MP Virtual Machines”, Steps 1, 11-14 (& 15 if required).</td></tr>
</table>

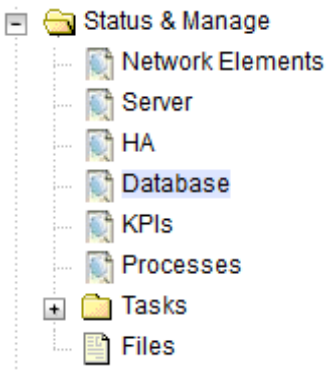
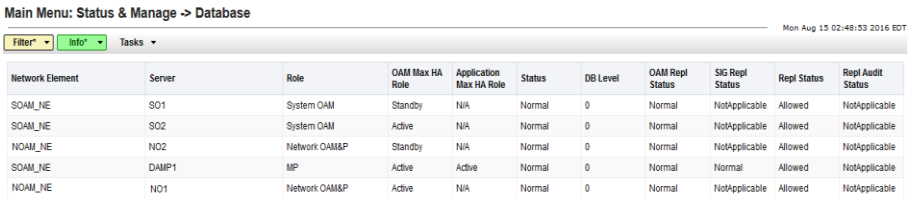
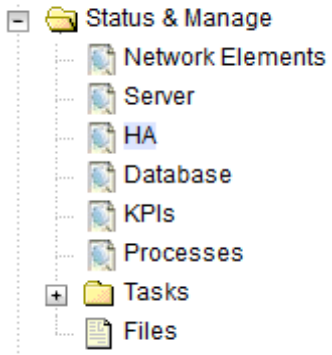
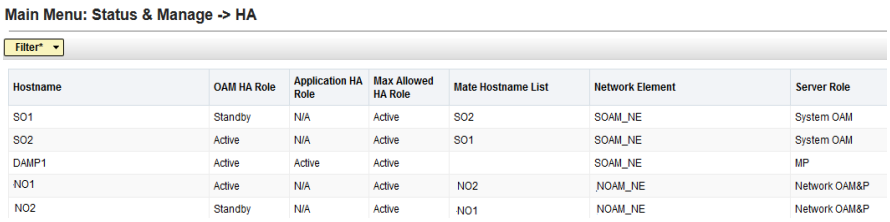
STEP #	Procedure	Description
33. ☐	**NOAM VIP GUI:** Restart DSR application for Recovered C-Level Server	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered server and click on **Restart**. 

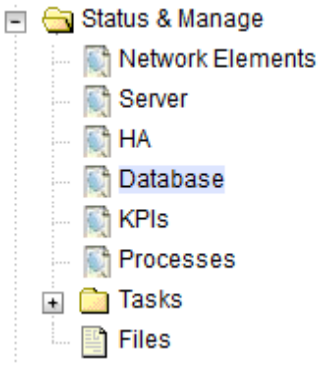
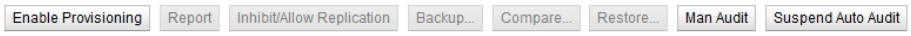
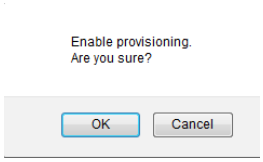
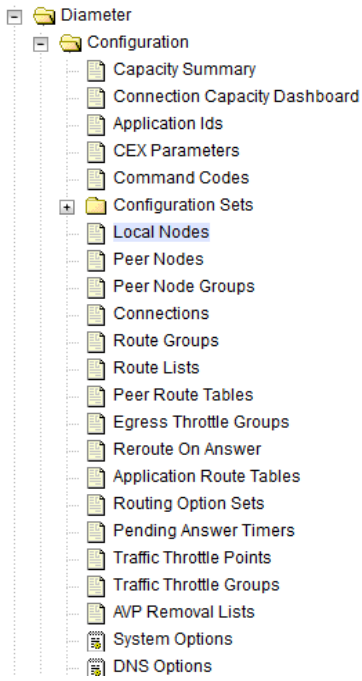
STEP #	Procedure	Description
34. ☐	**NOAM VIP GUI:** Start Replication on all C-Level Servers	Un-Inhibit *(Start)* Replication to the **ALL** C-Level Servers Navigate to **Status & Manage -> Database**  If the *"Repl Status"* is set to "Inhibited", click on the Allow Replication button as shown below using the following order: • Active NOAM Server • Standby NOAM Server • Active SOAM Server • Standby SOAM Server • Spare SOAM Server *(if applicable)* • MP/IPFE Servers Verify that the replication on all the working servers is allowed. This can be done by examining the Repl Status table as seen below: **OAM Repl Status** / **SIG Repl Status** / **Repl Status** / **Repl Audit Status** NotApplicable / NotApplicable / Allowed / NotApplicable Normal / NotApplicable / Allowed / NotApplicable Normal / NotApplicable / Allowed / NotApplicable Normal / NotApplicable / Allowed / NotApplicable

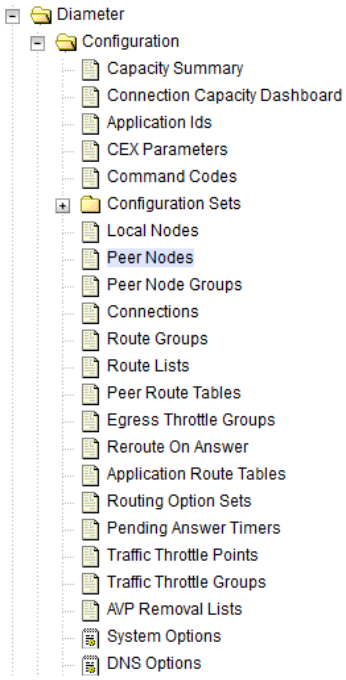
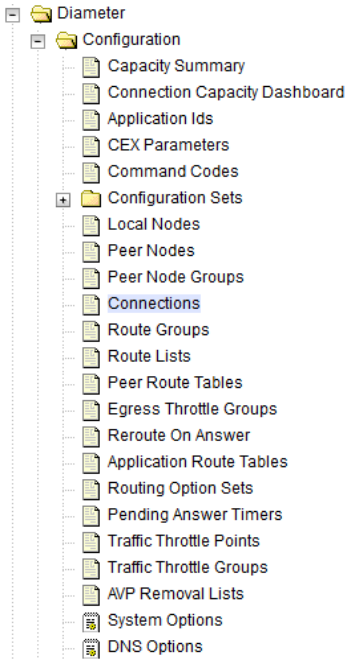
35. ☐	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen For each server whose Max Allowed HA Role is set to OOS, set it to **Active** Press **OK**
36. ☐	**ACTIVE NOAM:** Perform key exchange between the active-NOAM and recovered servers.	Establish an SSH session to the Active NOAM, login as ***admusr.*** Execute the following command to perform a key exchange from the active NOAM to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>` **Note:** If an export server is configured, perform this step.
37. ☐	**ACTIVE NOAM:** Activate Optional Features	Establish an SSH session to the active NOAM, login as ***admusr.*** **Note for PCA Feature Activation:** If you have PCA installed in the system being recovered, execute the procedure "*PCA Activation on Stand By NOAM server*" on recovered Standby NOAM Server and procedure "*PCA Activation on Active SOAM server*" on recovered Active SOAM Server from [3] to re-activate PCA Refer to **section** 1.5 Optional Features to activate any features that were previously activated. **Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: `iload#31000{S/W Fault}` **Note**: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature. Refer to **section** 1.5 Optional Features to activate any features that were previously activated.

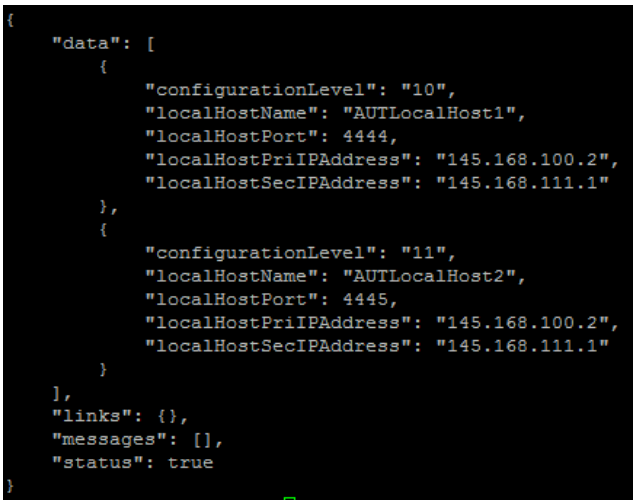
38. ☐	**NOAM VIP GUI:** Fetch and Store the database Report for the Newly Restored Data and Save it	Navigate to **Main Menu->Status & Manage->Database**
		 
		Select the **active** NOAM server and click on the **Report** button at the bottom of the page. The following screen is displayed:
		Main Menu: Status & Manage -> Database [Report]
		`dsr Database Status Report`
		`Report Generated: Tue Oct 11 13:24:26 2016 EDT`
		`From: Active Network OAM&P on host ZombieNOAM1`
		`Report Version: 8.0.0.0.0-80.9.0`
		`User: guiadmin`
		`General`
		`Hostname : ZombieNOAM1`
		`Database Birthday : 2016-07-11 11:21:50 EDT`
		`Appworks Database Version : 6.0`
		`Application Database Version :`
		`Capacities and Utilization`
		`Disk Utilization 8.4%: 585M used of 7.0G total, 6.0G available`
		`Memory Utilization 0.0%: used of total, 0M available`
		Click on **Save** and save the report to your local machine.

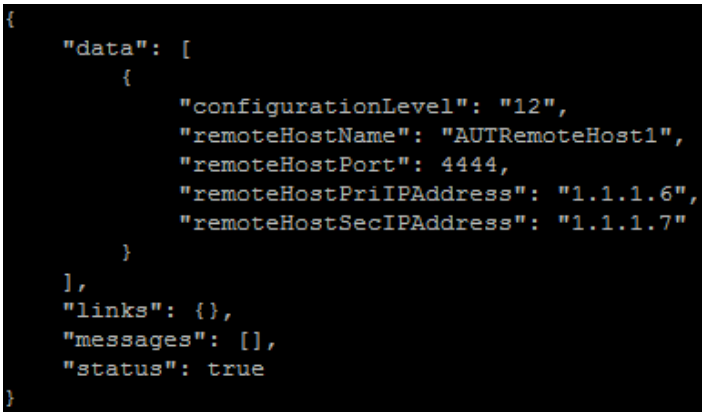
39. ☐	**ACTIVE NOAM:** Verify Replication Between Servers.	Login to the Active NOAM via SSH terminal as ***admusr*** user.
		Execute the following command:
		$ sudo irepstat –m
		
		Output like below shall be generated:
		
		`-- Policy 0 ActStb [DbReplication] ----------`
		`Oahu-DAMP-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.15%cpu 25B/s  A=me`
		`  CC To  Oahu-DAMP-2  Active  0  0.10  0.14%cpu 25B/s  A=me`
		`Oahu-DAMP-2 -- Stby`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.11%cpu 31B/s  A=C3642.212`
		`  CC From Oahu-DAMP-1  Active  0  0.10 ^0.14 1.16%cpu 31B/s A=C3642.212`
		`Oahu-IPFE-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 24B/s  A=C3642.212`
		`Oahu-IPFE-2 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 28B/s  A=C3642.212`
		`Oahu-NOAM-1 -- Stby`
		`  AA From Oahu-NOAM-2  Active  0  0.25 ^0.03%cpu 23B/s`
		`Oahu-NOAM-2 -- Active`
		`  AA To  Oahu-NOAM-1  Active  0  0.25 1%R 0.04%cpu 61B/s`
		`  AB To  Oahu-SOAM-2  Active  0  0.50 1%R 0.05%cpu 75B/s`
		`Oahu-SOAM-1 -- Stby`
		`  BB From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 27B/s`
		`Oahu-SOAM-2 -- Active`
		`  AB From Oahu-NOAM-2  Active  0  0.50 ^0.03%cpu 24B/s`
		`  BB To  Oahu-SOAM-1  Active  0  0.50 1%R 0.04%cpu 32B/s`
		`  BC To  Oahu-IPFE-1  Active  0  0.50 1%R 0.04%cpu 21B/s`
		
		`irepstat ( 40 lines) (h)elp (m)erged`

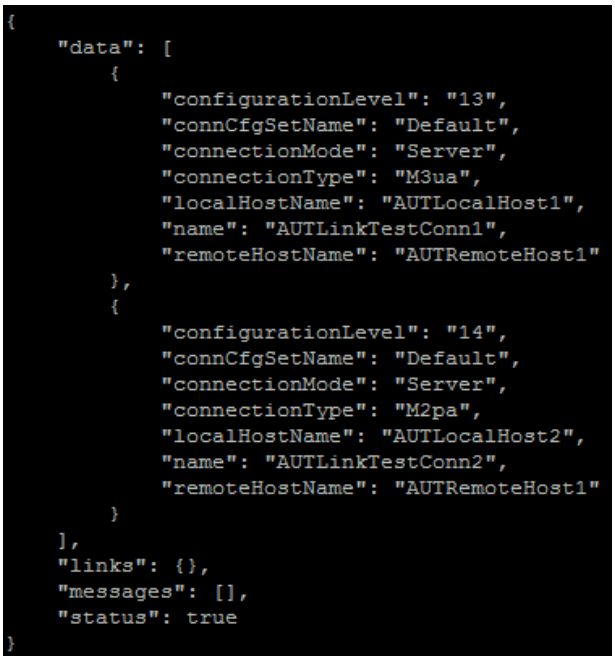
40. ☐	**NOAM VIP GUI:** Verify the Database states	Click on **Main Menu->Status and Manager->Database**  Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below: 
41. ☐	**NOAM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

42. ☐	**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. 
43. ☐	**SOAM VIP GUI:** Verify the Local Node Info	Navigate to **Main Menu->Diameter->Configuration->Local Node**  Verify that all the local nodes are shown.

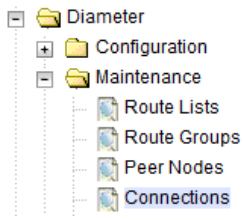
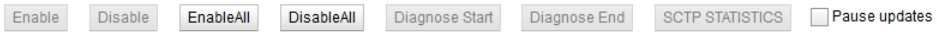
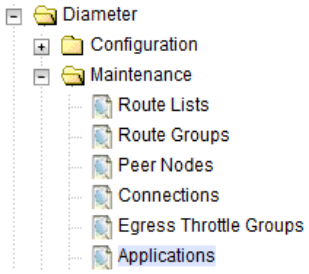
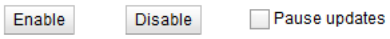
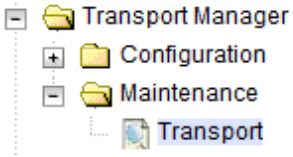
44. ☐	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.
45. ☐	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections**  Verify that all the connections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

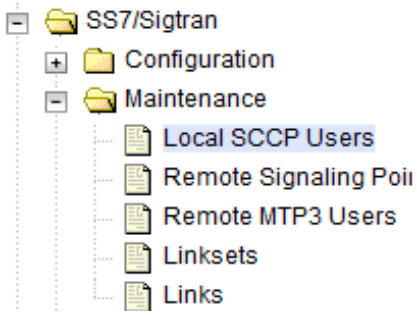
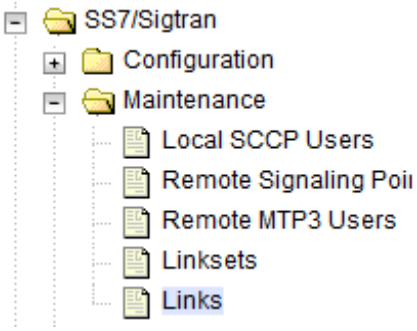
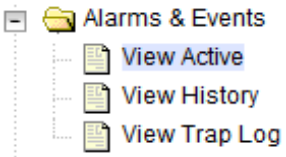
46. ☐	**For vSTP Only-SOAM VIP Server Console (Optional):** Verify the local nodes info	To verify the vSTP MP **Local nodes** info:
		1. Login to the SOAM VIP Server console as **admusr**
		2. Execute the following command
		[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts
		3. Verify the output similar to the below output
		  {
		"data": [
		{
		"configurationLevel": "10",
		"localHostName": "AUTLocalHost1",
		"localHostPort": 4444,
		"localHostPriIPAddress": "145.168.100.2",
		"localHostSecIPAddress": "145.168.111.1"
		},
		{
		"configurationLevel": "11",
		"localHostName": "AUTLocalHost2",
		"localHostPort": 4445,
		"localHostPriIPAddress": "145.168.100.2",
		"localHostSecIPAddress": "145.168.111.1"
		}
		],
		"links": {},
		"messages": [],
		"status": true
		}

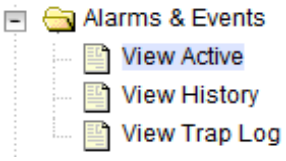
47. ☐	**For vSTP Only-SOAM VIP Server Console (Optional):** Verify the remote nodes info	To verify the vSTP MP **Remote nodes** info:
		1. Login to the SOAM VIP Server console as **admusr**
		2. Execute the following command
		[admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts
		3. Verify the output similar to the below output
		  {
		"data": [
		{
		"configurationLevel": "12",
		"remoteHostName": "AUTRemoteHost1",
		"remoteHostPort": 4444,
		"remoteHostPriIPAddress": "1.1.1.6",
		"remoteHostSecIPAddress": "1.1.1.7"
		}
		],
		"links": {},
		"messages": [],
		"status": true
		}

48. ☐	**For vSTP Only-SOAM VIP Server Console (Optional):** Verify the Connections info	To verify the vSTP MP **Connections** info:
		1. Login to the SOAM VIP Server console as **admusr**
		2. Execute the following command
		[admusr@SOAM1 ~]$ mmiclient.py /vstp/connections
		3. Verify the output similar to the below output
		  {
		"data": [
		{
		"configurationLevel": "13",
		"connCfgSetName": "Default",
		"connectionMode": "Server",
		"connectionType": "M3ua",
		"localHostName": "AUTLocalHost1",
		"name": "AUTLinkTestConn1",
		"remoteHostName": "AUTRemoteHost1"
		},
		{
		"configurationLevel": "14",
		"connCfgSetName": "Default",
		"connectionMode": "Server",
		"connectionType": "M2pa",
		"localHostName": "AUTLocalHost2",
		"name": "AUTLinkTestConn2",
		"remoteHostName": "AUTRemoteHost1"
		}
		],
		"links": {},
		"messages": [],
		"status": true
		}

49. ☐	**MP Servers:** Disable SCTP Auth Flag	For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [1]. Execute this procedure on all Failed MP Servers.

50. ☐	**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
51. ☐	**SOAM VIP GUI:** Enable Optional Features	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Select the optional feature application configured before. Click the **Enable** button. 
52. ☐	**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.

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

56. ☐	**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 My Oracle Support (MOS)
57. ☐	**Restore GUI Usernames and Passwords**	If applicable, Execute steps in **Section 6.0** to recover the user and group information restored.
58. ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **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 6. 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.

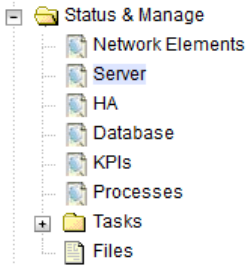
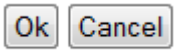
- Recover the software.
- Recover the Database.

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.

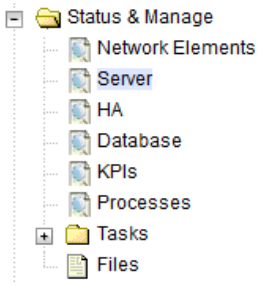
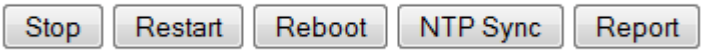
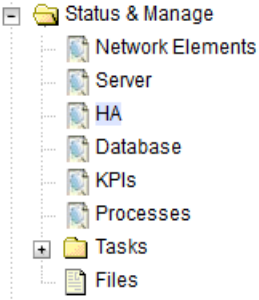
Procedure 6. Recovery Scenario 2

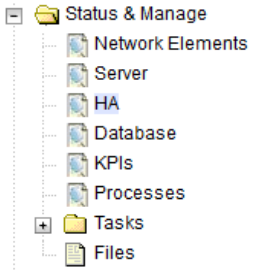
STEP #	Procedure	Description
This procedure performs recovery if at least 1 NOAM server is available but all SOAM servers in a site have failed. This includes any SOAM server that is in another location. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	**Workarounds**	Refer to **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

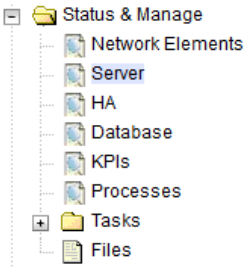
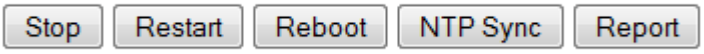
STEP #	Procedure	Description
3. ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 
4. ☐	**Active NOAM:** Set Failed Servers to OOS	Navigate to **Main Menu -> Status & Manage -> HA**  Select **Edit** Set the Max Allowed HA Role drop down box to **OOS** for the failed servers. Select **Ok** 

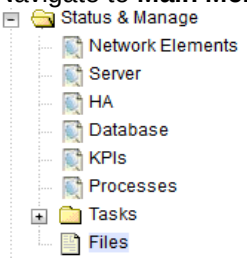
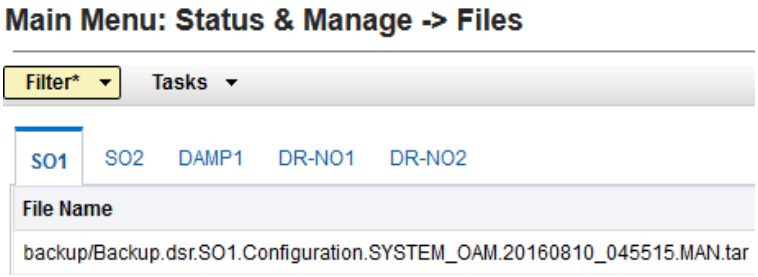
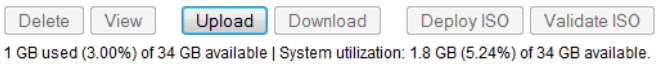
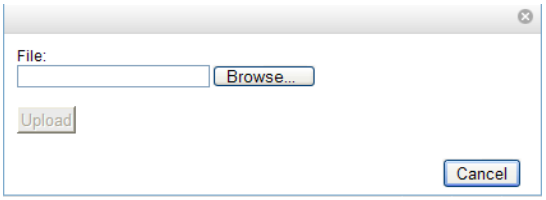
STEP #	Procedure	Description
5. ☐	**Create VMs Recover the Failed Software**	For VMWare based deployments: 1. For NOAMs execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 2 (VMWare Only). Configure NOAM guests based on resource profile 2. For SOAMs execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile For KVM/Openstack based deployments: 1. For NOAMs execute the following procedures from reference [1]: a. Procedure 4 (KVM/Openstack). "Import DSR OVA" [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 5 (KVM/Openstack). "Configure NOAM guests based on resource profile" 2. For SOAMs execute the following procedures from reference [1]: a. Procedure 4 (KVM/Openstack). "Import DSR OVA" [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests based on resource profile" For OVM-S/OVM-M based deployments: Execute the following procedures from reference [1]: a. Procedure 7 (OVM-S/OVM-M). Import DSR OVA and prepare for VM creation b. Procedure 8 (OVM-S/OVM-M). Configure each DSR VM ***Note***: While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs)
6. ☐	**Repeat for Remaining Failed Servers**	If necessary, repeat **step 5** for all remaining failed servers.

STEP #	Procedure	Description
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 15 “Configure the Second NOAM Server” steps 1, 3-7 Procedure 16 “Complete Configuring the NOAM Server Group” Step 4 **Note:** If Topology or nodeId alarms are persistent after the database restore, refer to Workarounds for Issues not fixed in this Release or the next step below.

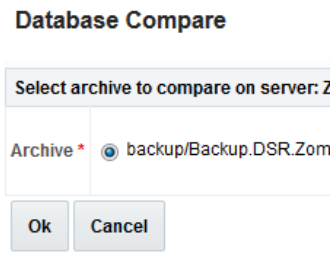
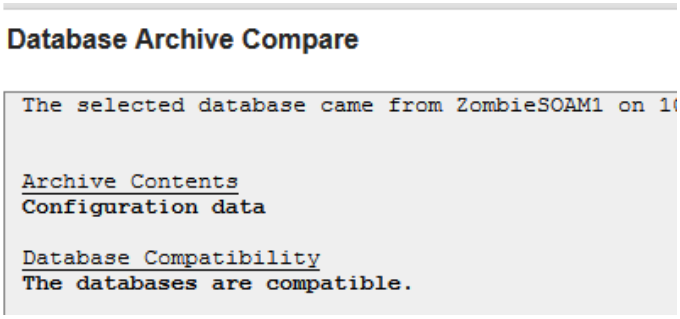
STEP #	Procedure	Description
9. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered standby NOAM server and click on **Restart**. 
10. ☐	**NOAM VIP GUI:** Set HA on Standby NOAM	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Select the standby NOAM server, set it to **Active** Press **OK**

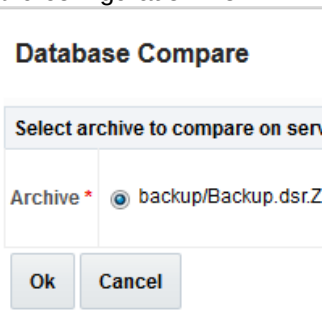
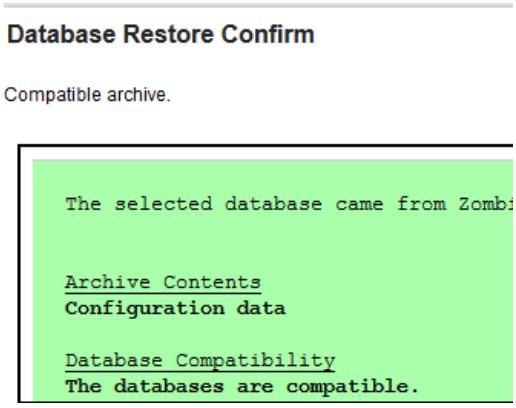
STEP #	Procedure	Description
11. ☐	**NOAM VIP GUI:** Stop Replication to the C-Level Servers of this Site.	Inhibit Replication to the working C Level Servers which belong to the **same site** as the failed SOAM servers, as the recovery of Active SOAM will cause the database wipeout in the C level servers because of the replication **If the spare SOAM is also present in the site and lost**: Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost) **If the spare SOAM is NOT deployed in the site:** Execute **Inhibit A** and B Level Replication on C-Level Servers
12. ☐	**NOAM VIP GUI:** Recover Active SOAM Server	Install the SOAM servers by executing procedure from reference [1]: Procedure 22 “Configure the SOAM Servers”, steps 1, 3- 7 **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**

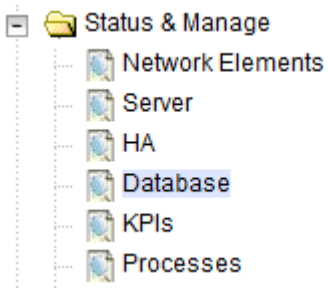
STEP #	Procedure	Description
14. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered Active SOAM server and click on **Restart**. 

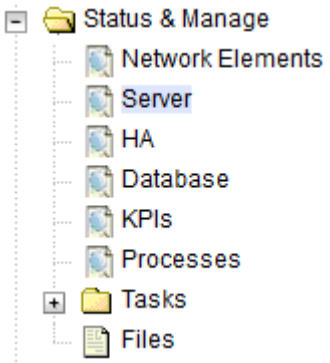
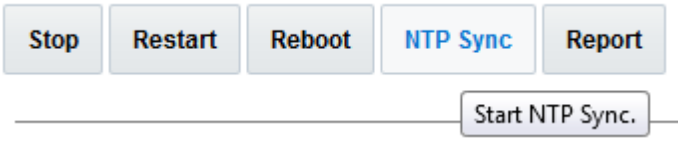
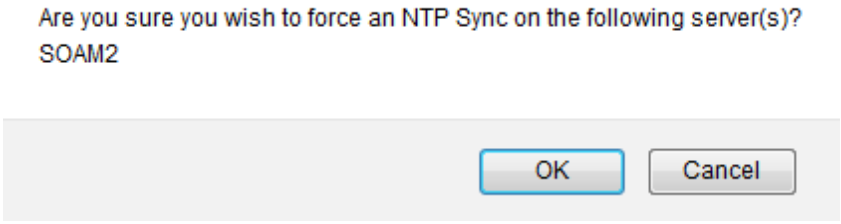
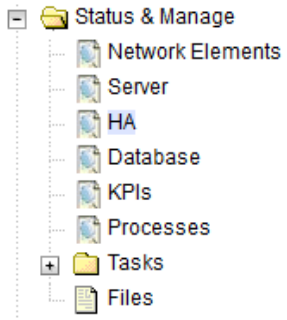
STEP #	Procedure	Description
15. ☐	**NOAM VIP GUI:** Upload the backed up SOAM Database file	Navigate to **Main Menu->Status & Manage->Files**  Select the Active SOAM server. The following screen will appear:  Click on **Upload** as shown below and select the file *"NO Provisioning and Configuration:"* 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.

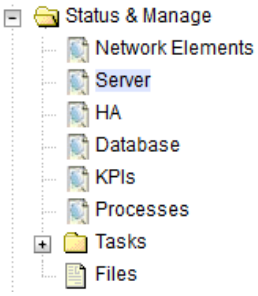
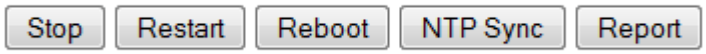
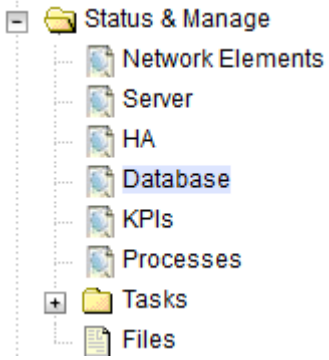
STEP #	Procedure	Description
16. ☐	**Recovered SOAM GUI:** Login	Establish a GUI session on the recovered SOAM server. Open the web browser and enter a URL of: `http://<Recovered_SOAM_IP_Address>` Login as the ***guiadmin*** user: 

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 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.

STEP #	Procedure	Description
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 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. The provisioning will be disabled after this step.
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.

STEP #	Procedure	Description
20. ☐	**NOAM VIP GUI:** Recover remaining SOAM Server	Install the SOAM servers by executing procedure from reference [1]: Procedure 22 “Configure the SOAM Servers”, steps 1, 3- 6 **NOTE:** Wait for server to reboot before continuing.
21.	**NOAM VIP GUI:** Start replication on the recovered SOAMs	Un-Inhibit *(Start)* Replication to the recovered SOAM servers Navigate to **Status & Manage -> Database**  Click on the Allow Replication button as shown below on the recovered SOAM servers. Verify that the replication on all SOAMs servers is allowed. This can be done by checking 'Repl status' column of respective server

STEP #	Procedure	Description
22. ☐	**Recovered Server:** Sync NTP	Navigate to **Status & Manage -> Server**  Select the Recovered server and click NTP Sync button  Click **Ok** 
23.	**NOAM VIP GUI:** Set HA on SOAM Servers	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**

STEP #	Procedure	Description
24. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered server and click on **Restart**. 
25.	**SOAM GUI:** Enable Provisioning	Click on **Main Menu->Status & Manage->Database**  Enable Provisioning by clicking on **Enable Site Provisioning** button at the bottom of the screen as shown below.  A confirmation window will appear, press **OK** to enable Provisioning.

<table>
<tr><th>STEP #</th><th>Procedure</th><th>Description</th></tr>
<tr><td>26.
☐</td><td>NOAM VIP GUI: Start Replication on working C-Level Servers</td><td>Un-Inhibit (Start) Replication to the working C-Level Servers which belong to the same site as of the failed SOAM servers.

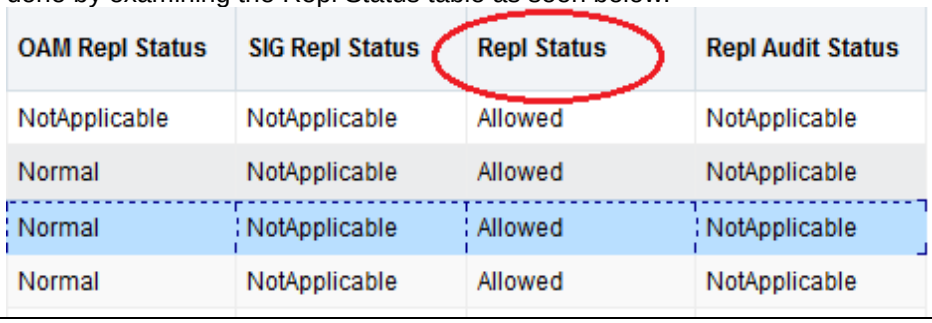
<u>If the spare SOAM is also present in the site and lost</u>: Execute Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)

<u>If the spare SOAM is NOT deployed in the site</u>: Execute 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
• 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 examining the Repl Status table as seen below:
 
<table>
<tr><th>OAM Repl Status</th><th>SIG Repl Status</th><th>Repl Status</th><th>Repl Audit Status</th></tr>
<tr><td>NotApplicable</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
</table></td></tr>
<tr><td>27.
☐</td><td>NOAM VIP GUI: Recover the C-Level Server (DA-MP, SBRs, IPFE, vSTP-MP)</td><td>Establish a SSH session to the C Level server being recovered, login as admusr.

Execute following command to set shared memory to unlimited:

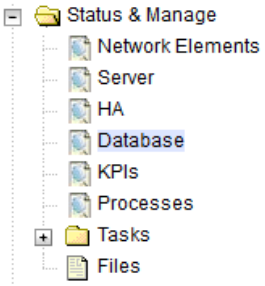
<code>$ sudo shl.set –m 0</code>

Execute the following procedures from [1] FOR EACH server that has been recovered:

Procedure 25 “Configure the MP Virtual Machines”, Steps 1, 8-14 (& 15 if required).</td></tr>
</table>

<table>
<tr><th>STEP #</th><th>Procedure</th><th>Description</th></tr>
<tr><td>28.
☐</td><td>NOAM VIP GUI: Start replication on ALL C-Level Servers</td><td>Un-Inhibit (Start) Replication to the ALL C-Level Servers

Navigate to Status & Manage -> Database

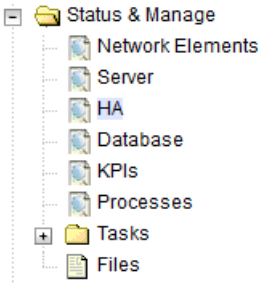
 

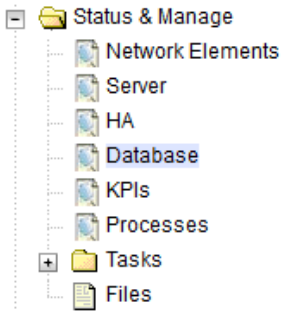
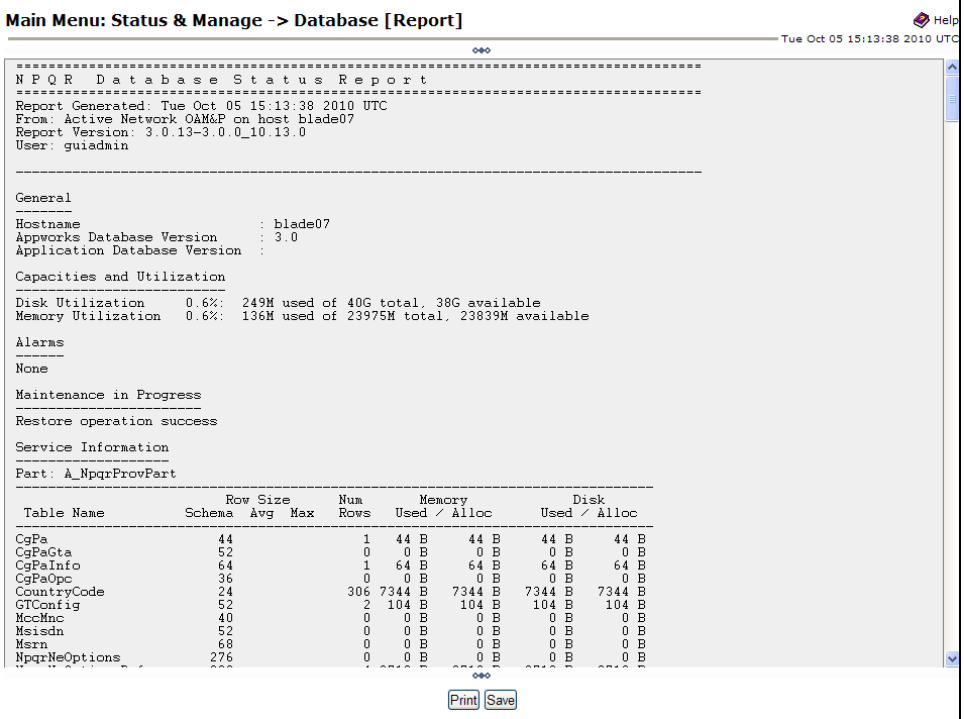
If the “Repl Status” is set to “Inhibited”, click on the Allow Replication button as shown below using the following order:

• Active NOAM Server
• Standby NOAM Server
• Active SOAM Server
• Standby SOAM Server
• Spare SOAM Server (if applicable)
• MP/IPFE Servers

Verify that the replication on all the working servers is allowed. This can be done by examining the Repl Status table as seen below:

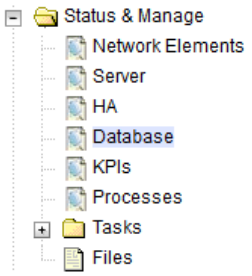
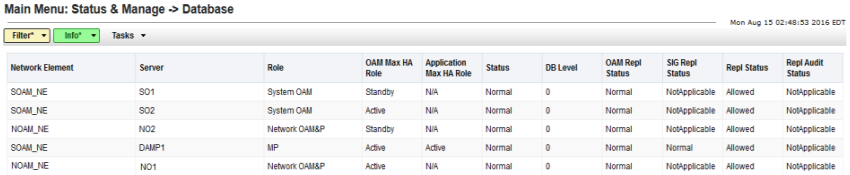
<table>
<tr><th>OAM Repl Status</th><th>SIG Repl Status</th><th>Repl Status</th><th>Repl Audit Status</th></tr>
<tr><td>NotApplicable</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
</table>
</td></tr>
</table>

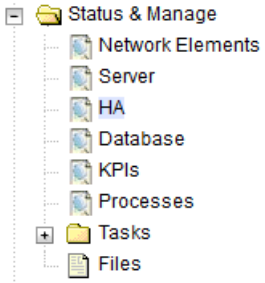
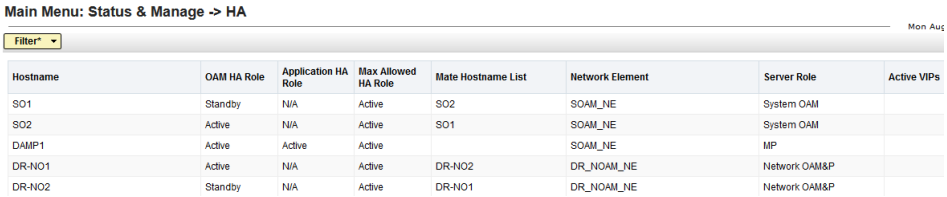
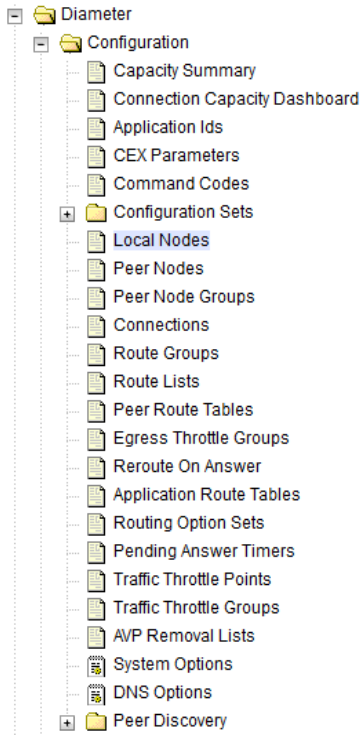
STEP #	Procedure	Description
29. ☐	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen For each server whose Max Allowed HA Role is set to Standby, set it to **Active** Press **OK**
30. ☐	**ACTIVE NOAM:** Perform key exchange 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.
31. ☐	**ACTIVE NOAM:** Activate Optional Features	Establish an SSH session to the active NOAM, login as ***admusr.*** **Note for PCA Feature Activation:** If you have PCA installed in the system being recovered, execute the procedure "*PCA Activation on Standby NOAM server*" on recovered NOAM Server and procedure "*PCA Activation on Stand By SOAM server*" on recovered Standby SOAM from [3] to re-activate PCA **Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: *iload#31000{S/W Fault}* **Note**: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature. Refer to **section** 1.5 Optional Features to activate any features that were previously activated.

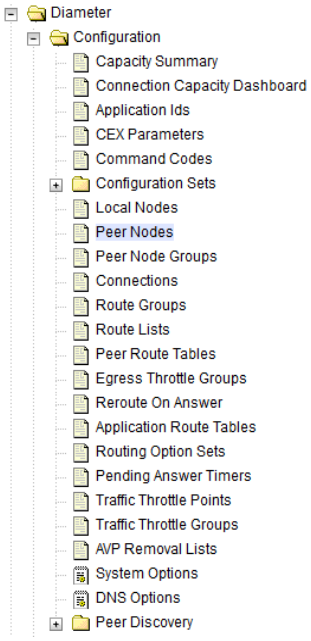
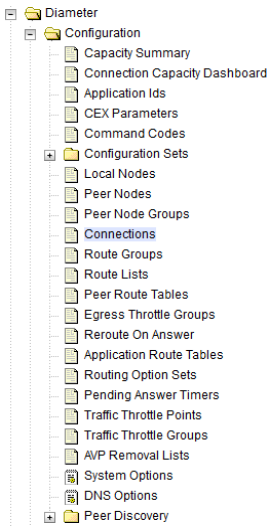
STEP #	Procedure	Description
32. ☐	**NOAM VIP GUI:** Fetch and Store the database Report for the Newly Restored Data and Save it	Navigate to **Main Menu->Status & Manage->Database**  Select the **active** NOAM server and click on the **Report** button at the bottom of the page. The following screen is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

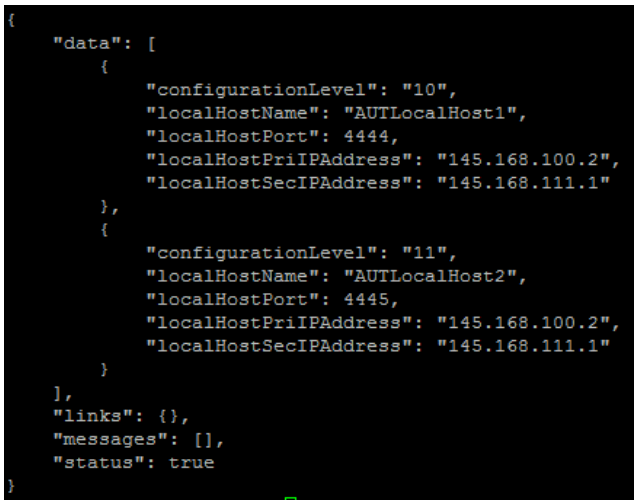
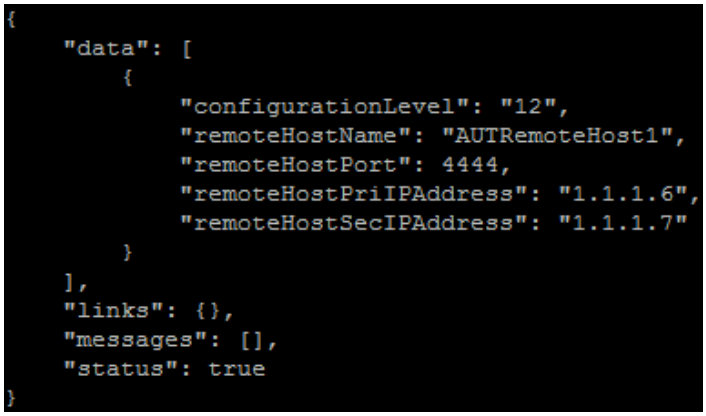
STEP #	Procedure	Description

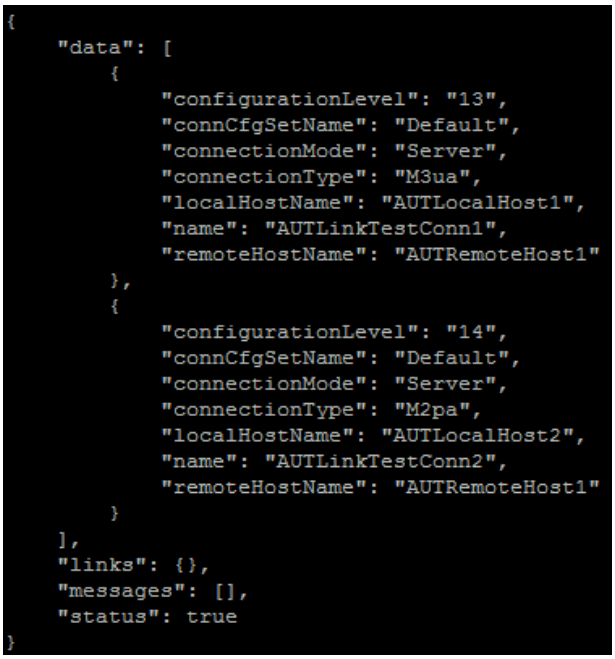
33. ☐	**ACTIVE NOAM:** Verify Replication Between Servers.	1. Login to the Active NOAM via SSH terminal as ***admusr*** user.
		2. Execute the following command:
		`$ sudo irepstat –m`
		Output like below shall be generated:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`Oahu-DAMP-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.15%cpu 25B/s  A=me`
		`  CC To  Oahu-DAMP-2  Active  0  0.10  0.14%cpu 25B/s  A=me`
		`Oahu-DAMP-2 -- Stby`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.11%cpu 31B/s  A=C3642.212`
		`  CC From Oahu-DAMP-1  Active  0  0.10 ^0.14 1.16%cpu 31B/s`
		`A=C3642.212`
		`Oahu-IPFE-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 24B/s  A=C3642.212`
		`Oahu-IPFE-2 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 28B/s  A=C3642.212`
		`Oahu-NOAM-1 -- Stby`
		`  AA From Oahu-NOAM-2  Active  0  0.25 ^0.03%cpu 23B/s`
		`Oahu-NOAM-2 -- Active`
		`  AA To  Oahu-NOAM-1  Active  0  0.25 1%R 0.04%cpu 61B/s`
		`  AB To  Oahu-SOAM-2  Active  0  0.50 1%R 0.05%cpu 75B/s`
		`Oahu-SOAM-1 -- Stby`
		`  BB From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 27B/s`
		`Oahu-SOAM-2 -- Active`
		`  AB From Oahu-NOAM-2  Active  0  0.50 ^0.03%cpu 24B/s`
		`  BB To  Oahu-SOAM-1  Active  0  0.50 1%R 0.04%cpu 32B/s`
		`  BC To  Oahu-IPFE-1  Active  0  0.50 1%R 0.04%cpu 21B/s`
		`irepstat ( 40 lines) (h)elp (m)erged`

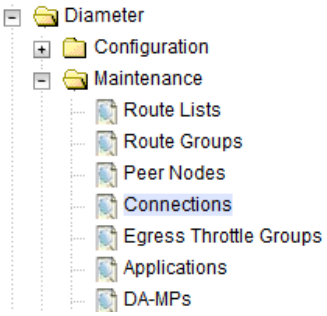
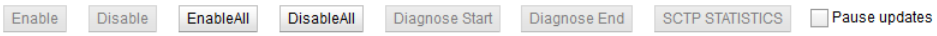
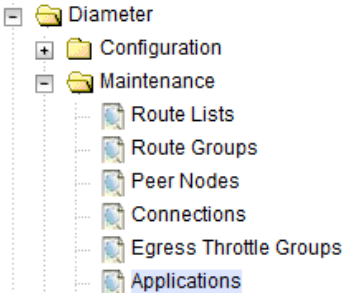
34. ☐	**NOAM VIP GUI:** Verify the Database states	Click on **Main Menu->Status and Manager->Database**  Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below: 

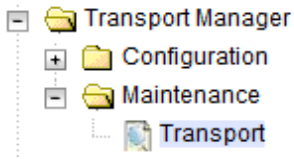
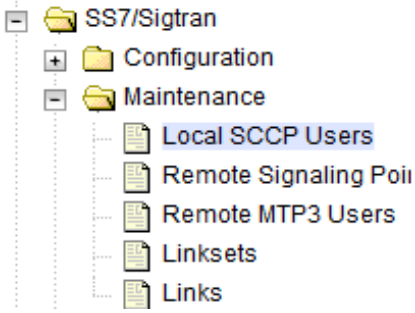
STEP #	Procedure	Description
35. ☐	**NOAM VIP GUI:** Verify the HA Status	Click on **Main Menu->Status and Manage->HA**  Select the row for all of the servers Verify that the “HA Role” is either “Active” or “Standby”.  Hostname / OAM HA Role / Application HA Role / Max Allowed HA Role / Mate Hostname List / Network Element / Server Role / Active VIPs SO1 / Standby / N/A / Active / SO2 / SOAM_NE / System OAM SO2 / Active / N/A / Active / SO1 / SOAM_NE / System OAM DAMP1 / Active / Active / Active / SOAM_NE / MP DR-NO1 / Active / N/A / Active / DR-NO2 / DR_NOAM_NE / Network OAM&P DR-NO2 / Standby / N/A / Active / DR-NO1 / DR_NOAM_NE / Network OAM&P
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.

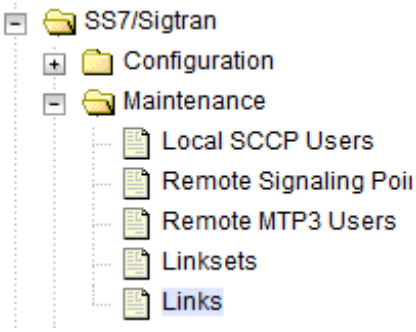
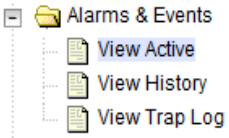
STEP #	Procedure	Description
37. ☐	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.
38. ☐	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections** 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

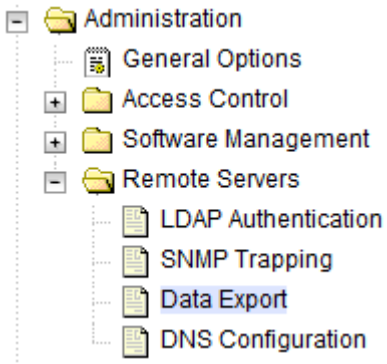
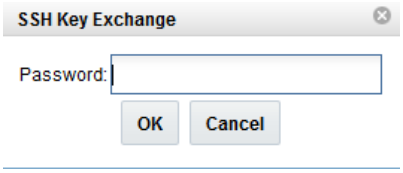
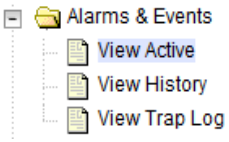
STEP #	Procedure	Description
39. ☐	**For vSTP Only- SOAM VIP Server Console (Optional):** Verify the local nodes info	To verify the vSTP MP **Local nodes** info: 1. Login to the SOAM VIP Server console as **admusr** 2. Execute the following command [admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts 3. Verify the output similar to the below output 
40. ☐	**For vSTP Only- SOAM VIP Server Console (Optional):** Verify the remote nodes info	To verify the vSTP MP **Remote nodes** info: 1. Login to the SOAM VIP Server console as **admusr** 2. Execute the following command [admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts 3. Verify the output similar to the below output 

STEP #	Procedure	Description
41. ☐	**For vSTP Only- SOAM VIP Server Console (Optional):** Verify the Connections info	To verify the vSTP MP **Connections** info: 1. Login to the SOAM VIP Server console as **admusr** 2. Execute the following command [admusr@SOAM1 ~]$ mmiclient.py /vstp/connections 3. Verify the output similar to the below output 
42. ☐	**MP Servers:** Disable SCTP Auth Flag	For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS procedure from reference [1]. Execute this procedure on all Failed MP Servers.

STEP #	Procedure	Description
43. ☐	**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.
44. ☐	**SOAM VIP GUI:** Enable Optional Features	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Select the optional feature application configured in **step 29**. Click the **Enable** button. 

STEP #	Procedure	Description
45. ☐	**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.
46. ☐	**SOAM VIP GUI:** Re-enable MAPIWF application if needed	Navigate to **Main Menu->Sigtran->Maintenance->Local SCCP Users**  Click on the **Enable** button corresponding to MAPIWF Application Name.  Verify that the SSN Status is Enabled.

STEP #	Procedure	Description
47. ☐	**SOAM VIP GUI:** Re-enable links if needed	Navigate to **Main Menu->Sigtran->Maintenance->Links**  Click on **Enable** button for each link.  Verify that the Operational Status for each link is Up.
48. ☐	**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 My Oracle Support (MOS)

STEP #	Procedure	Description
49.	**SOAM VIP GUI:** Perform Keyexchange with Export Server	Navigate to **Main Menu -> Administration -> Remote Servers -> Data Export**  Click on **Key Exchange** at the bottom of the screen Enter the Password and press **OK** 
50. ☐	**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 My Oracle Support (MOS).
51. ☐	**Backup and Archive All the Databases from the Recovered System**	Execute 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 7. 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.

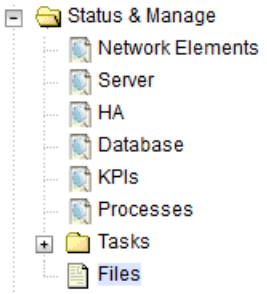
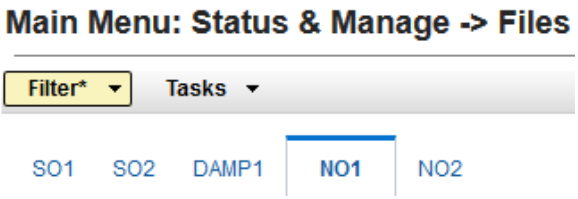
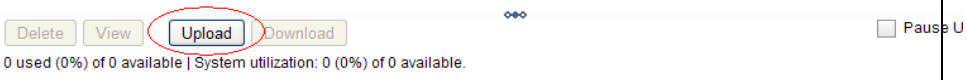
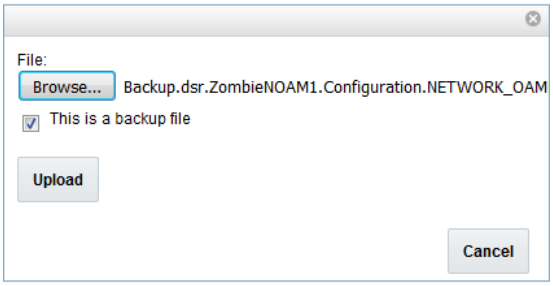
- Recover the software.
- Database is already intact at one SOAM server and does not require restoration at the other SOAM and MP servers.

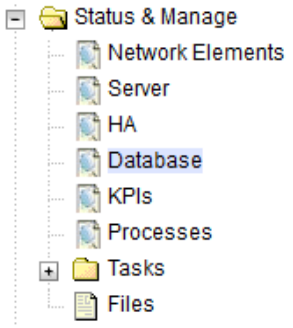
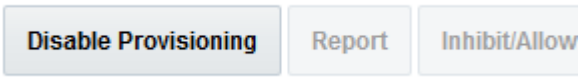
Procedure 7. Recovery Scenario 3

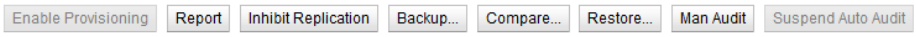
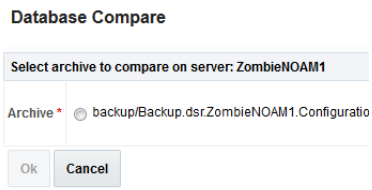
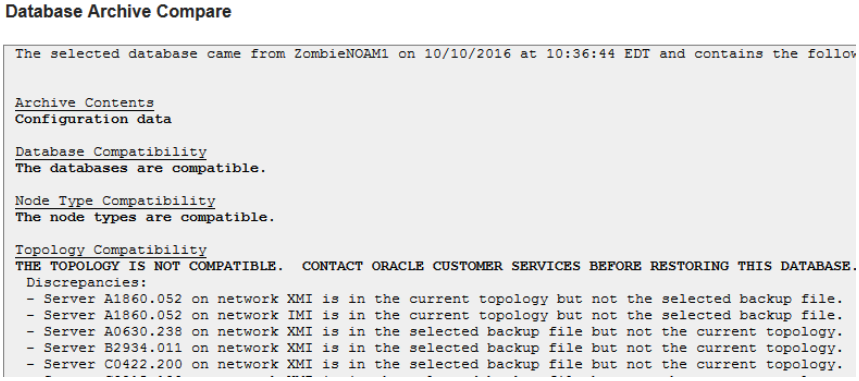
STEP #	Procedure	Description
This procedure performs recovery if ALL NOAM servers are failed but 1 or more SOAM servers are intact. This includes any SOAM server that is in another location (spare SOAM server). Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	**Workarounds**	Refer to **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

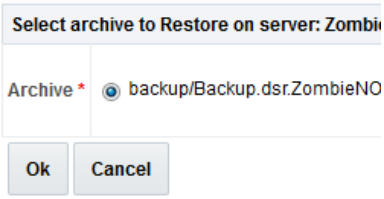
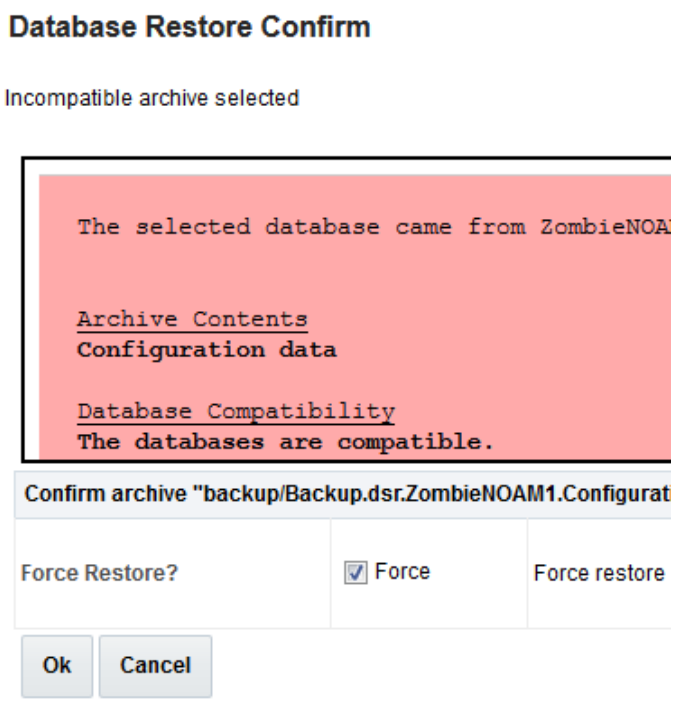
3. ☐	**Recover the Failed Software**	For VMWare based deployments: 1. For NOAMs execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 2 (VMWare Only). Configure NOAM guests based on resource profile 2. For SOAMs execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile 3. For failed MPs execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile For KVM/Openstack based deployments: 1. For NOAMs execute the following procedures from reference [1]: a. Procedure 4 (KVM/Openstack). "Import DSR OVA" [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 5 (KVM/Openstack). "Configure NOAM guests based on resource profile" 2. For SOAMs execute the following procedures from reference [1]: a. Procedure 4 (KVM/Openstack). "Import DSR OVA" [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests based on resource profile" 3. For failed MPs execute the following procedures from reference [1]: a. Procedure 4 (KVM/Openstack). "Import DSR OVA" [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests based on resource profile" For OVM-S / OVM-M based deployments: Execute the following procedures from reference [1]: a. Procedure 7 (OVM-S/OVM-M). Import DSR OVA and prepare for VM creation b. Procedure 8 (OVM-S/OVM-M). Configure each DSR VM ***Note***: While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs)

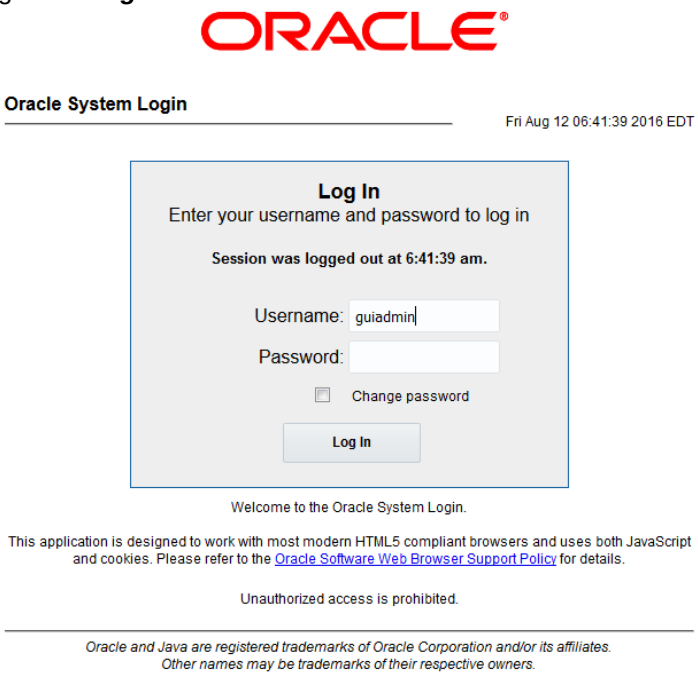
STEP #	Procedure	Description
4. ☐	**Obtain Latest Database Backup and Network Configuration Data.**	Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. From required materials list in **Section 3.1 Required Materials**; use site survey documents 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 13 “Configure the First NOAM NE and Server” and Procedure 14 “Configure the NOAM Server Group”.
6. ☐	**NOAM GUI:** Login	Login to the NOAM GUI as the ***guiadmin*** user: 

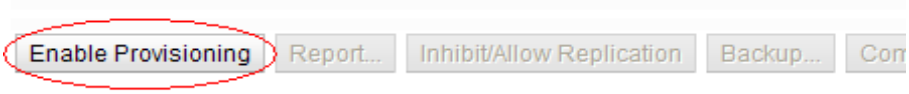
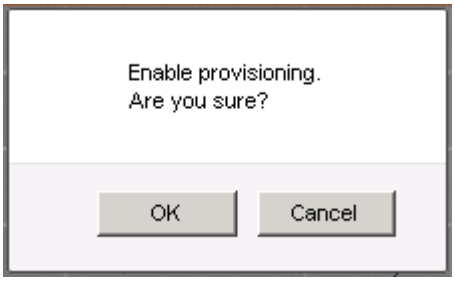
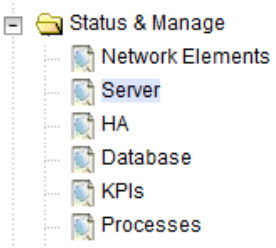
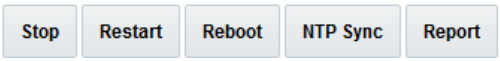
STEP #	Procedure	Description
7. ☐	**NOAM GUI:** Upload the Backed up Database File	Browse to **Main Menu->Status & Manage->Files**  Select the Active NOAM server. The following screen will appear:  Click on **Upload** as shown below and select the file *"NO Provisioning and Configuration:"* file backed 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.

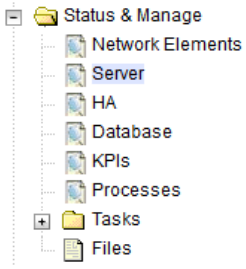
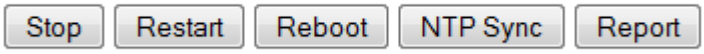
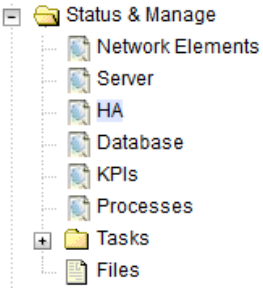
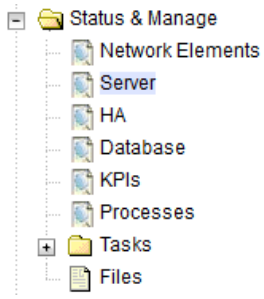
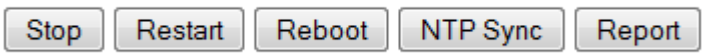
STEP #	Procedure	Description
8. ☐	**NOAM GUI:** Disable Provisioning	Click on **Main Menu->Status & Manage->Database**  Disable Provisioning by clicking on **Disable Provisioning** button at the bottom of the screen as shown below.  A confirmation window will appear, press **OK** to disable Provisioning.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

STEP #	Procedure	Description
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 7** 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 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.

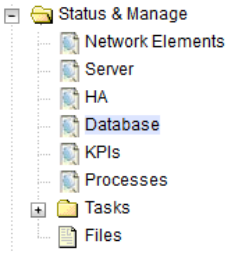
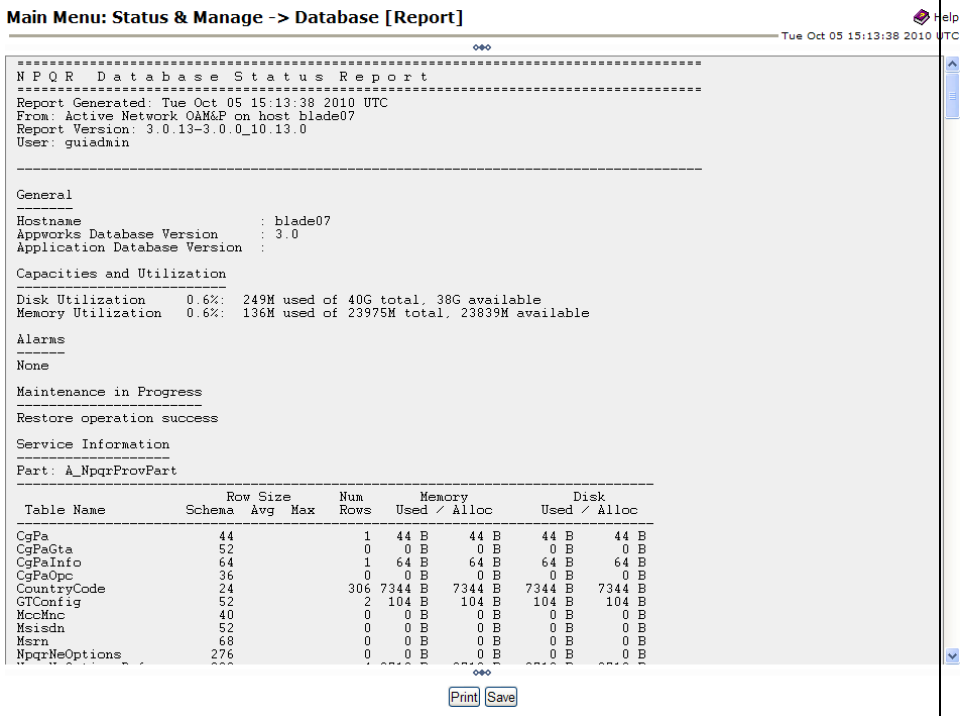
STEP #	Procedure	Description
10. ☐	**ACTIVE NOAM:** Restore the Database	Click on **Main Menu->Status & Manage->Database** Select the **Active NOAM** server, and click on **Restore** as shown below. The following screen will be displayed. Select the proper back up provisioning and configuration file.  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 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.

STEP #	Procedure	Description
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.

STEP #	Procedure	Description
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 15 “Configure the Second NOAM Server” steps 1, 3-7
16. ☐	**NOAM VIP GUI:** Recover Standby NOAM	Navigate to **Main Menu->Status & Manage->Server** and select the second NOAM server.  Click **Restart**.  Click **OK** on the confirmation screen. **Note**: If Topology or nodeId alarms are persistent after the database restore, refer to Workarounds for Issues not fixed in this Release or the next step below.
17. ☐	**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 22 “Configure the SOAM Servers”, steps 1, 3- 7 from reference [1]. **NOTE:** Wait for server to reboot before continuing.

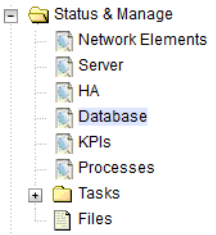
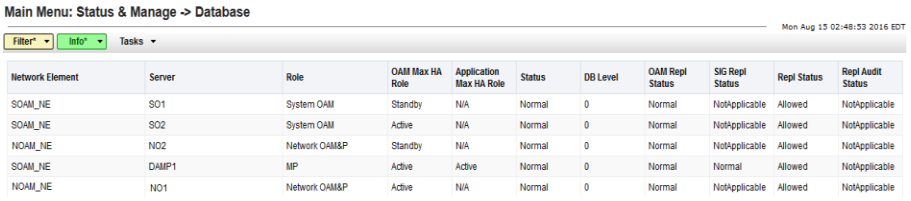
STEP #	Procedure	Description
18. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered server and click on **Restart**. 
19. ☐	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen For each server whose Max Allowed HA Role is not **Active**, set it to **Active** Press **OK**
20. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select each recovered server and click on **Restart**. 

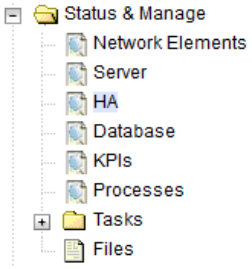
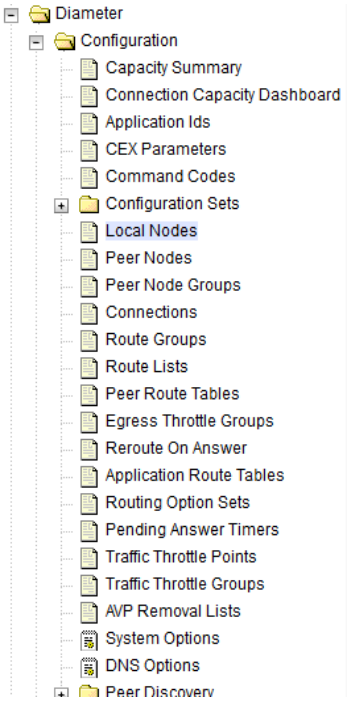
STEP #	Procedure	Description
21. ☐	**ACTIVE NOAM:** Perform key exchange between the active-NOAM and recovered servers.	Establish an SSH session to the Active NOAM, login as ***admusr.*** Execute the following command to perform a keyexchange from the active NOAM to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>` **Note:** If an export server is configured, perform this step.
22. ☐	**ACTIVE NOAM:** Activate Optional Features	Establish an SSH session to the active NOAM, login as ***admusr.*** **Note for PCA Feature Activation:** If you have PCA installed in the system being recovered, execute the procedure "*PCA Activation on Active NOAM server*" on recovered Active NOAM Server and procedure "*PCA Activation on Stand By SOAM server*" on recovered Standby SOAM from [3] to re-activate PCA **Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: *iload#31000{S/W Fault}* **Note**: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature. Refer to **section** 1.5 Optional Features to activate any features that were previously activated.

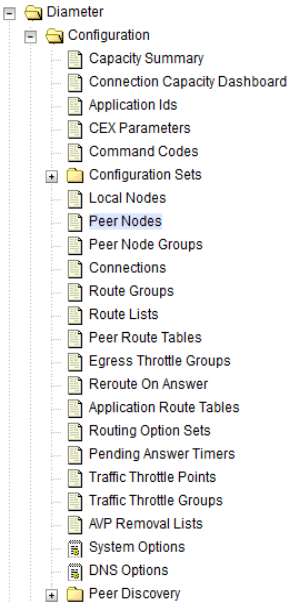
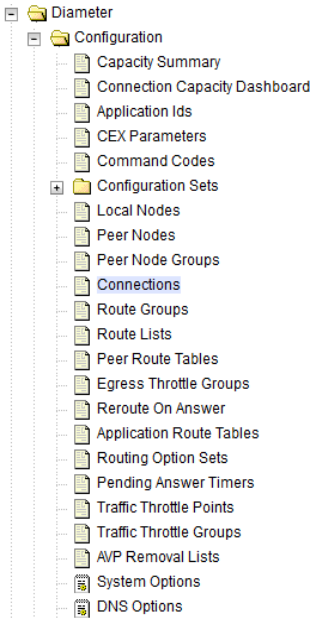
STEP #	Procedure	Description
23. ☐	**NOAM VIP GUI:** Fetch and Store the database Report for the Newly Restored Data and Save it	Navigate to **Main Menu->Status & Manage->Database**  Select the **active** NOAM server and click on the **Report** button at the bottom of the page. The following screen is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

STEP #	Procedure	Description

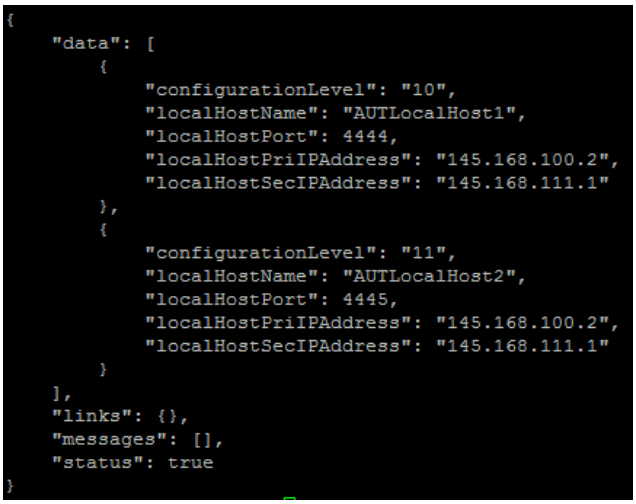
24. ☐	**ACTIVE NOAM:** Verify Replication Between Servers.	Login to the Active NOAM via SSH terminal as ***admusr*** user.
		Execute the following command:
		`$ sudo irepstat –m`
		Output like below shall be generated:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`RDU06-MP1 -- Stby`
		`BC From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

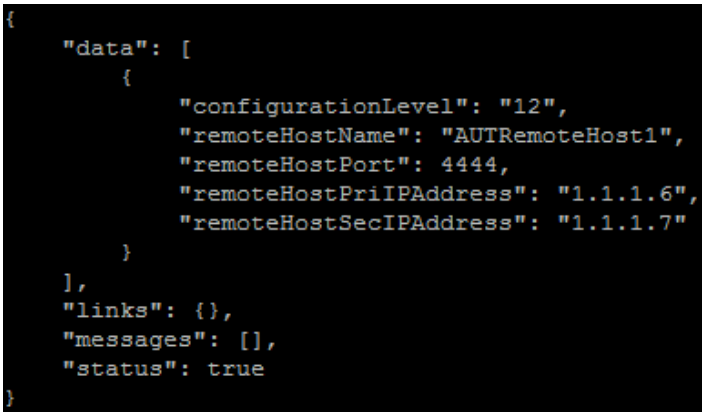
25. ☐	**NOAM VIP GUI:** Verify the Database states	Click on **Main Menu->Status and Manager->Database**  Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below: 

STEP #	Procedure	Description
26. ☐	**NOAM VIP GUI:** Verify the HA Status	Click on **Main Menu->Status and Manage->HA**  Select the row for all of the servers Verify that the “HA Role” is either “Active” or “Standby”. **Main Menu: Status & Manage -> HA** Filter* Hostname / OAM HA Role / Application HA Role / Max Allowed HA Role / Mate Hostname List / Network Element / Server Role SO1 / Standby / N/A / Active / SO2 / SOAM_NE / System OAM SO2 / Active / N/A / Active / SO1 / SOAM_NE / System OAM DAMP1 / Active / Active / Active / / SOAM_NE / MP NO1 / Active / N/A / Active / NO2 / NOAM_NE / Network OAM&P NO2 / Standby / N/A / Active / NO1 / NOAM_NE / Network OAM&P
27. ☐	**SOAM VIP GUI:** Verify the Local Node Info	Navigate to **Main Menu->Diameter->Configuration->Local Node**  Verify that all the local nodes are shown.

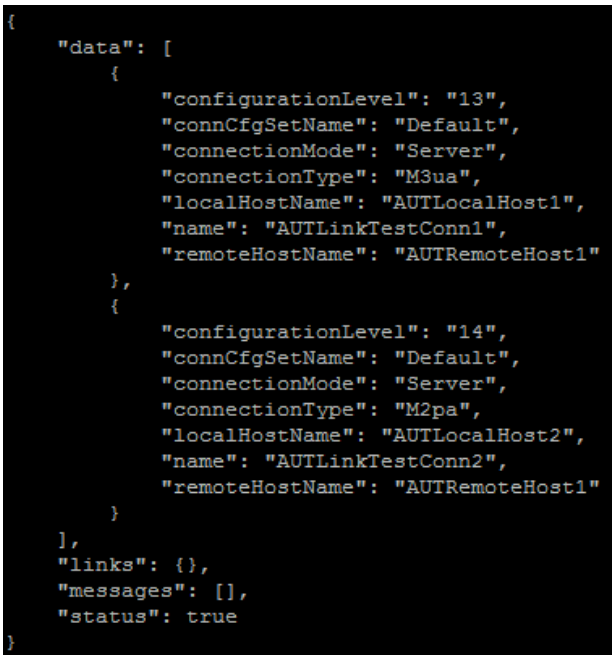
STEP #	Procedure	Description
28. ☐	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.
29. ☐	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections** 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

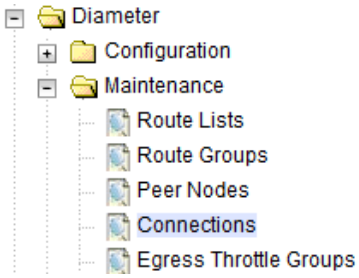
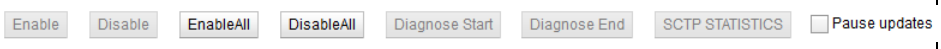
STEP #	Procedure	Description

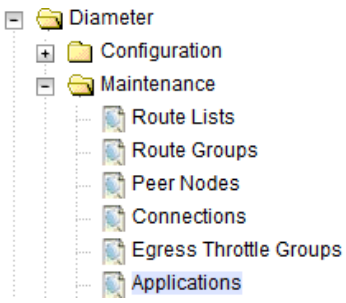
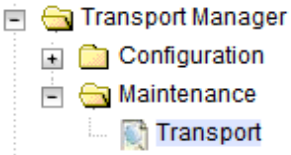
30. ☐	**For vSTP Only- SOAM VIP Server Console (Optional):** Verify the local nodes info	To verify the vSTP MP **Local nodes** info:
		1. Login to the SOAM VIP Server console as **admusr**
		2. Execute the following command
		[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts
		3. Verify the output similar to the below output
		  {
		"data": [
		{
		"configurationLevel": "10",
		"localHostName": "AUTLocalHost1",
		"localHostPort": 4444,
		"localHostPriIPAddress": "145.168.100.2",
		"localHostSecIPAddress": "145.168.111.1"
		},
		{
		"configurationLevel": "11",
		"localHostName": "AUTLocalHost2",
		"localHostPort": 4445,
		"localHostPriIPAddress": "145.168.100.2",
		"localHostSecIPAddress": "145.168.111.1"
		}
		],
		"links": {},
		"messages": [],
		"status": true
		}

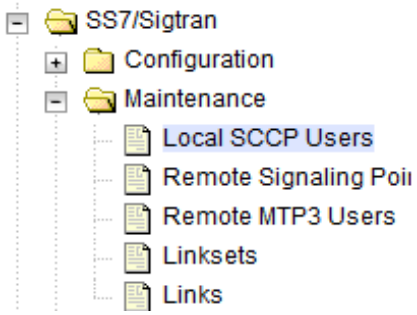
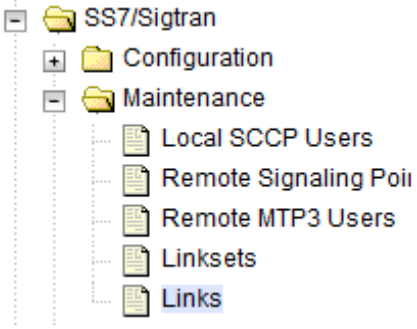
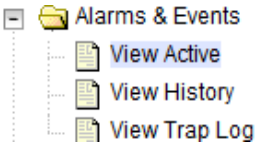
31. ☐	**For vSTP Only- SOAM VIP Server Console (Optional):** Verify the remote nodes info	To verify the vSTP MP **Remote nodes** info:
		1. Login to the SOAM VIP Server console as **admusr**
		2. Execute the following command
		[admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts
		3. Verify the output similar to the below output
		  {
		"data": [
		{
		"configurationLevel": "12",
		"remoteHostName": "AUTRemoteHost1",
		"remoteHostPort": 4444,
		"remoteHostPriIPAddress": "1.1.1.6",
		"remoteHostSecIPAddress": "1.1.1.7"
		}
		],
		"links": {},
		"messages": [],
		"status": true
		}

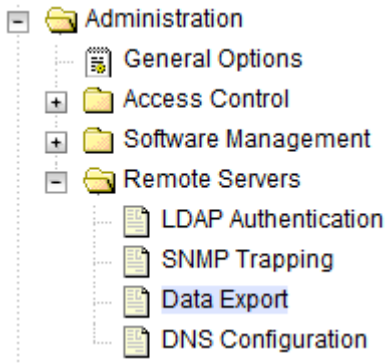
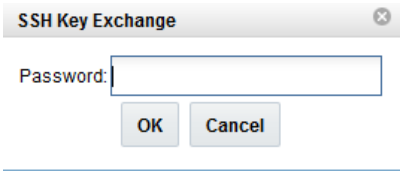
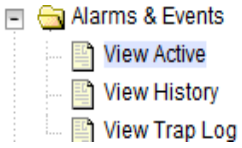
STEP #	Procedure	Description

32. ☐	**For vSTP Only- SOAM VIP Server Console (Optional):** Verify the Connections info	To verify the vSTP MP **Connections** info:
		1. Login to the SOAM VIP Server console as **admusr**
		2. Execute the following command
		[admusr@SOAM1 ~]$ mmiclient.py /vstp/connections
		3. Verify the output similar to the below output
		  {
		"data": [
		{
		"configurationLevel": "13",
		"connCfgSetName": "Default",
		"connectionMode": "Server",
		"connectionType": "M3ua",
		"localHostName": "AUTLocalHost1",
		"name": "AUTLinkTestConn1",
		"remoteHostName": "AUTRemoteHost1"
		},
		{
		"configurationLevel": "14",
		"connCfgSetName": "Default",
		"connectionMode": "Server",
		"connectionType": "M2pa",
		"localHostName": "AUTLocalHost2",
		"name": "AUTLinkTestConn2",
		"remoteHostName": "AUTRemoteHost1"
		}
		],
		"links": {},
		"messages": [],
		"status": true
		}

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.

STEP #	Procedure	Description
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.

STEP #	Procedure	Description
36. ☐	**SOAM VIP GUI:** Re-enable MAPIWF application if needed	Navigate to **Main Menu->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->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 My Oracle Support (MOS)

STEP #	Procedure	Description
39.	**NOAM VIP GUI:** Perform Keyexchange with Export Server	Navigate to **Main Menu -> Administration -> Remote Servers -> Data Export**  Click on **Key Exchange** at the bottom of the screen Enter the Password and press **OK** 
40. ☐	**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 My Oracle Support (MOS).
41. ☐	**Restore GUI Usernames and Passwords**	If applicable, Execute steps in **Section 6.0** to recover the user and group information restored.
42. ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **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.

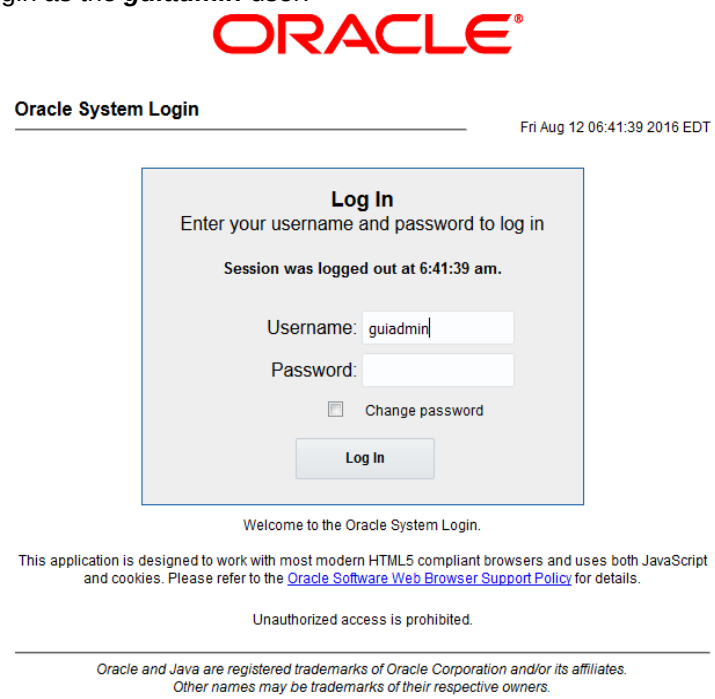
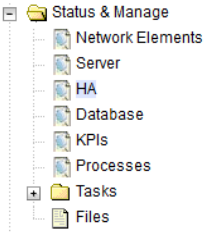
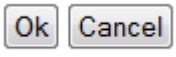
- Recover any failed SO and MP servers by recovering software.
- Recover the software.

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

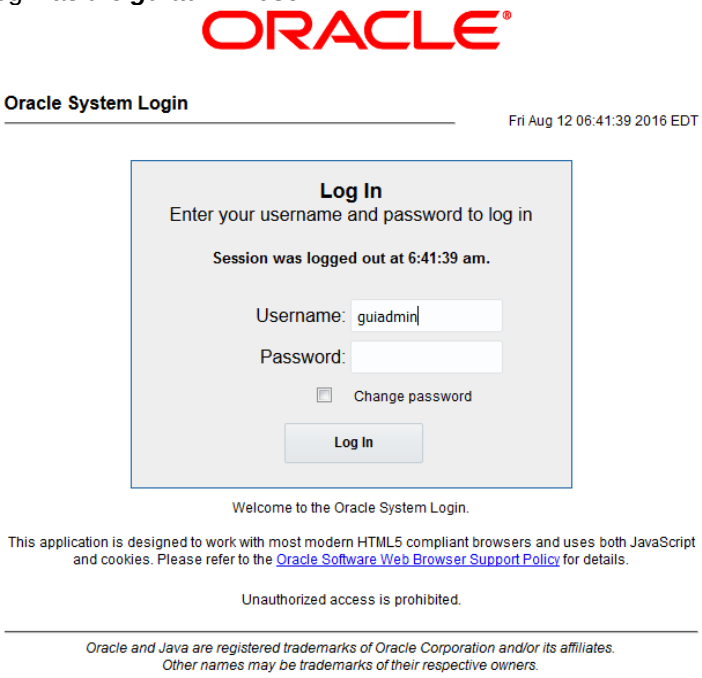
- Re-apply signaling networks configuration if the failed VM is an MP.

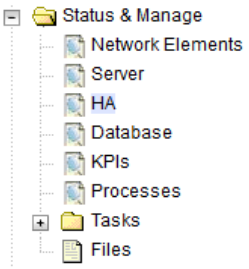
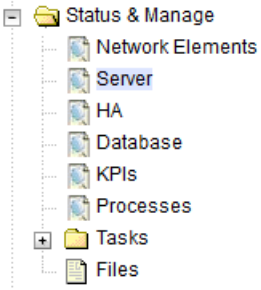
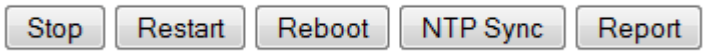
Procedure 8. Recovery Scenario 4

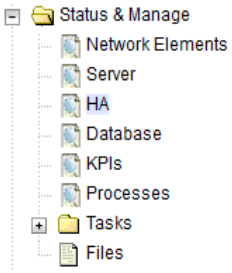
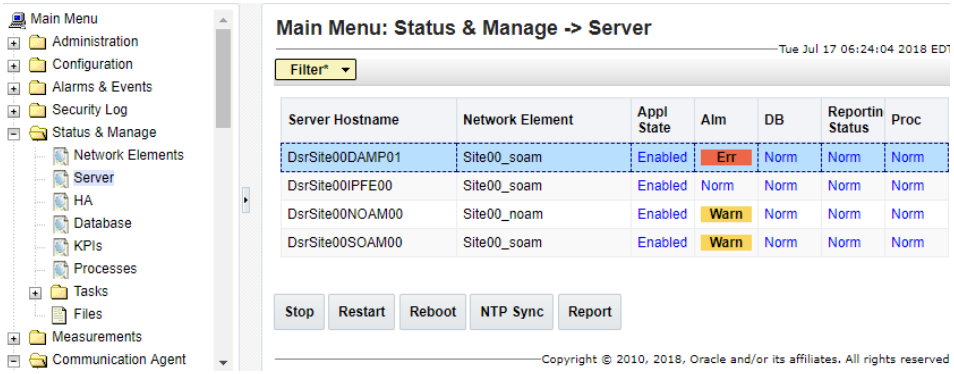
STEP #	Procedure	Description
This procedure performs recovery if at least 1 NOAM server is intact and available and 1 SOAM server is intact and available. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	**Workarounds**	Refer to **Release to** understand/apply any workarounds required during this procedure.
2. ☐	**Gather Required Materials**	Gather the documents and required materials listed in **Section 3.1** Required Materials

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

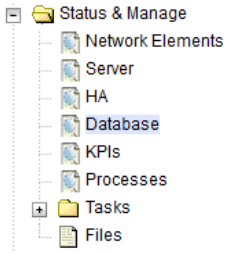
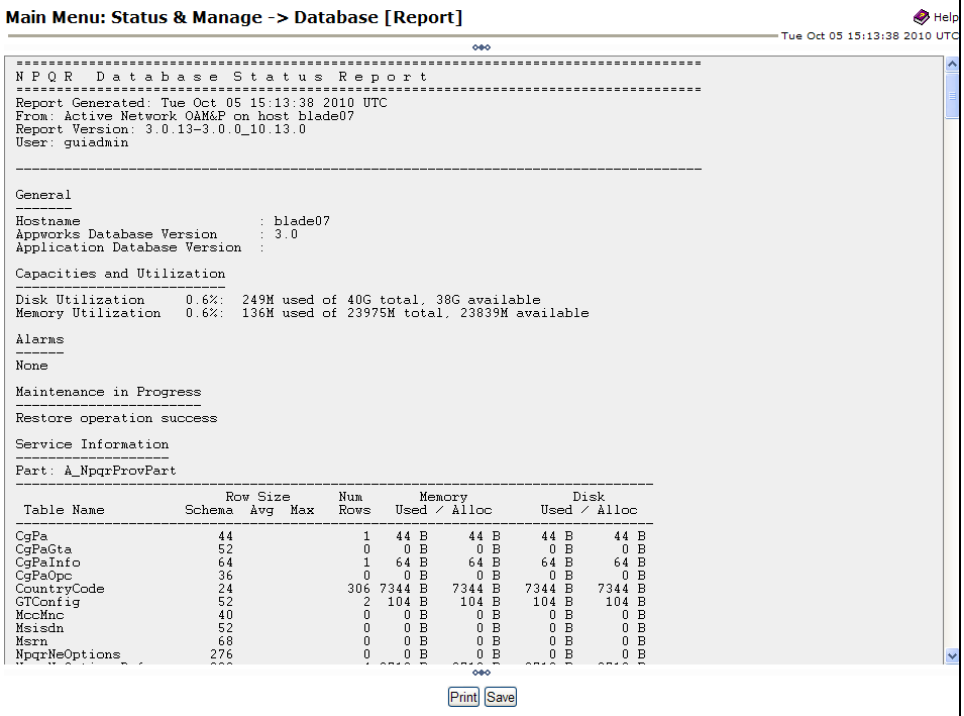
5. ☐	**Recover the Failed Software**	For VMWare based deployments: 1. For NOAMs execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 2 (VMWare Only). Configure NOAM guests based on resource profile 2. For SOAMs execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile 3. For failed MPs execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile For KVM/Openstack based deployments: 1. For NOAMs execute the following procedures from reference [1]: a. Procedure 4 (KVM/Openstack). "Import DSR OVA" [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 5 (KVM/Openstack). "Configure NOAM guests based on resource profile" 2. For SOAMs execute the following procedures from reference [1]: a. Procedure 4 (KVM/Openstack). "Import DSR OVA" [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests based on resource profile" 3. For failed MPs execute the following procedures from reference [1]: a. Procedure 4 (KVM/Openstack). "Import DSR OVA" [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests based on resource profile” For OVM-S/OVM-M based deployments: Execute the following procedures from reference [1]: a. Procedure 7 (OVM-S/OVM-M). Import DSR OVA and prepare for VM creation b. Procedure 8 (OVM-S/OVM-M). Configure each DSR VM

STEP #	Procedure	Description
		Note: While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs)
6. ☐	**Repeat for Remaining Failed Servers**	If necessary, repeat **5** for all remaining failed servers.
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 15 “Configure the Second NOAM Server” steps 1, 3-7 Procedure 16 “Complete Configuring the NOAM Server Group” Step 4 **Note:** If Topology or nodeId alarms are persistent after the database restore, refer to Workarounds for Issues not fixed in this Release, or the next step below.

STEP #	Procedure	Description
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 22 “Configure the SOAM Servers”, steps 1, 3- 7 from reference [1]. **NOTE:** Wait for server to reboot before continuing.
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. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered server and click on **Restart**. 

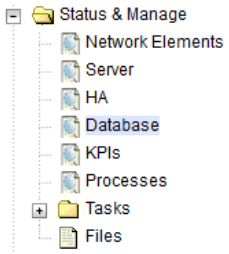
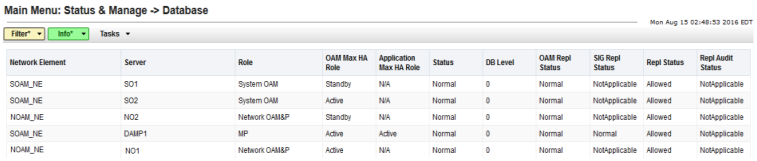
STEP #	Procedure	Description
12. ☐	**NOAM VIP GUI:** Recover the C-Level Server (DA-MP, SBRs, IPFE, vSTP-MP)	Establish a SSH session to the C Level server being recovered, login as ***admusr.*** Execute the following procedures from [1] **FOR EACH** server that has been recovered: Procedure 25 “Configure the MP Virtual Machines”, Steps 1, 8-14 (& 15 if required).
13.	**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**
14. ☐	**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**.
15. ☐	**ACTIVE NOAM:** Login	Login to the recovered Active NOAM via SSH terminal as ***admusr*** user.
16. ☐	**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>`

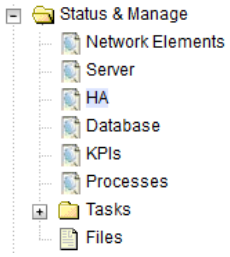
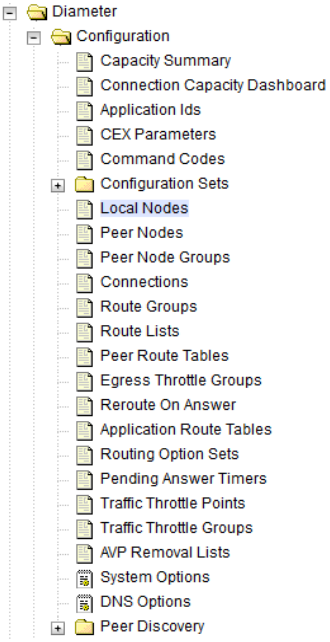
STEP #	Procedure	Description
17. ☐	**ACTIVE NOAM:** Activate Optional Features	Establish an SSH session to the active NOAM, login as ***admusr.*** **Note For PCA Activation:** If you have PCA installed in the system being recovered, execute the procedure "*PCA Activation on Stand By NOAM* server" on recovered StandBy NOAM Server and procedure "*PCA Activation on Stand By SOAM server*" on recovered StandBy SOAM Server from [3] to re-activate PCA Refer to **1.5** Optional Features **to** activate any features that were previously activated. **Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: `iload#31000{S/W Fault}` **Note**: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.

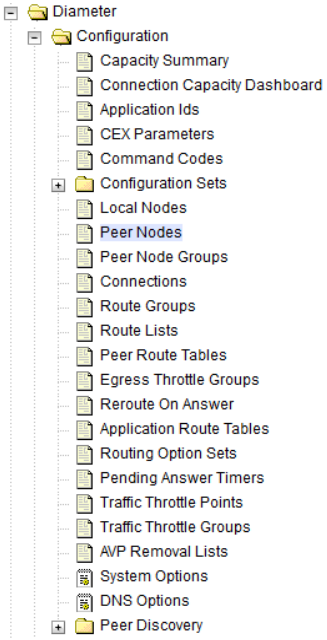
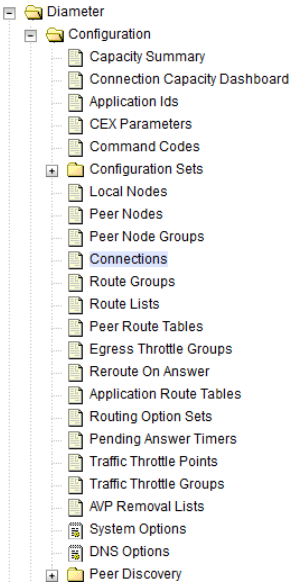
STEP #	Procedure	Description
18. ☐	**NOAM VIP GUI:** Fetch and Store the database Report for the Newly Restored Data and Save it	Navigate to **Main Menu->Status & Manage->Database**  Select the **active** NOAM server and click on the **Report** button at the bottom of the page. The following screen is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

STEP #	Procedure	Description

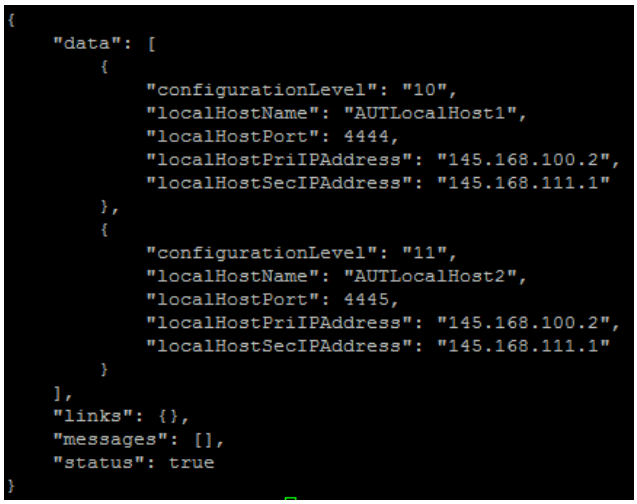
19. ☐	**ACTIVE NOAM:** Verify Replication Between Servers.	Login to the Active NOAM via SSH terminal as ***admusr*** user.
		Execute the following command:
		
		$ sudo irepstat –m
		
		Output like below shall be generated:
		
		`-- Policy 0 ActStb [DbReplication] ----------`
		`RDU06-MP1 -- Stby`
		`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

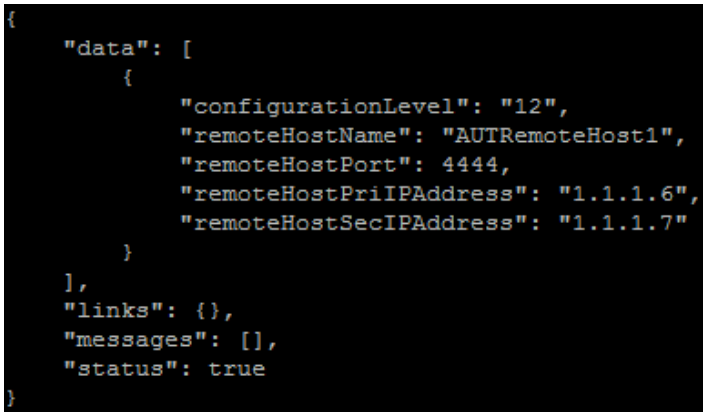
20. ☐	**NOAM VIP GUI:** Verify the Database states	Click on **Main Menu->Status and Manager->Database**  Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below: 

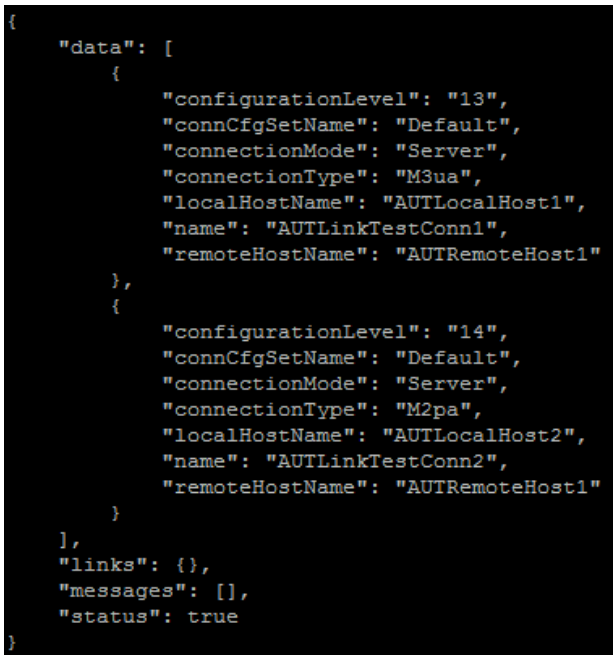
STEP #	Procedure	Description
21. ☐	**NOAM VIP GUI:** Verify the HA Status	Click on **Main Menu->Status and Manage->HA**  Select the row for all of the servers Verify that the “HA Role” is either “Active” or “Standby”. **Main Menu: Status & Manage -> HA** Filter* Hostname / OAM HA Role / Application HA Role / Max Allowed HA Role / Mate Hostname List / Network Element / Server Role SO1 / Standby / N/A / Active / SO2 / SOAM_NE / System OAM SO2 / Active / N/A / Active / SO1 / SOAM_NE / System OAM DAMP1 / Active / Active / Active / / SOAM_NE / MP NO1 / Active / N/A / Active / NO2 / NOAM_NE / Network OAM&P NO2 / Standby / N/A / Active / NO1 / NOAM_NE / Network OAM&P
22. ☐	**SOAM VIP GUI:** Verify the Local Node Info	Navigate to **Main Menu->Diameter->Configuration->Local Node**  Verify that all the local nodes are shown.

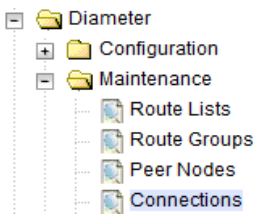
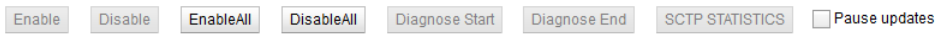
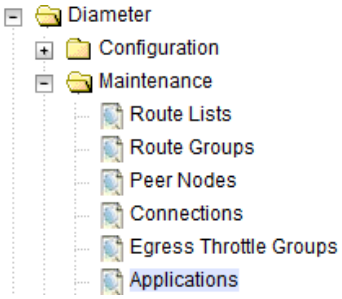
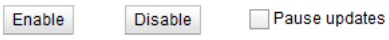
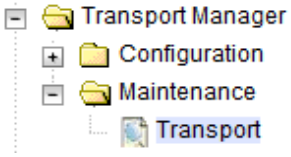
STEP #	Procedure	Description
23. ☐	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.
24. ☐	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections**  Verify that all the connections are shown.

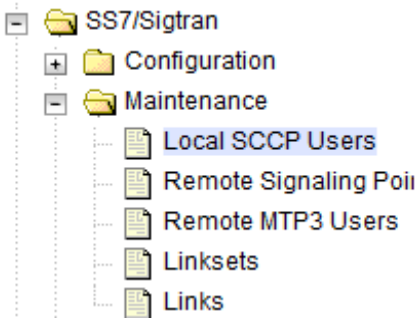
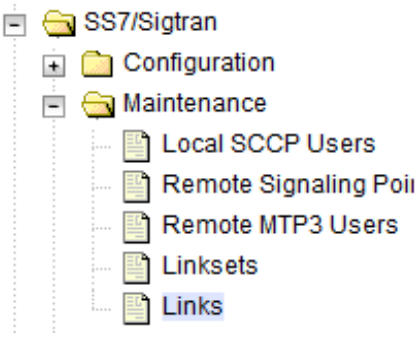
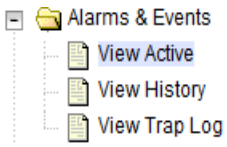
STEP #	Procedure	Description

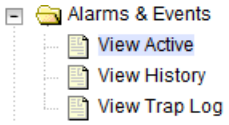
25. ☐	**For vSTP Only-SOAM VIP Server Console (Optional):** Verify the local nodes info	To verify the vSTP MP **Local nodes** info:
		1. Login to the SOAM VIP Server console as **admusr**
		2. Execute the following command
		[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts
		3. Verify the output similar to the below output
		  {
		"data": [
		{
		"configurationLevel": "10",
		"localHostName": "AUTLocalHost1",
		"localHostPort": 4444,
		"localHostPriIPAddress": "145.168.100.2",
		"localHostSecIPAddress": "145.168.111.1"
		},
		{
		"configurationLevel": "11",
		"localHostName": "AUTLocalHost2",
		"localHostPort": 4445,
		"localHostPriIPAddress": "145.168.100.2",
		"localHostSecIPAddress": "145.168.111.1"
		}
		],
		"links": {},
		"messages": [],
		"status": true
		}

26. ☐	**For vSTP Only-SOAM VIP Server Console (Optional):** Verify the remote nodes info	To verify the vSTP MP **Remote nodes** info:
		1. Login to the SOAM VIP Server console as **admusr**
		2. Execute the following command
		[admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts
		3. Verify the output similar to the below output
		  {
		"data": [
		{
		"configurationLevel": "12",
		"remoteHostName": "AUTRemoteHost1",
		"remoteHostPort": 4444,
		"remoteHostPriIPAddress": "1.1.1.6",
		"remoteHostSecIPAddress": "1.1.1.7"
		}
		],
		"links": {},
		"messages": [],
		"status": true
		}

STEP #	Procedure	Description
27. ☐	**For vSTP Only-SOAM VIP Server Console (Optional):** Verify the Connections info	To verify the vSTP MP **Connections** info: 1. Login to the SOAM VIP Server console as **admusr** 2. Execute the following command [admusr@SOAM1 ~]$ mmiclient.py /vstp/connections 3. Verify the output similar to the below output 
28. ☐	**MP Servers:** Disable SCTP Auth Flag	For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [1]. Execute this procedure on all Failed MP Servers.

STEP #	Procedure	Description
29. ☐	**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.
30. ☐	**SOAM VIP GUI:** Enable Optional Features	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Select the optional feature application Click the **Enable** button. 
31. ☐	**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.

STEP #	Procedure	Description
32. ☐	**SOAM VIP GUI:** Re-enable MAPIWF application if needed	Navigate to **Main Menu->Sigtran->Maintenance->Local SCCP Users**  Click on the **Enable** button corresponding to MAPIWF Application Name.  Verify that the SSN Status is Enabled.
33. ☐	**SOAM VIP GUI:** Re-enable links if needed	Navigate to **Main Menu->Sigtran->Maintenance->Links**  Click on **Enable** button for each link.  Verify that the Operational Status for each link is Up.
34. ☐	**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 My Oracle Support (MOS).

STEP #	Procedure	Description
35. ☐	**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 My Oracle Support (MOS).

36. ☐	**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`

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

5.1.5 Recovery Scenario 5 (Partial Server Outage with all NOAM servers failed with DR-NOAM available)

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

Switch DR NOAM from secondary to primary

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

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

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

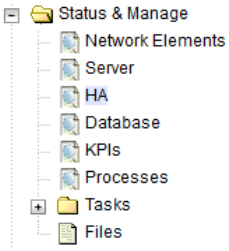
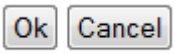
- Recover the base hardware.
- Recover the software.
- The database in intact at the active NOAM server and does not require restoration at the SOAM and MP servers.

Procedure 9. Recovery Scenario 5

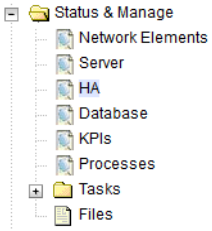
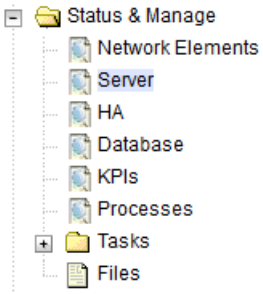
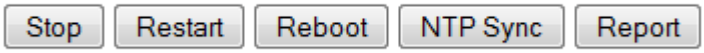
STEP #	Procedure	Description
This procedure performs recovery if both NOAM servers have failed but a DR NOAM is available Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1 ☐	**Workarounds**	Refer to **Workarounds for** Issues not fixed in this Release to understand any workarounds required during this procedure.
2 ☐	**Gather Required Materials**	Gather the documents and required materials listed in **Section 3.1** Required Materials
3 ☐	**Switch DR NOAM to Primary**	Refer to DSR / SDS NOAM Failover User's Guide [2]

4 ☐	**Recover the Failed Software**	For VMWare based deployments: 1. For NOAMs execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 2 (VMWare Only). Configure NOAM guests based on resource profile 2. For SOAMs execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile 3. For failed MPs execute the following procedures from reference [1]: a. Procedure 1 (VMWare). Import DSR OVA [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 3 (VMWare Only). Configure Remaining DSR guests based on resource profile For KVM/Openstack based deployments: 1. For NOAMs execute the following procedures from reference [1]: a. Procedure 4 (KVM/Openstack). "Import DSR OVA" [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 5 (KVM/Openstack). "Configure NOAM guests based on resource profile" 2. For SOAMs execute the following procedures from reference [1]: a. Procedure 4 (KVM/Openstack). "Import DSR OVA" [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests based on resource profile" 3. For failed MPs execute the following procedures from reference [1]: a. Procedure 4 (KVM/Openstack). "Import DSR OVA" [***Note***: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] b. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests based on resource profile" For OVM-S/OVM-M based deployments: Execute the following procedures from reference [1]: a. Procedure 7 (OVM-S/OVM-M). Import DSR OVA and prepare for VM creation

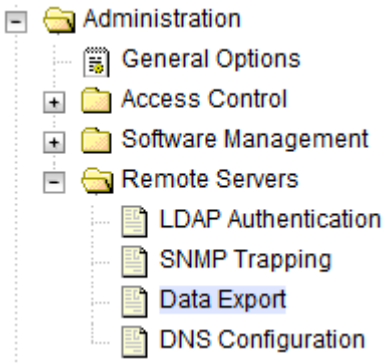
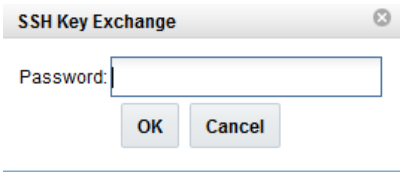
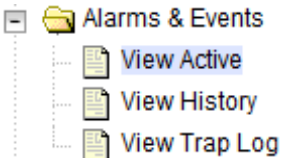
STEP #	Procedure	Description
		b. Procedure 8 (OVM-S/OVM-M). Configure each DSR VM ***Note***: While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs)
5 ☐	**Recover Failed SOAMs**	If **ALL** SOAM servers have failed, execute Procedure 2
6 ☐	**DR-NOAM VIP GUI:** Login	Establish a GUI session on the DR-NOAM server by using the VIP IP address of the DR-NOAM server. Open the web browser and enter a URL of: `http://<Primary_DR-NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

STEP #	Procedure	Description
7 ☐	**DR-NOAM VIP GUI:** Set Failed NOAM 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 NOAM servers. Select **Ok** 
8 ☐	**DR-NOAM VIP GUI:** Export the Initial Configuration	Navigate to **Main Menu -> Configuration -> Servers.** **From the GUI screen, select the Failed NOAM server and then select Export to generate the initial configuration data for that server.** 
9 ☐	**DR-NOAM VIP GUI:** Copy Configuration File to Failed NOAM Server	Obtain a terminal session to the DR-NOAM VIP, login as the ***admusr*** user. Execute the following command to configure the failed NOAM server: `$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<Failed_NOAM_Hostname>.sh admusr@<Failed_NOAM_xmi_IP_address>:/var/tmp/TKLCConfigData.sh`

STEP #	Procedure	Description
10 ☐	**Recovered NOAM Server:** Verify configuration was called and Reboot the Server	Establish an SSH session to the Recovered NOAM server (Recovered_NOAM_xmi_IP_address) Login as the ***admusr*** user. The automatic configuration daemon will look for the file named ***"TKLCConfigData.sh"*** in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server. Verify awpushcfg was called by checking the following file **$ sudo cat /var/TKLC/appw/logs/Process/install.log** Verify the following message is displayed: [SUCCESS] script completed successfully! Now Reboot the Server: **$ sudo init 6** Wait for the server to reboot
11 ☐	**Recovered NOAM Server:** Verify Server Health	Execute the following command on the failed NOAM server and make sure that no errors are returned: **$ sudo syscheck** Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log
12 ☐	**Repeat for Additional 2nd Failed NOAM**	Repeat steps 8-11 for the 2nd failed NOAM server.

STEP #	Procedure	Description
13 ☐	**Perform Key exchange between Active NOAM and Recovered NOAMs**	Perform a keyexchange between the newly active NOAM and the recovered NOAM servers: From a terminal window connection on the active NOAM as the ***admusr*** user, exchange SSH keys for ***admusr*** between the active NOAM and the recovered NOAM servers using the keyexchange utility, using the host names of the recovered NOAMs. When prompted for the password, enter the password for the ***admusr*** user of the recovered NOAM servers. `$ keyexchange admusr@<Recovered_NOAM Hostname>`
14 ☐	**NOAM VIP GUI:** Set HA on Recovered NOAMs	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen For each NOAM server whose Max Allowed HA Role is set to Standby, set it to **Active** Press **OK**
15 ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select each recovered NOAM server and click on **Restart**. 

STEP #	Procedure	Description
16 ☐	**Recovered NOAM servers:** Activate Optional Features	**Map-Diameter Interworking (MAP-IWF) and/or Policy and Charging Application (PCA) Only** Activate the features Map-Diameter Interworking (MAP-IWF) and Policy and Charging Application (PCA) as follows: For **PCA**: 1. Establish SSH sessions to the all the recovered NOAM servers and login as admusr. Refer [3] and execute procedure “PCA Activation on Standby NOAM server” on all recovered NOAM Servers to re-activate PCA. Establish SSH session to the recovered active NOAM, login as ***admusr.*** For **MAP-IWF:** ***1.*** Establish SSH session to the recovered active NOAM, login as ***admusr.*** Refer [4] to activate Map-Diameter Interworking (MAP-IWF) **Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: `iload#31000{S/W Fault}` **Note**: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.
17 ☐	**Switch DR NOAM Back to Secondary**	Once the system have been recovered: Refer to DSR / SDS NOAM Failover User's Guide [2]

STEP #	Procedure	Description
18	**NOAM VIP GUI:** Perform Keyexchange with Export Server	Navigate to **Main Menu -> Administration -> Remote Servers -> Data Export**  Click on **Key Exchange** at the bottom of the screen Enter the Password and press **OK** 
19 ☐	**Recovered Servers:** Verify Alarms	Navigate to **Main Menu -> Alarms & Events -> View Active**  Verify the recovered servers are not contributing to any active alarms (Replication, Topology misconfiguration, database impairments, NTP, etc.)
20 ☐	**NOAM VIP GUI:** Recover Standby/Spare SOAM and C-Level Servers	If necessary, refer to Procedure 3 to recover any standby or Spare SOAMs as well as any C-Level servers.

5.1.6 Recovery Scenario 6 (Database Recovery)

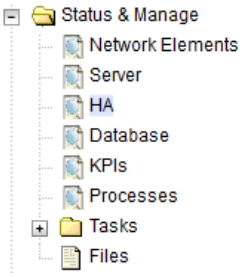
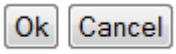
5.1.6.1 Recovery Scenario 6: Case 1

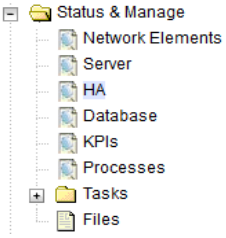
For a partial outage with

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

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

Procedure 10. Recovery Scenario 6 (Case 1)

STEP #	Procedure	Description
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 My Oracle Support (MOS), and ask for assistance.		
1. ☐	**Workarounds**	Refer to **Workarounds for** Issues not fixed in this Release to understand/apply any workarounds required during this procedure.
2.	**NOAM VIP GUI:** Set Failed Servers to OOS	Navigate to **Main Menu -> Status & Manage -> HA**  Select **Edit** Set the Max Allowed HA Role drop down box to **OOS** 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:** Change runlevel to 3	Execute the following command to bring the system to runlevel 3: `$ sudo init 3`

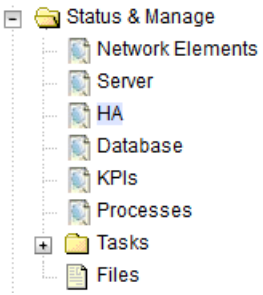
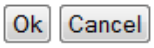
STEP #	Procedure	Description
5. ☐	**Server in Question:** Recover System	Execute the following command and follow the instructions appearing the console prompt: `$ sudo /usr/TKLC/appworks/sbin/backout_restore`
6. ☐	**Server in Question:** Change runlevel to 4	Execute the following command to bring the 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`
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 OOS, set it to **Active** Press **OK**
9. ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **DSR Database** Backup to back up the Configuration databases:

5.1.6.2 Recovery Scenario 6: Case 2

For a partial outage with

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

Procedure 11. Recovery Scenario 6 (Case 2)

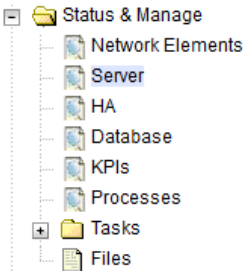
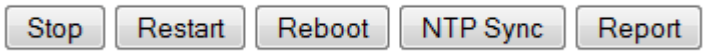
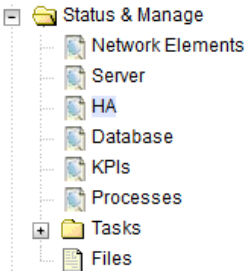
STEP #	Procedure	Description
This procedure performs recovery if database got corrupted in the system and system is in the state to get replicated Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	**Workarounds**	Refer to **Release to** understand/apply any workarounds required during this procedure.
2. ☐	**NOAM VIP GUI:** Set Failed Servers to OOS	Navigate to **Main Menu -> Status & Manage -> HA**  Select **Edit** Set the Max Allowed HA Role drop down box to **OOS** 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`
		`$ sudo 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:
		
		`$ sudo bash -l`
		`$ sudo prod.start`

STEP #	Procedure	Description

6. ☐	**Server in Question:** Verify the Server State	Execute the following commands to verify the processes are up and running:
		`$ sudo pm.getprocs`
		Execute the following command to verify if replication channels are up and running:
		`$ sudo irepstat`
		Execute the following command to verify if merging channels are up and running:
		`$ sudo inetmstat`

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 OOS, set it to **Active** Press **OK**

STEP #	Procedure	Description
9. ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **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

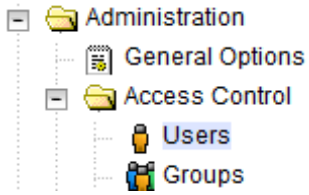
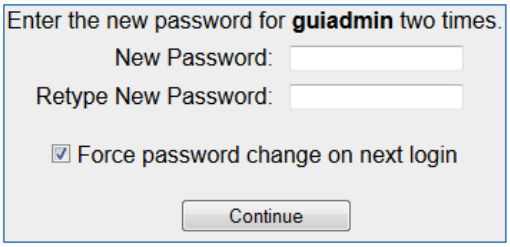
```
- User 'testuser' exists in the selected backup file but not in the current
database.
```

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 12. Keep Restored User

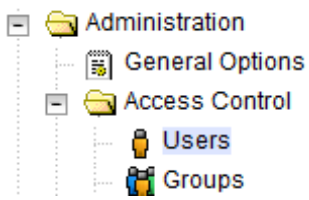
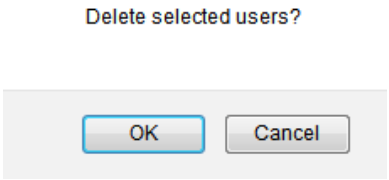
STEP #	Procedure	Description
Perform this procedure to keep users that will be restored by system restoration. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
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: 

STEP #	Procedure	Description
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 13. Remove the Restored User

STEP #	Procedure	Description
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 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: 

STEP #	Procedure	Description
2. ☐	**After Restoration:** Delete user	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 **My Oracle Support (MOS)** for resetting passwords for a user.

6.5 Restoring an Archive that does not contain a Current User

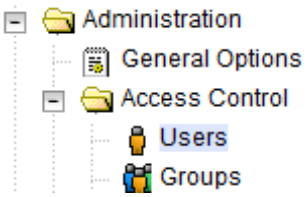
These users have been created after the creation of the backup and archive file. The will be deleted by system restoration of that file.

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

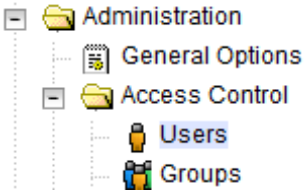
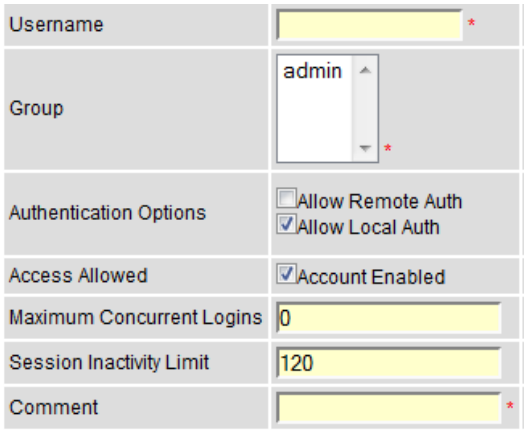
If the user is no longer desired, do not perform any additional steps. The user is permanently removed.

Procedure 14. Restoring an Archive that does not Contain a Current User

STEP #	Procedure	Description
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 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.

STEP #	Procedure	Description
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: 
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

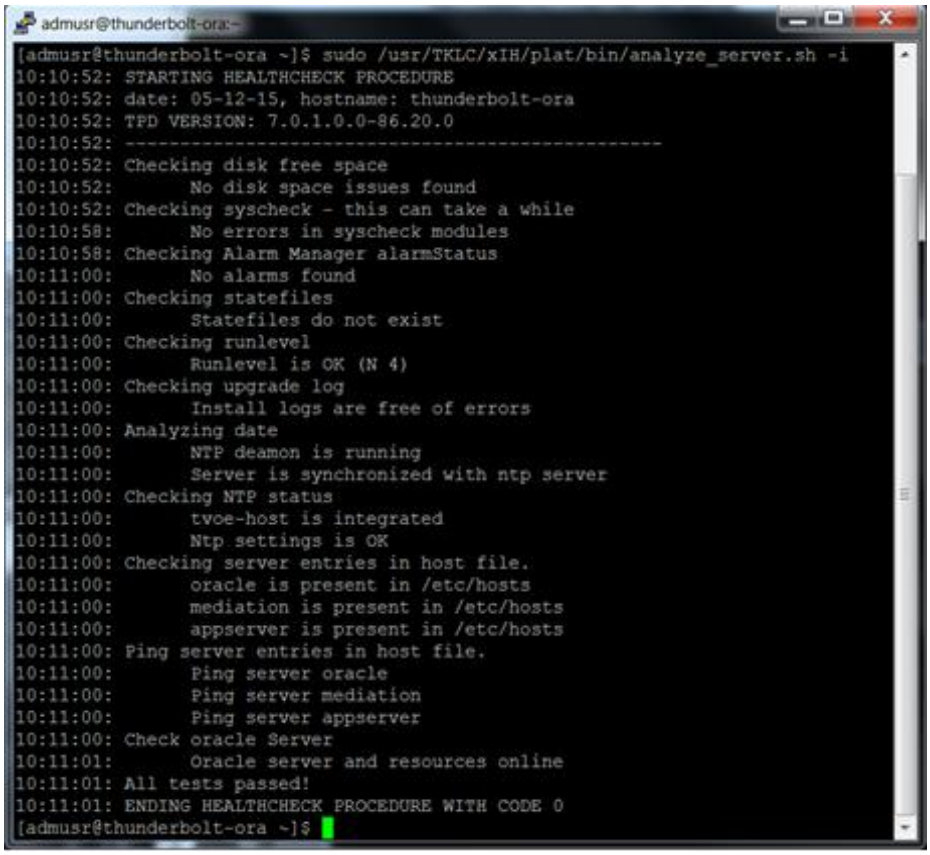
STEP #	Procedure	Description
4. ☐	**After Restoration :** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

STEP #	Procedure	Description
5. ☐	**After Restoration :** Recreate affected user and required group	Navigate to **Administration -> Access Control -> Users**  Click **Insert**  Recreate the user using the data collected in **Step 4.**  Click **Ok** 
6. ☐	**After Restoration :** Repeat for Additional Users	Repeat **Step 5** to recreate additional users and groups.
7. ☐	**After Restoration :** Reset the Passwords	See 6.2 Keeping a Restored user for resetting passwords for a user.

7.0 IDIH Disaster Recovery

Procedure 15. IDIH Disaster Recovery Preparation

STEP #	Procedure	Description
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 My Oracle Support (MOS), and ask for assistance.		
1. ☐	**Oracle Guest:** Login	Establish an SSH session to the Oracle guest, login as ***admusr***.

STEP #	Procedure	Description
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 from reference [1]: For VMware based deployments: Section 5.6 (Procedure 34) : Create iDIH Virtual Machines (VMWare) Section 5.9 (Procedure 37 – 40) : Configure iDIH Virtual Machines For KVM/Openstack based deployments: Section 5.7 (Procedure 35) : Create iDIH Virtual Machines (KVM/Openstack) Section 5.9 (Procedure 37 – 40) : Configure iDIH Virtual Machines For OVM-S/OVM-M based deployments: Section 5.8 (Procedure 36): (OVM-S/OVM-M). Import three IDIH OVA's and create and configure a VM for each Section 5.9 (Procedure 37 – 40) : Configure iDIH Virtual Machines

STEP #	Procedure	Description

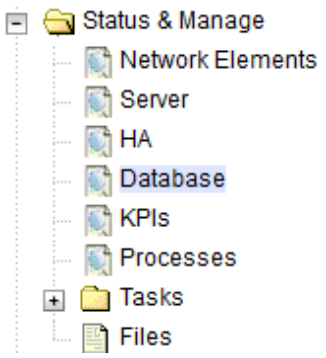
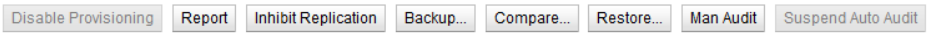
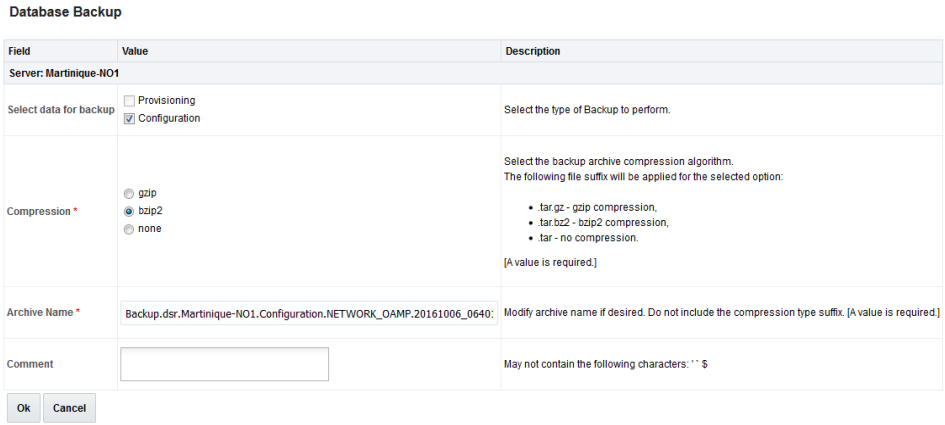
Procedure 16. IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

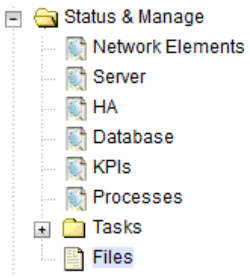
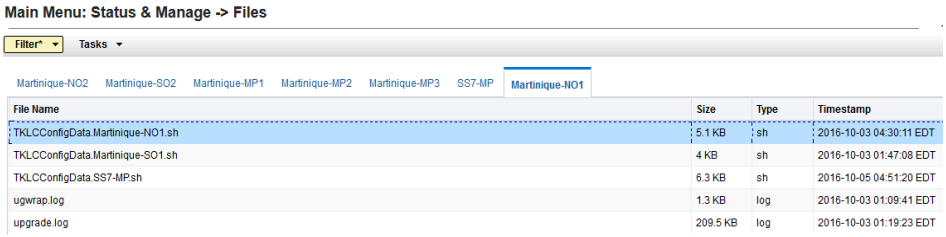
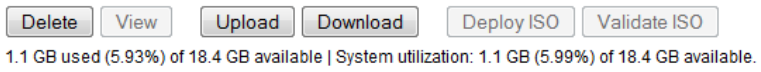
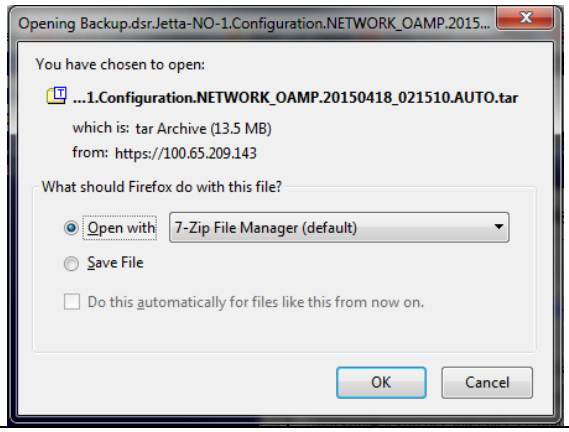
STEP #	Procedure	Description
This procedure performs disaster recovery for the IDIH by re-installing the mediation and application servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (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 34 "(VMware only) Create iDIH Oracle, Mediation and Application VMs" For KVM / Openstack based deployments: Procedure 35. (KVM/OpenStack only) Create iDIH Oracle, Mediation and Application VMs (Optional) For OVM-S / OVM-M based deployments: Procedure 36. (OVM-S/OVM-M). Import three IDIH OVA's and create and configure a VM for each
2. ☐	**Configure iDIH VM Networks**	Execute the following procedure from [1] to configure the VM networks on the Application and Mediation VMs only: Procedure 37 "Configure iDIH VM Networks"
3. ☐	**Configure VMs**	Execute the following procedure from [1]: Procedure 38 "Run Post Installation scripts on iDIH VMs", steps 3 - 7
4. ☐	**Integrate into DSR (Optional)**	If integration is needed execute the following procedure from [1]: Procedure 41 Integrate iDIH into DSR

Appendix A. DSR Database Backup

Procedure 17. Back up the provision and configuration data

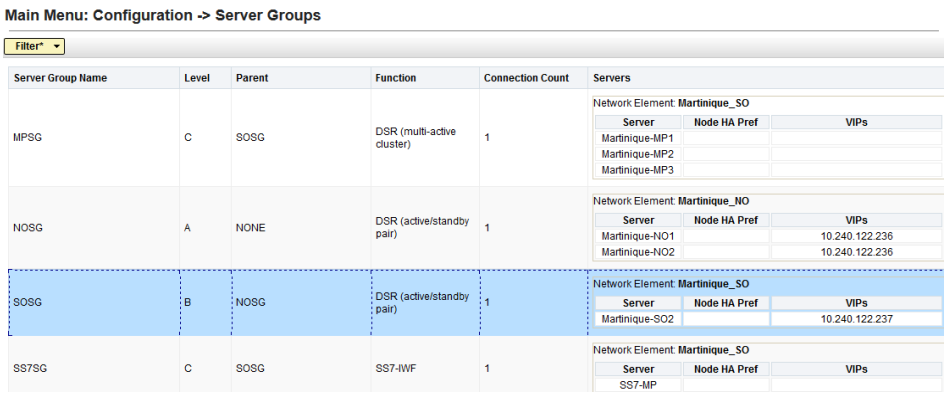
STEP #	Procedure	Description
The intent of this procedure is to back up the provision and configuration information from an NOAM or SOAM server after the disaster recovery is complete Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact 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: 

STEP #	Procedure	Description
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**

STEP #	Procedure	Description
3. ☐	**NOAM/SOAM VIP:** Verify the backup file existence.	Navigate to **Main Menu -> Status & Manage -> Files**   Select the Active NOAM or SOAM tab. The files on this server will be displayed. Verify the existence of the backup file.
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

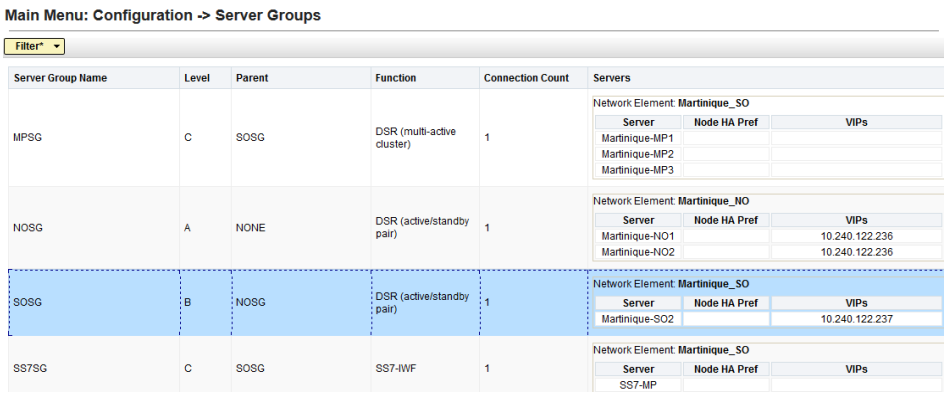
Procedure 18. Inhibit A and B Level Replication on C-Level Servers

STEP #	Procedure	Description
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 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.  Main Menu: Configuration -> Server Groups Filter* Server Group Name / Level / Parent / Function / Connection Count / Servers MPSG — C — SOSG — DSR (multi-active cluster) — 1 — Network Element: Martinique_SO — Server: Martinique-MP1, Martinique-MP2, Martinique-MP3 NOSG — A — NONE — DSR (active/standby pair) — 1 — Network Element: Martinique_NO — Server: Martinique-NO1 (10.240.122.236), Martinique-NO2 (10.240.122.236) SOSG — B — NOSG — DSR (active/standby pair) — 1 — Network Element: Martinique_SO — Server: Martinique-SO2 (10.240.122.237) SS7SG — C — SOSG — SS7-IWF — 1 — Network Element: Martinique_SO — Server: SS7-MP

STEP #	Procedure	Description
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 19. Un-Inhibit A and B Level Replication on C-Level Servers

STEP #	Procedure	Description
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 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. 

3. ☐	**Active NOAM:** Verify Replication has been un-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 empty 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. Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)

Procedure 20. Inhibit A and B Level Replication on C-Level Servers

STEP #	Procedure	Description
The intent of this procedure is to inhibit A and B level replication on all C Level servers of this site **when Active, Standby and Spare SOAMS are lost** Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS)		
1. ☐	**Active NOAM:** Login	Login to the Active NOAM server via SSH as ***admusr*** user.

STEP #	Procedure	Description

2. ☐	**Active NOAM:** Inhibit replication on all C level Servers	Execute the script from /usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh, if available.
		
		/usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh --replication=inhibit --SO_SG_Name=<SOAM server group name>
		
		If script doesn't exist then please use below manual command.
		
		Alternate to above script (if above mentioned script is not present in the specific path):
		
		`$ for i in $(sudo Imysql.client -B -N -e "`
		`SELECT DISTINCT CS.hostname`
		`  FROM appworks.Server CS, appworks.Server PS,`
		`appworks.Server2SG C2SG, appworks.Server2SG P2SG,`
		`appworks.ServerGroup CSG, appworks.ServerGroup PSG,`
		`comcol.ClusterInfo CCI, comcol.ClusterInfo PCI,`
		`comcol.ClusterGroupInfo`
		`  WHERE CS._h_Server_ID = C2SG._h_Server_ID`
		`  AND C2SG._h_SG_ID = CSG._h_SG_ID`
		`  AND CSG.clusterId = CCI.clusterId`
		`  AND CCI.groups = comcol.ClusterGroupInfo.groupId`
		`  AND comcol.ClusterGroupInfo.parentGroup = PCI.groups`
		`  AND PCI.clusterId = PSG.clusterId`
		`  AND PSG.ServerGroupName='<SOAM_SG_NAME>'`
		`"); do iset -finhibitRepPlans='A B' NodeInfo where`
		`"nodeName='$i'"; done`
		
		Note: SOAM_SG_NE name of the Server Group 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.
		
		 
		DRNO_SG A NONE DSR (active/standby pair) 1
		Network Element: DSR_DR_NO_NE
		Server / Node HA Pref / VIPs
		DRNOAM1
		DRNOAM2
		NO_SG A NONE DSR (active/standby pair) 1
		Network Element: DSR_NO_NE
		Server / Node HA Pref / VIPs
		NOAM1
		NOAM2
		SO_SG B NO_SG DSR (active/standby pair) 1
		Network Element: DSR_SO_NE
		Server / Node HA Pref / VIPs
		SOAM1
		SOAM2

STEP #	Procedure	Description
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 server group e.g. Server group SO_SG 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 E. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)

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

STEP #	Procedure	Description
The intent of this procedure is to Un-inhibit A and B level replication on all C Level servers of this site **when Active, Standby and Spare SOAMS are lost.** Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	**Active NOAM:** Login	Login to the Active NOAM server via SSH as ***admusr*** user.

STEP #	Procedure	Description
2. ☐	**Active NOAM:** Un-Inhibit replication on all C level Servers	Execute the script from /usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh, if available. /usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh --replication=allow --SO_SG_Name=<SOAM server group name> If script doesn't exist then please use below manual command. Alternate to above script (if above mentioned script is not present in the specific path): **$ for i in $(sudo Imysql.client -B -N -e "** **SELECT DISTINCT CS.hostname** **FROM appworks.Server CS, appworks.Server PS, appworks.Server2SG C2SG, appworks.Server2SG P2SG, appworks.ServerGroup CSG, appworks.ServerGroup PSG, comcol.ClusterInfo CCI, comcol.ClusterInfo PCI, comcol.ClusterGroupInfo** **WHERE CS._h_Server_ID = C2SG._h_Server_ID** **AND C2SG._h_SG_ID = CSG._h_SG_ID** **AND CSG.clusterId = CCI.clusterId** **AND CCI.groups = comcol.ClusterGroupInfo.groupId** **AND comcol.ClusterGroupInfo.parentGroup = PCI.groups** **AND PCI.clusterId = PSG.clusterId** **AND PSG.ServerGroupName='<SOAM_SG_NAME>'** **"); do iset -finhibitRepPlans='' NodeInfo where "nodeName='$i'"; done** **Note: SOAM_SG_NAME** 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. 

STEP #	Procedure	Description
3. ☐	**Active NOAM:** Verify Replication has been un-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 server group e.g. Server group SO_SG shall be set as ' ': 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 F. Workarounds for Issues not fixed in this Release

Procedure 22. Backup directory

STEP #	Procedure	Description
This procedure will provide the steps to check and create backup directory. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	**NOAM/SOAM VIP console**: Determine if backup directory is created	Execute following command on console of Active NOAM/SOAM server (accessed via the VIP) and compare the output: **$ cd /var/TKLC/db/filemgmt/** **$ ls -ltr** Look for backup directory in the output. Check if directory is already created with correct permission. Directory will look like:- drwxrwx--- 2 awadmin awadm 4096 Dec 19 02:15 backup In case, directory is already there with right permissions then skip steps 2 and 3. If directory is not with right permissions then execute step 3. Otherwise go to next step.
2. ☐	**NOAM/SOAM VIP console:** Create backup directory	Assuming present working directory is **/var/TKLC/db/filemgmt/** Otherwise, do **cd /var/TKLC/db/filemgmt/** #Create backup directory $mkdir backup **Verify directory is created:-** **$ ls -ltr /var/TKLC/db/filemgmt/backup** Error should not come "No such file or directory". Rather it will show the directory, as directory will be empty it will show total 0 as content.

STEP #	Procedure	Description
3. □	**NOAM/SOAM VIP console:** Change permissions of backup directory	Assuming backup directory is created **Verify directory is created:-** **$ ls -ltr /var/TKLC/db/filemgmt/backup** Error should not come "No such file or directory". Rather it will show the directory, as directory will be empty it will show total 0 as content. If directory is not created go back to step 2. Else proceed. #Change permissions of backup directory **$ chmod 770 /var/TKLC/db/filemgmt/backup** #Change ownership of backup directory **$ sudo chown -R awadmin:awadm /var/TKLC/db/filemgmt/backup** After changing the permissions and ownership of the backup directory. **Directory will look like** **drwxrwx--- 2 awadmin awadm 4096 Dec 22 02:15 backup**
4.	**NOAM/SOAM VIP console:** Copy the backup file which we need to restore in backup directory	Copy the backup file to backup directory $ **cp BACKUPFILE /var/TKLC/db/filemgmt/backup** Provide permissions to backup file inside backup directory. # Make sure about present working directory. $cd **/var/TKLC/db/filemgmt/backup** #Change permissions of files inside backup directory $chmod 666 Backup.* # Change ownership of files inside backup directory $ **sudo chown -R awadmin:awadm** Backup.*

Appendix G. 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, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request
2. Select 3 for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), Select 1.
   - For Non-technical issues such as registration or assistance with MOS, Select 2.

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, and 365 days a year.

Appendix H. Emergency Response

In the event of a critical service situation, emergency response is offered by the CAS main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Appendix I. Locate Product Documentation on the Oracle Help Center

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the **Oracle Help Center** site at http://docs.oracle.com.
1. Click Industries.
2. Under the **Oracle Communications** subheading, click the **Oracle Communications documentation** link. The Communications Documentation page appears. Most products covered by these documentation sets display under the headings **Network Session Delivery and Control Infrastructure** or "**Platforms**."
3. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release displays. To download a file to your location, right-click the PDF link, select `Save target as` (or similar command based on your browser), and save to a local folder.