Oracle® Communications

Diameter Signaling Router

DSR Cloud Disaster Recovery Guide

Release 8.3

E93228-01

November 2018

ORACLE

Oracle Communications Diameter Signaling Router Cloud Disaster Recovery Guide, Release 8.3

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

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html.

See more information on My Oracle Support (MOS) in Appendix G.

Table of Contents

List of Tables

List of Figures

List of Procedures

1. Introduction

This document describes the 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.

1.1 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

1.2 Acronyms

An alphabetized list of acronyms used in the document.

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

Acronym	Definition
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

1.3 Terminology

Multiple server types may be involved with the procedures in this manual. Therefore, most steps in the written procedures begin with the name or type of server to which the step applies.

Table 2. Terminology

Term	Definition
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.

1.4 How to Use This Document

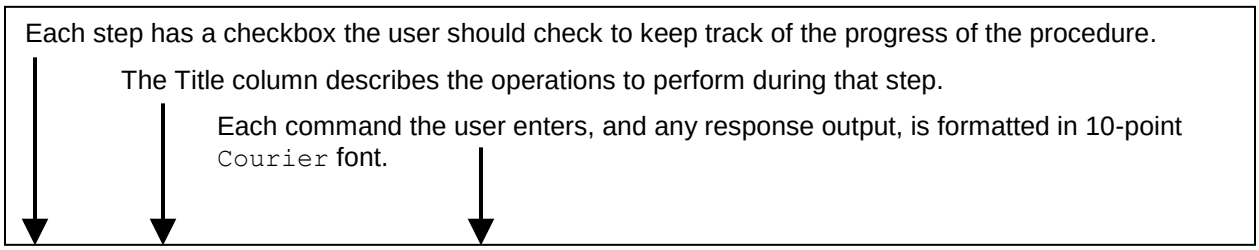
Although this document is primarily to be used as an initial installation guide, its secondary purpose is as a reference for disaster recovery procedures. When executing this document for either purpose, there are a few points to help ensure you understand this document's intent. These points are:

1. Before beginning a procedure, completely read the instructional text (it will appear immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.
2. Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.

If a procedural STEP fails to execute successfully, STOP and contact Oracle's Customer Service for assistance before attempting to continue. See Appendix G, for information on contacting Oracle Customer Support.

Figure 1 shows an example of a procedural step used in this document.

- Any sub-steps within a step are referred to as step X.Y. The example in Figure 1 shows steps 1 through 3, and step 3.1.
- GUI menu items, action links, and buttons to be clicked on are in bold Arial font.
- GUI fields and values to take note of during a step are in bold Arial font.
- Where it is necessary to explicitly identify the server on which a particular step is to be taken, the server name is given in the title box for the step (for example, “ServerX” in step 2 Figure 1).



	Title	Directive/Result Step
1. ☐	Change directory	Change to the backout directory. `$ cd /var/TKLC/backout`
2. ☐	ServerX: Connect to the console of the server	Establish a connection to the server using cu on the terminal server/console. `$ cu -l /dev/ttyS7`
3. ☐	Verify Network Element data	1. View the Network Elements configuration data; verify the data; save and print report. 2. Select **Configuration > Network Elements** to view Network Elements Configuration screen.

Figure 1. Example of a Procedure Steps Used in This Document

1.5 Optional Features

Further configuration and/or installation steps will need to be taken for optional features that may be present in this deployment. Please refer to these documents for disaster recovery steps needed for their components

Table 3. Optional Features

Feature	Document
Diameter Mediation	DSR Meta Administration Feature Activation Procedure
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. 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:

Table 4. Recovery Scenarios

Procedure	State of NOAM and/or SOAM Server(s)
Recovery of the entire network from a total outage • 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 • 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 • 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. • 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 • 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. • Recovery Scenario 6 (Database Recovery)	• Server having a corrupted database

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 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.

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 and then restoring database backups to the active NOAM and SOAM servers.

Database backups are taken from customer offsite backup storage locations (assuming these were performed and stored offsite before 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. The database is restored on the SOAM server and replication recovers 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

The database is restored on the NOAM and replication recovers 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 recovers 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 a partial outage with both NOAM servers failed but a DR NOAM available. The DR NOAM is switched from secondary to primary and 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 a Comcol upgrade barrier), and the database backup is available.

Case 2: Database is corrupted but replication channel is active.

3. Procedure Overview

This section lists the materials required to perform disaster recovery procedures and a general overview (disaster recovery strategy) of the procedures.

3.1 Required Materials

These 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.
2. Read and review the content in this document.
3. Gather required materials in section Required Materials.
4. From the failure conditions, determine the Recovery Scenario and procedure to follow (using Figure 2.).
5. Execute appropriate recovery procedures (listed in section 4).

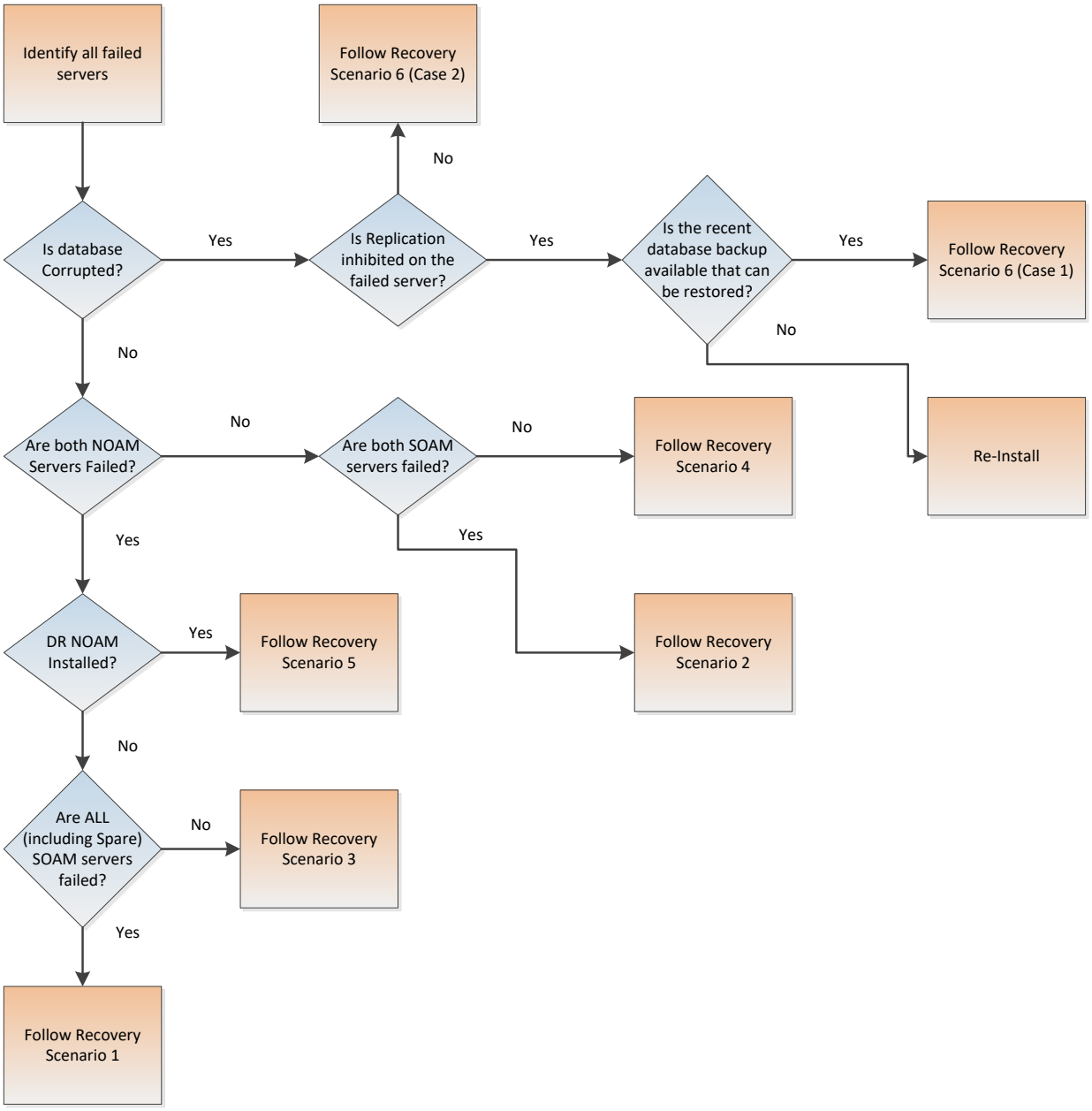


Figure 2. Determining Recovery Scenario

4. Disaster Recovery Procedure

Call My Oracle Support (MOS) before 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!!

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.

4.1 Recovering and Restoring System Configuration

Disaster recovery requires configuring the system as it was before the disaster and restoration of operational information. There are eight distinct procedures to select from depending on the type of recovery needed. Only one of these scenarios should be followed, not all.

!!WARNING!!

When there is a need to restore the database backup for NOAM and SOAM servers in any of the recovery scenarios described in the following sections, the backup directory may not be there in the system since the system is DRed. In this case, refer to Workarounds for Issues Not Fixed in this Release for steps to check and create the backup directory.

File format for recovery is when the backup was taken. Generally, the backup file is in the following format.

Backup.DSR.HPC02-NO2.FullDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2

4.1.1 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 vase 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.

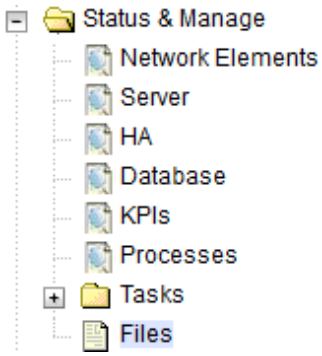
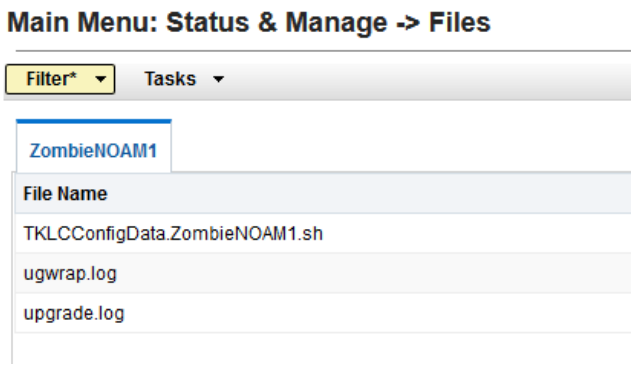
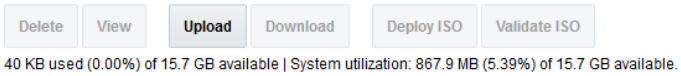
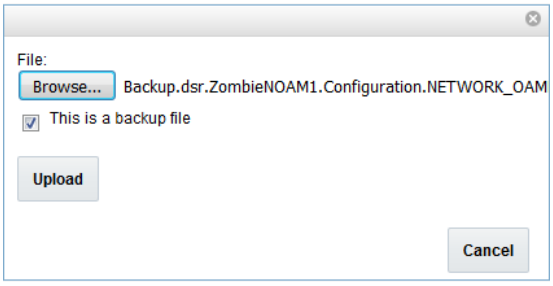
Note: Any other applications DR recovery actions (SDS and IDIH) may occur in parallel. These actions can/should be worked simultaneously; doing so would allow faster recovery of the complete solution, that is, stale DB on DP servers do not receive updates until SDS-SOAM servers are recovered.

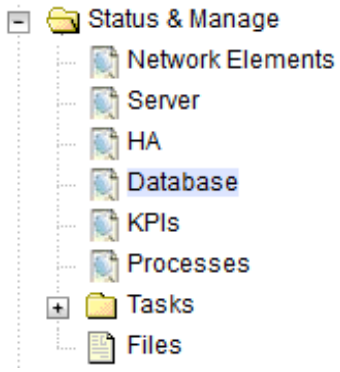
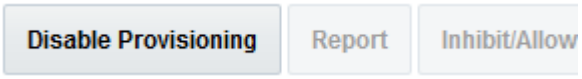
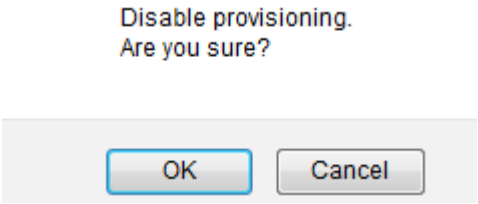
Procedure 1. Recovery Scenario 1		
This procedure performs recovery if both NOAM servers are failed and all SOAM servers are failed. This procedure also covers the C-level server failure. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If 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 the Required Materials section.

Procedure 1. Recovery Scenario 1		
3. ☐	Recover the failed software	For VMWare based deployments: • 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 the procedure to import OVA. b. Procedure 2 **(VMWare Only) Configure NOAM Guests Based on Resource Profile**. • For SOAMs or 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 the procedure to import OVA. b. Procedure 3 **(VMWare Only) Configure Remaining DSR Guests Based on Resource Profile**. For KVM/Openstack based deployments: • 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 the procedure to import OVA. b. Procedure 5 (**KVM/Openstack Only) Configure NOAM Guests Based on Resource Profile**. • For SOAMs or 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 the procedure to import 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]: 1. Procedure 7 **(OVM-S/OVM-M) Import DSR OVA and Prepare for VM Creation**. 2. 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 (for example, file servers) or tape backup sources. From required materials list in the Required Materials section; use site survey documents and network element report (if available), to determine network configuration data.

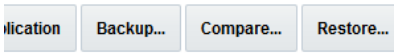
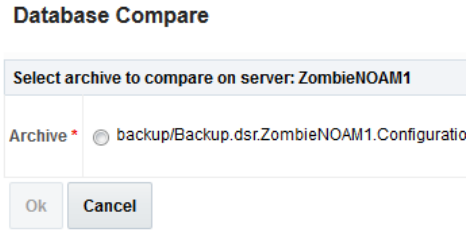
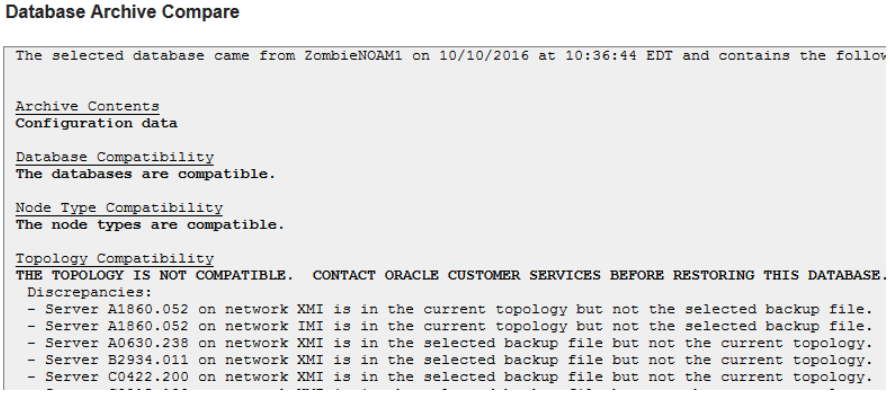
Procedure 1. Recovery Scenario 1		
5. ☐	Execute DSR installation procedure for the first NOAM	Verify the networking data for network elements. ***Note:*** Use the backup copy of network configuration data and site surveys (step 2.). Execute installation procedures for the first NOAM server from reference [1]: 1. Procedure 13 **Configure the First NOAM NE and Server**. 2. Procedure 14 **Configure the NOAM Server Group**.
6. ☐	**NOAM GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 

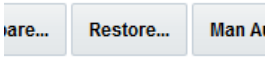
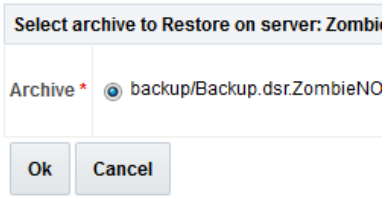
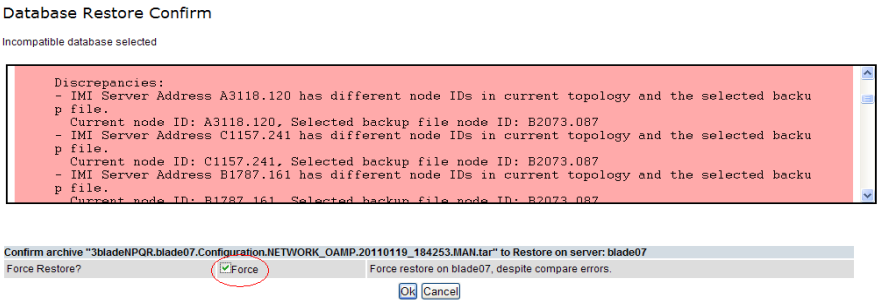
Procedure 1. Recovery Scenario 1

7. ☐	**NOAM GUI**: Upload the backed up database file	1. Navigate to **Status and Manage > Files**.  2. Select the active NOAM server.  3. Click **Upload** and select the **NO Provisioning and Configuration** file backed up after initial installation and provisioning.  4. Click **Browse** and locate the backup file. 5. Mark the **This is a backup file** checkbox. 6. Click **Upload**.  The file takes a few seconds to upload depending on the size of the backup data. The file is visible on the list of entries after the upload is complete.

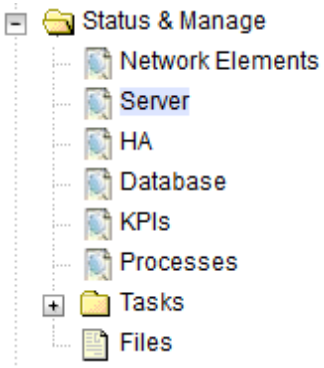
Procedure 1. Recovery Scenario 1		
8. ☐	**NOAM GUI**: Disable provisioning	1. Navigate to **Status and Manage > Database**.  2. Click **Disable Provisioning**.  3. Click **OK** on the confirmation screen to disable provisioning. 

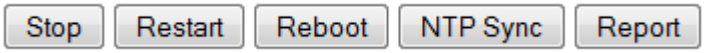
Procedure 1. Recovery Scenario 1

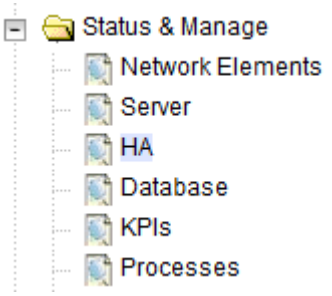
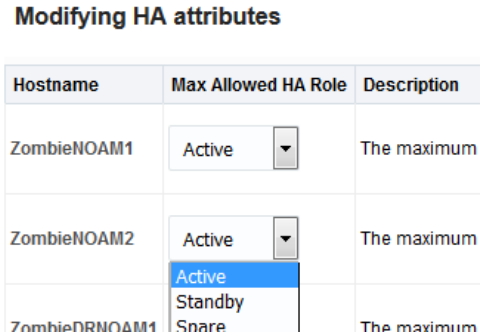
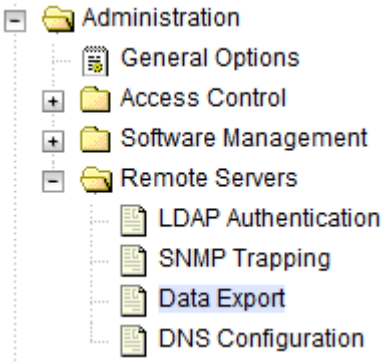
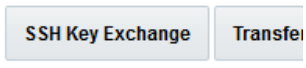
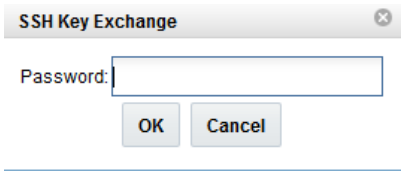
9. ☐	**NOAM GUI**: Verify the archive contents and database compatibility	1. Select the active NOAM server and click **Compare**.  2. Click the button for the restored database file uploaded as a part of step 7. of this procedure.  3. Verify the output window matches the screen below. ***Note:*** A database mismatch regarding the NodeIDs of the VMs displays. That is expected. If that is the only mismatch, proceed; otherwise, stop and contact My Oracle Support (MOS).  ***Notes***: • Archive Contents and Database Compatibilities must be the following: **Archive Contents**: Configuration data. **Database Compatibility**: The databases are compatible. • The following is expected output for the Topology Compatibility Check since we are restoring from an existing backed up database to a database with just one NOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. • We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility. 4. If the verification is successful, click **Back** and continue to the next step.

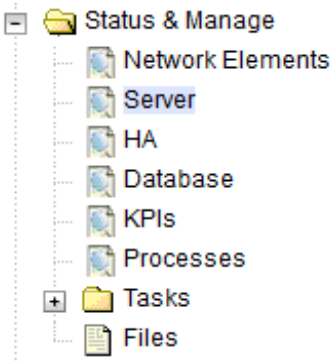
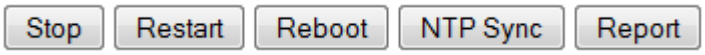
Procedure 1. Recovery Scenario 1		
10. ☐	**Active NOAM**: Restore the database	1. From **Status and Manage > Database**. 2. Select the active NOAM server and click **Restore**.  3. Select the backup provisioning and configuration file.  4. Click **OK**. ***Note:*** A database mismatch regarding the NodeIDs of the VMs displays. That is expected. If that is the only mismatch, proceed; otherwise, stop and contact My Oracle Support (MOS). 5. Mark the **Force** checkbox and click **OK** to proceed with the database restore.  After the restore has started, the user is logged out of the XMI NOAM GUI since the restored topology is old data.

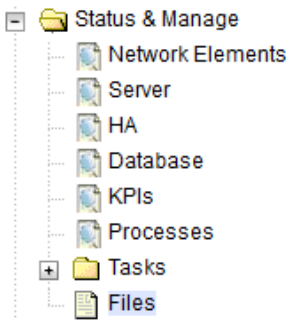
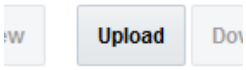
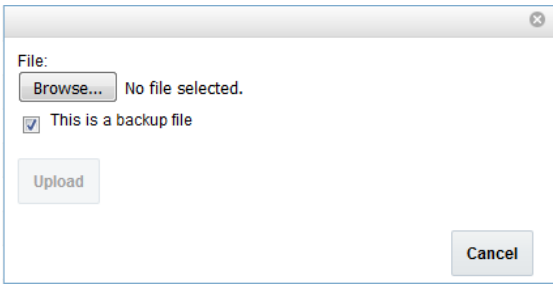
Procedure 1. Recovery Scenario 1		
11. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 
12. ☐	**NOAM VIP GUI**: Monitor and confirm database restoral	1. Wait for 5-10 minutes for the system to stabilize with the new topology. 2. Monitor the Info tab for Success. This indicates the restore is complete and the system is stabilized. Ignore these alarms 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). ***Notes***: • Do not pay attention to alarms until all the servers in the system are completely restored. • The Configuration and Maintenance information will be in the same state it was backed up during initial backup.
13. ☐	**Active NOAM**: Login	Log into the recovered active NOAM with the SSH terminal as **admusr**.

<table>
<tr><th colspan="3">Procedure 1. Recovery Scenario 1</th></tr>
<tr><td>14. ☐</td><td>NOAM VIP GUI: Recover standby NOAM</td><td>Install the second NOAM server by executing procedures from reference [1]:
1. Procedure 15 Configure the Second NOAM Server, steps 1, 3-7.
2. Procedure 16 Complete Configuring the NOAM Server Group, step 4.</td></tr>
<tr><td>15. ☐</td><td>Active NOAM: Correct the Recognized Authority table</td><td>1. Establish an SSH session to the active NOAM and login as admusr.
2. Execute this command:
<pre>$ sudo top.setPrimary
- Using my cluster: A1789
- New Primary Timestamp: 11/09/15 20:21:43.418
- Updating A1789.022: <DSR_NOAM_B_hostname>
- Updating A1789.144: <DSR_NOAM_A_hostname></pre></td></tr>
<tr><td>16. ☐</td><td>NOAM VIP GUI: Restart DSR application</td><td>1. Navigate to Status and Manage > Server.
 

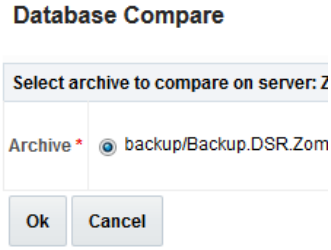
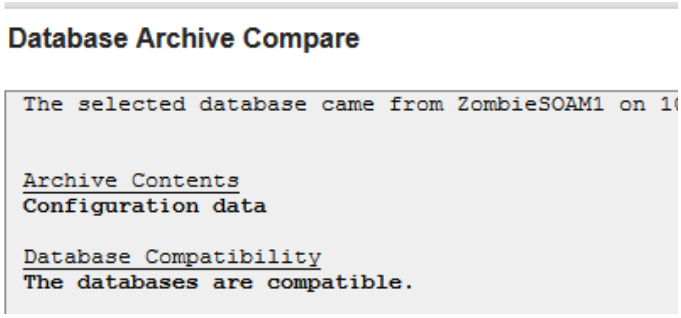
2. Select the recovered standby NOAM server and click Restart.
 
</td></tr>
</table>

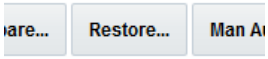
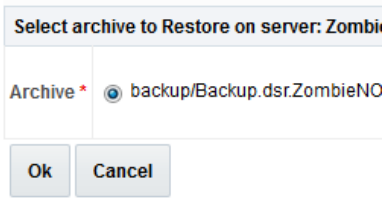
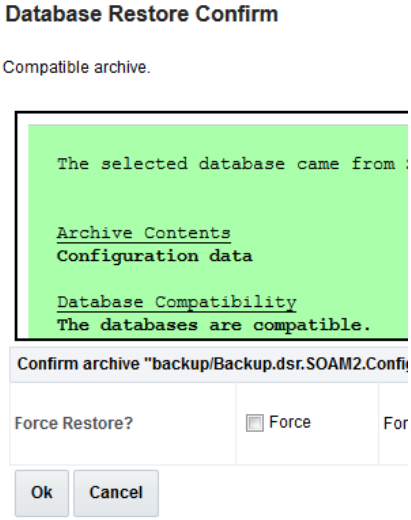
Procedure 1. Recovery Scenario 1		
17. ☐	**NOAM VIP GUI**: Set HA on standby NOAM	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Select the standby NOAM server and set it to **Active**.  4. Click **OK**.
18. ☐	**NOAM VIP GUI**: Perform key exchange with export server	1. Navigate to **Administration > Remote Servers > Data Export**.  2. Click **SSH Key Exchange** at the bottom of the screen.  3. Type the **Password** and click **OK**. 

Procedure 1. Recovery Scenario 1		
19. ☐	**NOAM VIP GUI**: Stop replication to the C-level servers of this site 	**!!Warning!!** Inhibit replication to the working C-level servers that belong to the same site as the failed SOAM servers since recovery of the active SOAM causes the database wipeout in the C level servers because of the replication. **If the spare SOAM is also present in the site and lost**, execute Appendix D Inhibit A and B Level Replication on C-Level Servers (When Active, Standby, and Spare SOAMs are Lost) to inhibit replication to working C-level servers before continuing. **If the spare SOAM is NOT deployed in the site**, execute Appendix B Inhibit A and B Level Replication on C-Level Servers to inhibit replication to working C-level servers before continuing.
20. ☐	**NOAM VIP GUI**: Recover active SOAM server	Install the SOAM servers by executing procedure 22 **Configure the SOAM Servers**, steps 1, 3-6, from reference [1]. ***Note:*** Wait for server to reboot before continuing.
21. ☐	**NOAM VIP GUI**: Restart DSR application on recovered active SOAM server	1. Navigate to **Status and Manage > Server**.  2. Select the recovered server and click **Restart**. 

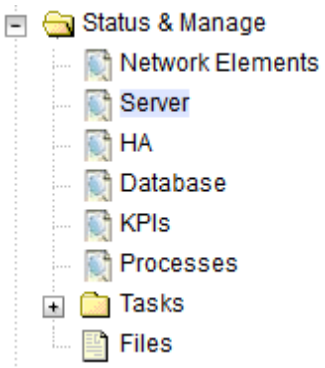
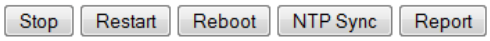
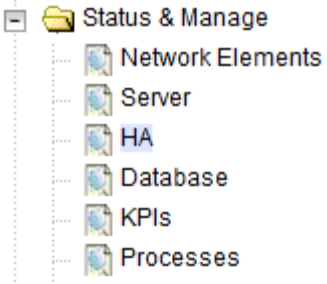
Procedure 1. Recovery Scenario 1		
22. ☐	**NOAM VIP GUI**: Upload the backed up SOAM database file	1. Navigate to **Status and Manage > Files**.  2. Select the active SOAM server. 3. Click **Upload** and select the **SO Provisioning and Configuration** file backed up after initial installation and provisioning.  4. Click **Browse** and locate the backup file. 5. Mark the **This is a backup file** checkbox. 6. Click **Upload**.  The file takes a few seconds to upload depending on the size of the backup data. The file is visible on the list of entries after the upload is complete.

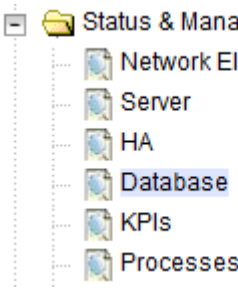
Procedure 1. Recovery Scenario 1		
23. ☐	**Recovered SOAM GUI**: Login	1. Establish a GUI session on the recovered SOAM server. 2. Open the web browser and enter a URL of: `http://<Recovered_SOAM_IP_Address>` 3. Login as the **guiadmin** user: 

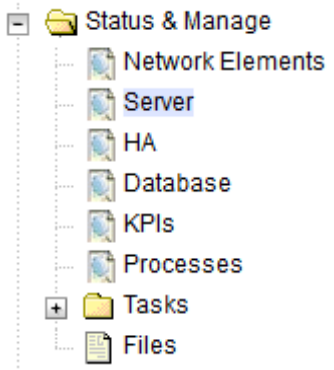
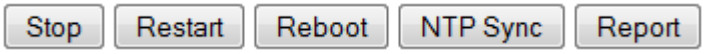
Procedure 1. Recovery Scenario 1		
24. ☐	**Recovered SOAM GUI**: Verify the archive contents and database compatibility	1. Navigate to **Status and Manage > Database**. 2. Select the active SOAM server and click **Compare**.  3. Click the button for the restored database file that was uploaded as a part of step 7. of this procedure.  4. Verify the output window matches the screen below. ***Note:*** A database mismatch regarding the NodeIDs of the VMs displays. That is expected. If that is the only mismatch, proceed; otherwise, stop and contact My Oracle Support (MOS).  ***Notes***: • Archive Contents and Database Compatibilities must be the following: **Archive Contents**: Configuration data. **Database Compatibility**: The databases are compatible. • The following is expected output for the Topology Compatibility Check since we are restoring from an existing backed up database to a database with just one SOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. • We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility. 5. If the verification is successful, click **Back** and continue to the next step.

Procedure 1. Recovery Scenario 1		
25. ☐	**Recovered SOAM GUI**: Restore the database	1. Navigate to **Status and Manage > Database**. 2. Select the active SOAM server and click **Restore**.  3. Select the backup provisioning and configuration file.  4. Click **OK**. ***Note:*** A database mismatch regarding the NodeIDs of the VMs displays. That is expected. If that is the only mismatch, proceed; otherwise, stop and contact My Oracle Support (MOS). 5. Mark the **Force** checkbox and click **OK** to proceed with the database restore.  After the restore has started, the user is logged out of the XMI SOAM GUI since the restored topology is old data.
26. ☐	**Recovered SOAM GUI**: Monitor and confirm database restoral	1. Wait for 5-10 minutes for the system to stabilize with the new topology. 2. Monitor the Info tab for **Success**. This indicates the backup is complete and the system is stabilized. ***Notes***: • Do not pay attention to alarms until all the servers in the system are completely restored. • The Configuration and Maintenance information is in the same state it was when backed up during the initial backup.

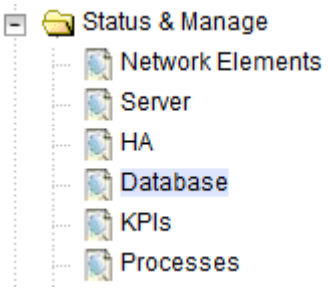
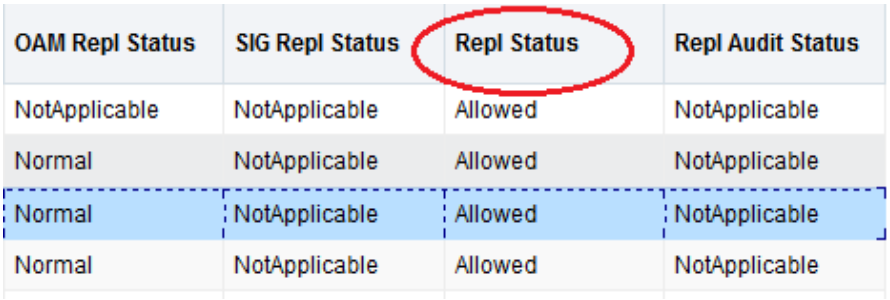
Procedure 1. Recovery Scenario 1		
27. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 
28. ☐	**NOAM VIP GUI**: Recover remaining SOAM server	Install the SOAM servers by executing procedure 22 **Configure the SOAM Servers**, steps 1, 3-6, from reference [1]. ***Note:*** Wait for server to reboot before continuing.

Procedure 1. Recovery Scenario 1		
29. ☐	**NOAM VIP GUI**: Restart DSR application on remaining SOAM server(s)	1. Navigate to **Status and Manage > Server**.  2. Select the recovered server and click **Restart**. 
30. ☐	**NOAM VIP GUI**: Set HA on recovered standby SOAM server	***Note:*** For non-HA sites, **skip** this step. 1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Set the Max Allowed HA Role to **Active**. 4. Click **OK**.

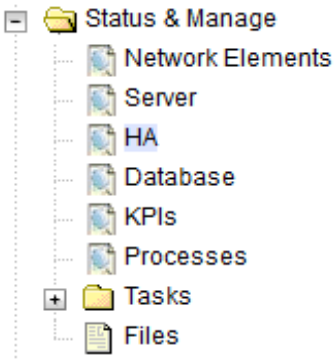
Procedure 1. Recovery Scenario 1		
31. ☐	**NOAM VIP GUI**: Start replication on working C-level servers	Un-inhibit (start) replication to the **working** C-level servers that belong to the same site as of the failed SOAM servers. **If the spare SOAM is also present in the site and lost**, execute Appendix E Un-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 Appendix C Un-Inhibit A and B Level Replication on C-Level Servers. 1. Navigate to **Status and Manage > Database**.  2. If the **Repl Status** is set to **Inhibited**, click **Allow Replication** using this order; otherwise, if none of the servers are inhibited, skip this step and continue with the next step: • Active NOAM server • Standby NOAM server • Active SOAM server • Standby SOAM server • Spare SOAM server, if applicable • Active DR NOAM server • Standby DR NOAM server • MP/IPFE servers • SBRs (if SBR servers are configured, start with the active SBR, then standby, then spare) 3. Verify the replication on all the working servers is allowed. This can be done by checking the **Repl Status** column. **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

Procedure 1. Recovery Scenario 1		
32. ☐	**NOAM VIP GUI**: Recover the C-level servers (DA-MP, SBRs, IPFE, vSTP-MP)	1. Establish an SSH session to the C-level server being recovered and login as **admusr**. 2. Execute this command to set shared memory to unlimited: `$ sudo shl.set -m 0` 3. Execute the procedure 25 **Configure the MP Virtual Machines**, steps 1, 8-14 (and 15, if required), from [1] for **EACH** server that has been recovered.
33. ☐	**NOAM VIP GUI**: Restart DSR application for recovered C-level server	1. Navigate to **Status and Manage > Server**.  2. Select the recovered server and click **Restart**. 

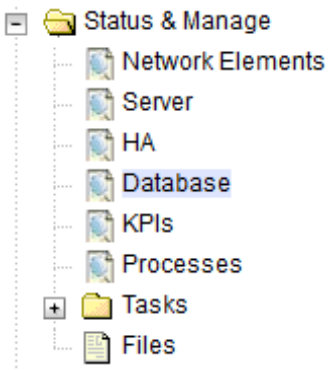
Procedure 1. Recovery Scenario 1

34. ☐	**NOAM VIP GUI**: Start replication on ALL C-level servers	Un-Inhibit (Start) Replication to the **ALL** C-level servers. 1. Navigate to **Status and Manage > Database**.  2. If the **Repl Status** is set to **Inhibited**, click **Allow Replication** using this order: • Active NOAMP server • Standby NOAMP server • Active SOAM server • Standby SOAM server • Spare SOAM server (if applicable) • Active DR NOAM server • Standby DR NOAM Server • MP/IPFE servers (if MPs are configured as active/standby, start with the Active MP; otherwise, the order of the MPs does not matter). 3. Verify the replication on all servers is allowed. This can be done by checking the **Repl Status** column. 

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

Procedure 1. Recovery Scenario 1		
35. ☐	**NOAM VIP GUI**: Set HA on all C-level servers	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. For each server whose Max Allowed HA Role is set to OOS, set it to **Active**. 4. Click **OK**.
36. ☐	**Active NOAM**: Perform key exchange between the active NOAM and recovered servers	1. Establish an SSH session to the active NOAM and login as **admusr**. 2. 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.
37. ☐	**Active NOAM**: Activate optional features	Establish an SSH session to the active NOAM and login as **admusr**. **Note for PCA Feature Activation:** If you have PCA installed in the system being recovered, re-activate the PCA by executing **PCA Activation on Standby NOAM server** on the recovered standby NOAM server, and **PCA Activation on Active SOAM Server** on the recovered active SOAM server from [3]. Refer to section 1.5 Optional Features to activate any features that were previously activated. ***Notes***: • While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored: `iload#31000{S/W Fault}` • If any of the MPs are failed and recovered, then these MP servers should be restarted after activation of the feature.

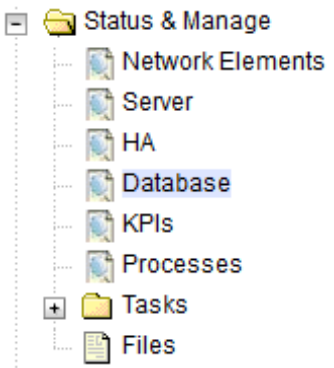
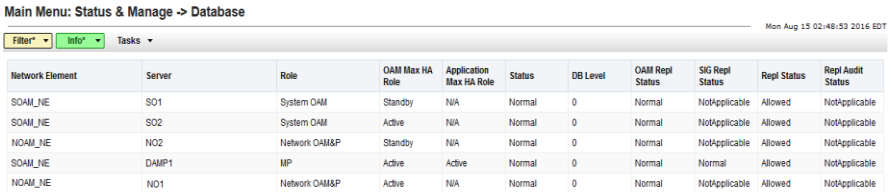
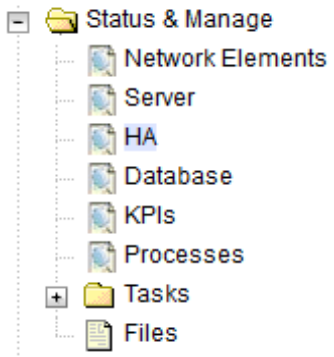
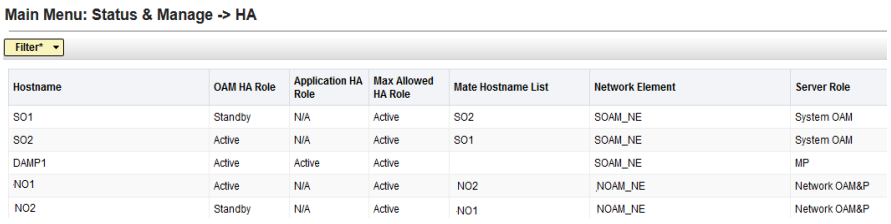
Procedure 1. Recovery Scenario 1		

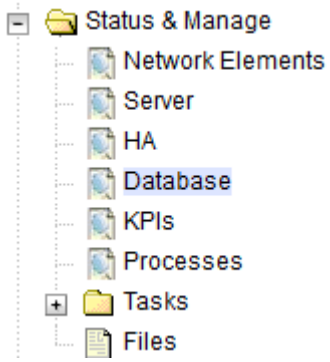
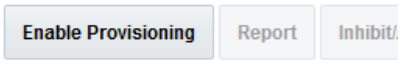
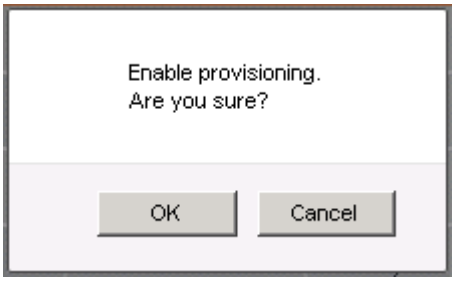
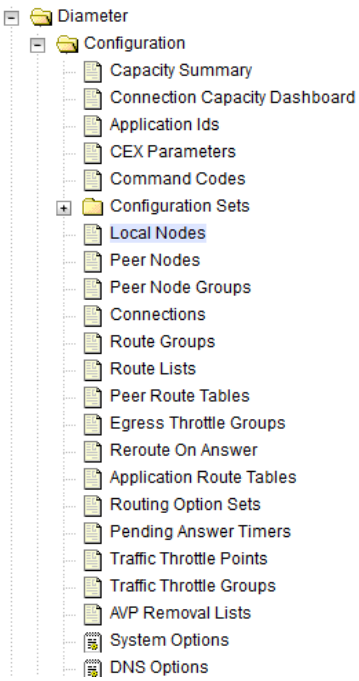
38. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status and Manage > Database**.
		 
		2. Select the active NOAM server and click **Report**.
		Main Menu: Status & Manage -> Database [Report]
		`dsr Database Status Report`
		`Report 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`
		3. Click **Save** to save the report to your local machine.

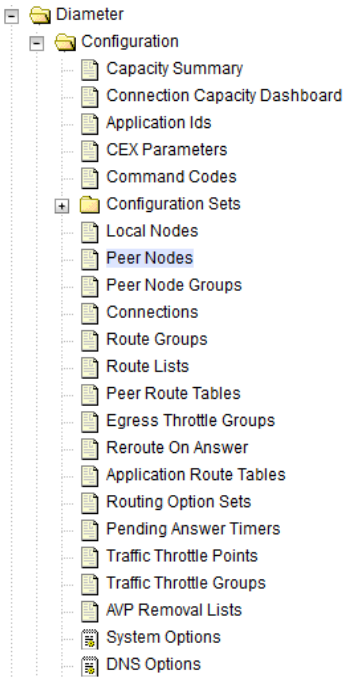
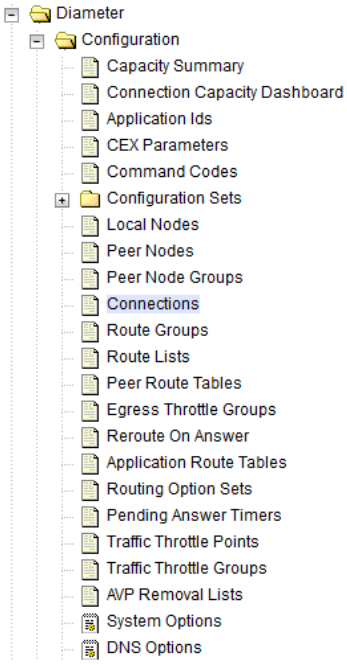
Procedure 1. Recovery Scenario 1		

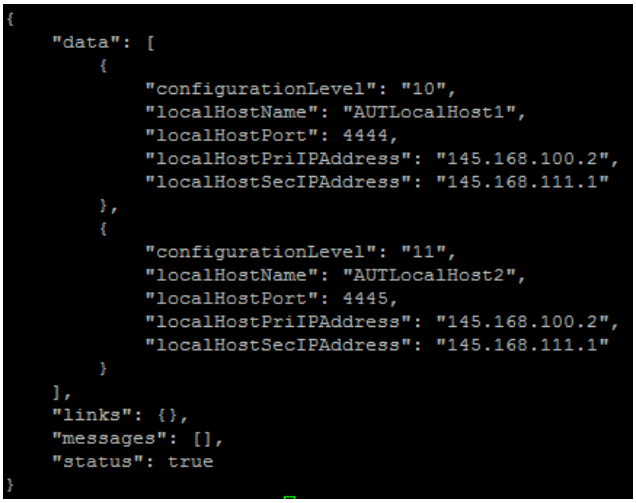
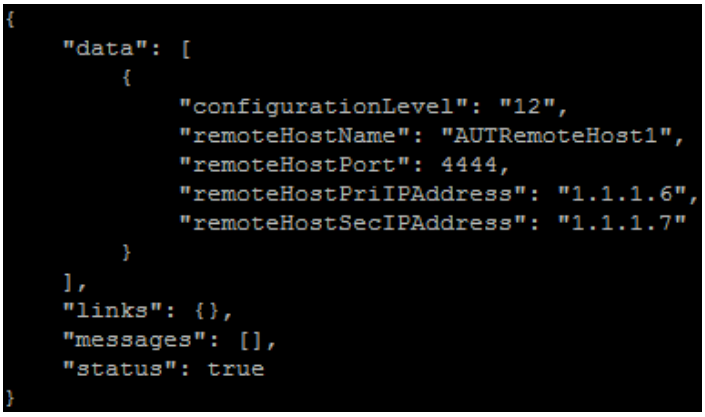
39. ☐	**Active NOAM**: Verify replication between servers	1. Log into the active NOAM using SSH terminal as **admusr**.
		2. Execute this command:
		`$ sudo irepstat –m`
		Output:
		`-- Policy 0 ActStb [DbReplication] ------------------`
		`Oahu-DAMP-1 – Act/Act`
		`  BC From Oahu-SOAM-2  Active   0   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 – Act/Stb`
		`  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`

Procedure 1. Recovery Scenario 1

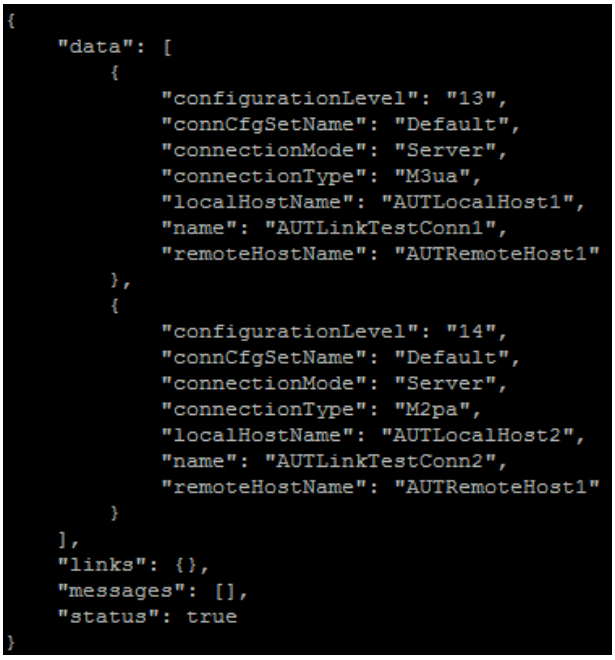
40. ☐	**NOAM VIP GUI**: Verify the database states	1. Navigate to **Status and Manager > Database**.  2. Verify the OAM Max HA Role is either **Active** or **Standby** for NOAM and SOAM; Application Max HA Role for MPs is **Active**; and status is **Normal**. 
41. ☐	**NOAM VIP GUI**: Verify the HA status	1. Navigate to **Status and Manage > HA**.  2. Select the row for all of the servers. 3. Verify the HA Role is either **Active** or **Standby**. 

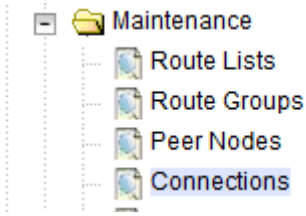
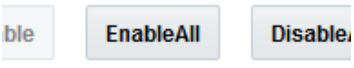
Procedure 1. Recovery Scenario 1		
42. ☐	**NOAM VIP GUI**: Enable provisioning	1. Navigate to **Status and Manage > Database**.  2. Click **Enable Provisioning**.  3. Click **OK** on the confirmation screen to enable provisioning. 
43. ☐	**SOAM VIP GUI**: Verify the local node information	1. Navigate to **Diameter > Configuration > Local Node**.  2. Verify all the local nodes are shown.

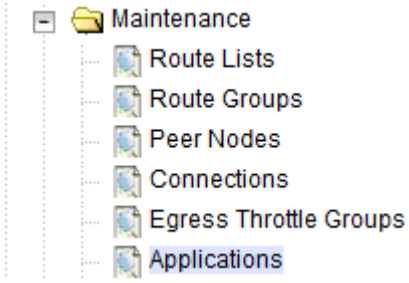
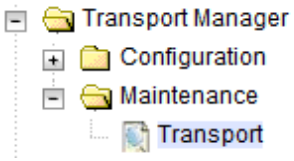
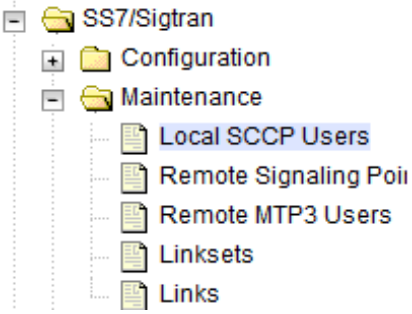
Procedure 1. Recovery Scenario 1		
44. ☐	**SOAM VIP GUI**: Verify the peer node information	1. Navigate to **Diameter > Configuration > Peer Node**.  2. Verify all the peer nodes are shown.
45. ☐	**SOAM VIP GUI**: Verify the connections information	1. Navigate to **Diameter > Configuration > Connections**.  2. Verify all the connections are shown.

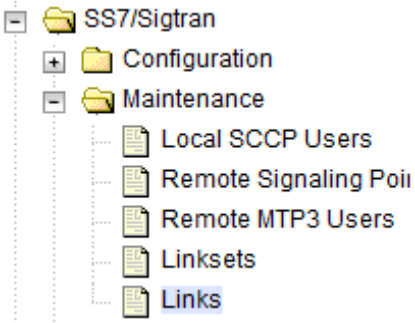
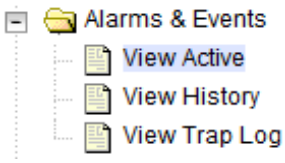
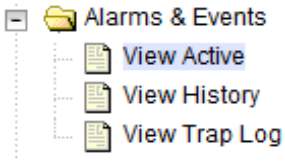
Procedure 1. Recovery Scenario 1		
46. ☐	For vSTP only **SOAM VIP Server Console**: Verify the vSTP MP local nodes information (optional)	1. Log into the SOAM VIP server console as **admusr**. 2. Execute this command: `[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts` 3. Verify output is similar to this: 
47. ☐	For vSTP only **SOAM VIP Server Console**: Verify the vSTP MP remote nodes information (optional)	1. Log into the SOAM VIP server console as **admusr**. 2. Execute this command: `[admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts` 3. Verify output is similar to this: 

Procedure 1. Recovery Scenario 1

48. ☐	For vSTP only
	SOAM VIP Server Console: Verify the vSTP MP connections information (optional)
		1. Log into the SOAM VIP server console as **admusr**.
		2. Execute this command:
		`[admusr@SOAM1 ~]$ mmiclient.py /vstp/connections`
		3. Verify output is similar to this:
		  {
		"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 authorization flag	For SCTP connections without DTLS enabled, refer to the **Enable/Disable DTLS** appendix in reference [1]. Execute the procedure on all failed MP servers.
50. ☐	**SOAM VIP GUI**: Enable connections, if needed	1. Navigate to **Diameter > Maintenance > Connections**.  2. Select each connection and click **Enable**. Alternatively, you can enable all the connections by clicking **EnableAll**.  3. Verify 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.

Procedure 1. Recovery Scenario 1		
51. ☐	**SOAM VIP GUI**: Enable optional features	1. Navigate to **Diameter > Maintenance > Applications**.  2. Select the optional feature application configured in step 37. 3. Click **Enable**. 
52. ☐	**SOAM VIP GUI**: Re-enable transports, if needed	1. Navigate to **Transport Manager > Maintenance > Transport**.  2. Select each transport and click **Enable**.  3. Verify the Operational Status for each transport is **Up**.
53. ☐	**SOAM VIP GUI**: Re-enable MAPIWF application, if needed	1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.  2. Click **Enable** for the corresponding to MAPIWF Application Name.  3. Verify the SSN Status is **Enabled**.

Procedure 1. Recovery Scenario 1		
54. ☐	**SOAM VIP GUI**: Re-enable links if needed	1. Navigate to **SS7/Sigtran > Maintenance > Links**.  2. Click **Enable** for each link.  3. Verify the Operational Status for each link is **Up**.
55. ☐	**SOAM VIP GUI**: Examine all alarms	1. Navigate to **Alarms & Events > View Active**.  2. 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	1. Log into the NOAM VIP, if not already logged in. 2. Navigate to **Alarms & Events > View Active**.  3. 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 5 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.

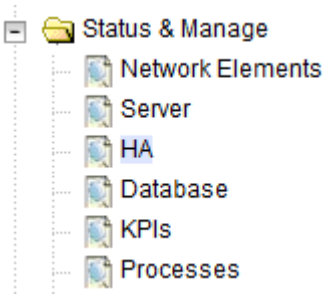
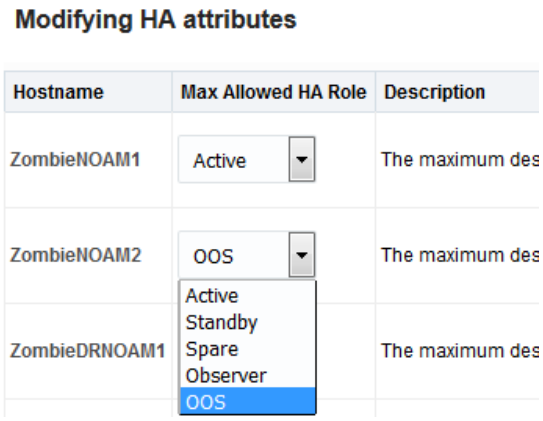
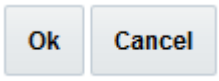
4.1.2 Recovery Scenario 2 (Partial Server Outage with One NOAM Server Intact and Both SOAMs Failed)

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 . The major activities are summarized as follows:

- Recover **Standby NOAM** server (if needed) by recovering software and the database.
  - Recover the software.
- Recover **Active SOAM** server by recovering software.
  - Recover the software.
  - Recover the Database.
- Recover any failed **SOAM** and **MP** servers by recovering software.
  - Recover the software.
  - The database has already been restored at the active SOAM server and does not require restoration at the SO and MP servers.

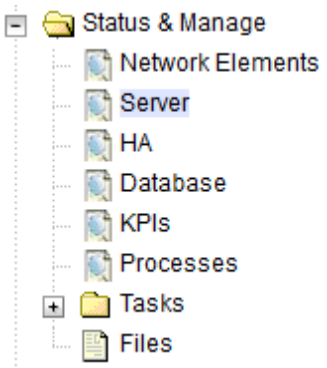
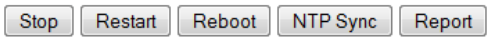
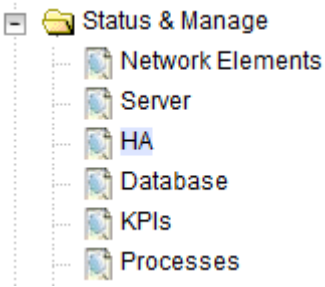
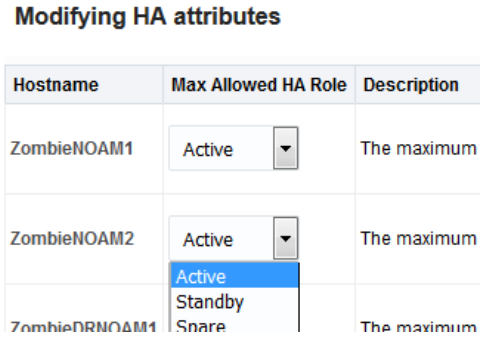
Procedure 2. Recovery Scenario 2		
This procedure performs recovery if at least 1 NOAM server is available but all SOAM servers in a site have failed. This includes any SOAM server that is in another location. Check off (√) each step as it is completed. Boxes have been provided for this purpose under 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 the Required Materials section.

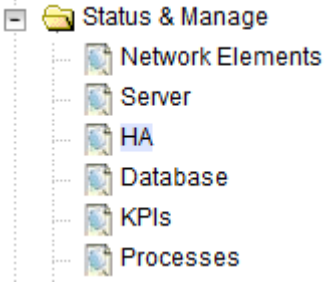
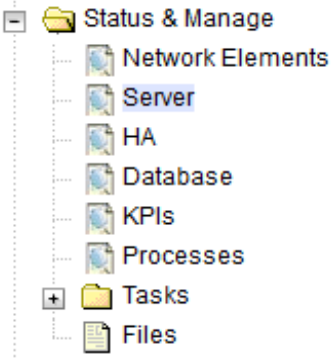
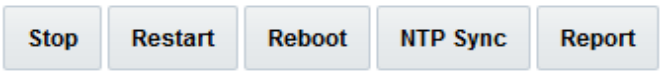
Procedure 2. Recovery Scenario 2		
3. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 

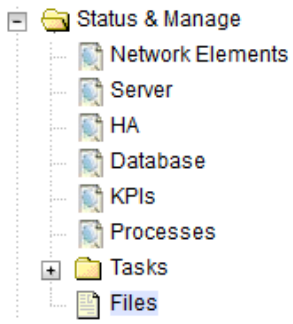
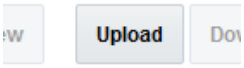
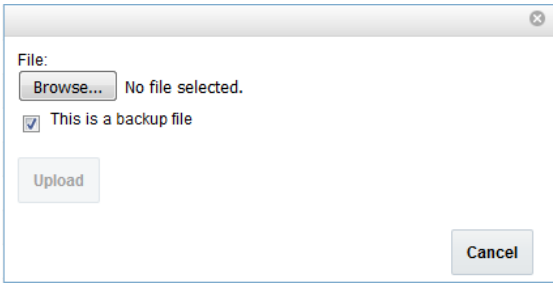
Procedure 2. Recovery Scenario 2		
4. ☐	**Active NOAM**: Set failed servers to standby	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Set the Max Allowed HA Role option to **OOS** for the failed servers.  4. Click **OK**. 

Procedure 2. Recovery Scenario 2		
5. ☐	Create VMs and recover the failed software	For VMWare based deployments: • 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 the procedure to import OVA. b. Procedure 2 **(VMWare Only) Configure NOAM Guests Based on Resource Profile**. • 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 the procedure to import OVA. b. Procedure 3 **(VMWare Only) Configure Remaining DSR Guests Based on Resource Profile**. For KVM/Openstack based deployments: • 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 the procedure to import OVA. b. Procedure 5 (**KVM/Openstack Only) Configure NOAM Guests Based on Resource Profile**. • 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 the procedure to import 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]: 1. Procedure 7 **(OVM-S/OVM-M) Import DSR OVA and Prepare for VM Creation**. 2. Procedure 8 **(OVM-S/OVM-M) Configure Each DSR VM**. 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.

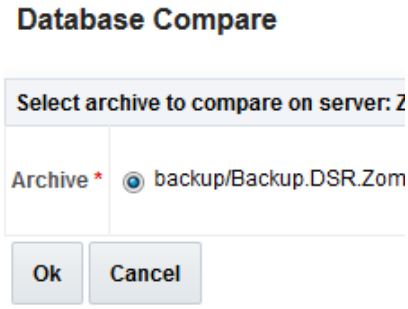
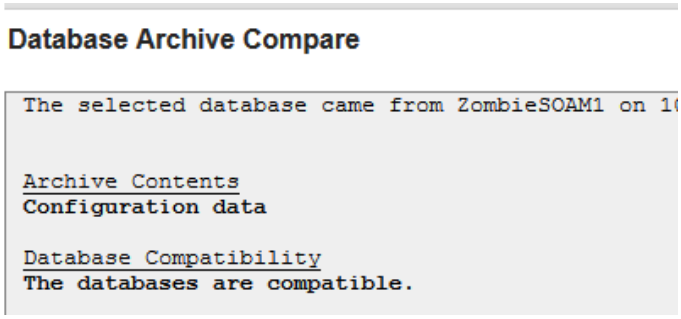
Procedure 2. Recovery Scenario 2		
7. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 
8. ☐	**NOAM VIP GUI**: Recover standby NOAM	Install the second NOAM server by executing procedures from reference [1]: 1. Procedure 15 **Configure the Second NOAM Server**, steps 1, 3-7. 2. 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.

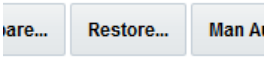
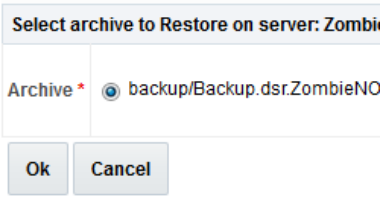
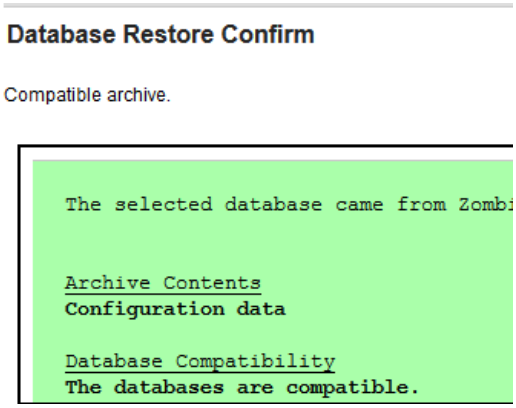
Procedure 2. Recovery Scenario 2		
9. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**. 
10. ☐	**NOAM VIP GUI**: Set HA on standby NOAM	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Select the standby NOAM server and set it to **Active**.  4. Click **OK**.

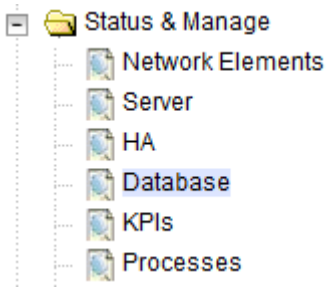
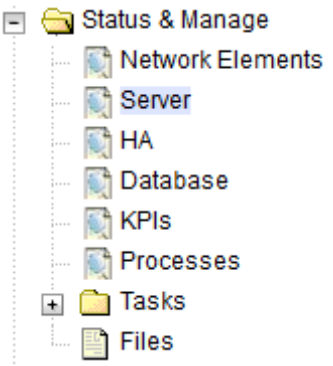
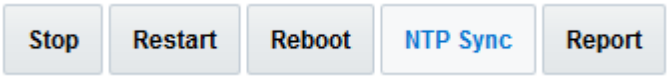
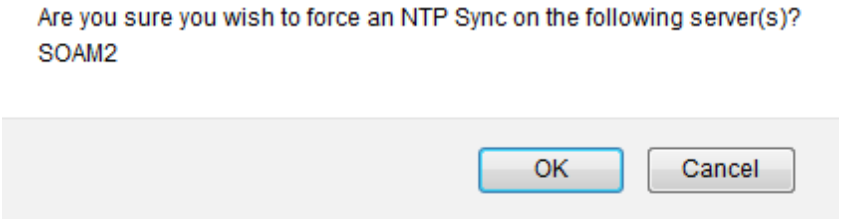
Procedure 2. Recovery Scenario 2		
11. ☐	**NOAM VIP GUI**: Stop replication to the C-level servers of this site 	**!!Warning!!** Inhibit replication to the working C-level servers that belong to the same site as the failed SOAM servers since recovery of the active SOAM causes the database wipeout in the C level servers because of the replication. **If the spare SOAM is also present in the site and lost**, execute Appendix D Inhibit A and B Level Replication on C-Level Servers (When Active, Standby, and Spare SOAMs are Lost) to inhibit replication to working C-level servers before continuing. **If the spare SOAM is NOT deployed in the site**, execute Appendix B Inhibit A and B Level Replication on C-Level Servers to inhibit replication to working C-level servers before continuing.
12. ☐	**NOAM VIP GUI**: Recover active SOAM server	Install the SOAM servers by executing procedure 22 **Configure the SOAM Servers**, steps 1, 3-6, from reference [1]. ***Note:*** Wait for server to reboot before continuing.
13. ☐	**NOAM VIP GUI**: Set HA on active SOAM	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Select the active SOAM server and set it to **Active**. 4. Click **OK**.
14. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered server and click **Restart**. 

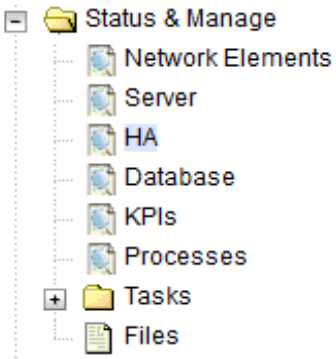
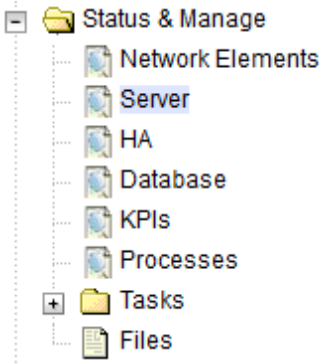
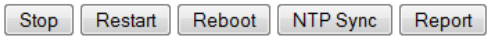
Procedure 2. Recovery Scenario 2		
15. ☐	**NOAM VIP GUI**: Upload the backed up SOAM database file	1. Navigate to **Status and Manage > Files**.  2. Select the active SOAM server. 3. Click **Upload** and select the **SO Provisioning and Configuration** file backed up after initial installation and provisioning.  4. Click **Browse** and locate the backup file. 5. Mark the **This is a backup file** checkbox. 6. Click **Upload**.  The file takes a few seconds to upload depending on the size of the backup data. The file is visible on the list of entries after the upload is complete.

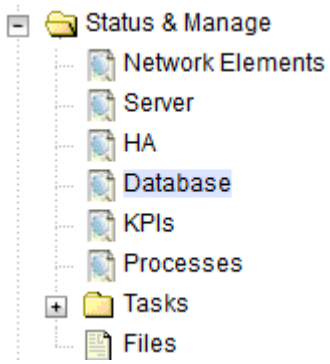
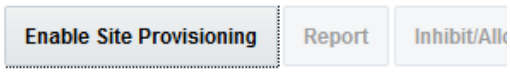
Procedure 2. Recovery Scenario 2		
16. ☐	**Recovered SOAM GUI**: Login	1. Establish a GUI session on the recovered SOAM server. 2. Open the web browser and enter a URL of: `http://<Recovered_SOAM_IP_Address>` 3. Login as the **guiadmin** user: 

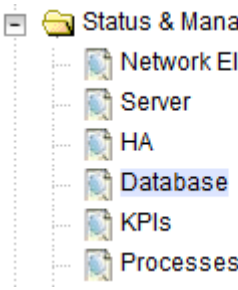
Procedure 2. Recovery Scenario 2		
17. ☐	**Recovered SOAM GUI**: Verify the archive contents and database compatibility	1. Navigate **to Status and Manage > Database**. 2. Select the active SOAM server and click **Compare**.  3. Click the button for the restored database file uploaded as a part of step 15. this procedure.  4. Verify the output window matches the screen below. ***Note:*** A database mismatch regarding the NodeIDs of the VMs displays. That is expected. If that is the only mismatch, proceed; otherwise, stop and contact My Oracle Support (MOS).  ***Notes***: • Archive Contents and Database Compatibilities must be the following: **Archive Contents**: Configuration data. **Database Compatibility**: The databases are compatible. • The following is expected output for the Topology Compatibility Check since we are restoring from an existing backed up database to a database with just one SOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. • We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility. 4. If the verification is successful, click **Back** and continue to the next step.

Procedure 2. Recovery Scenario 2		
18. ☐	**Recovered SOAM GUI**: Restore the database	1. From **Status and Manage > Database**. 2. Select the active NOAM server and click **Restore**.  3. Select the backup provisioning and configuration file.  4. Click **OK**. 5. If a database mismatch regarding the NodeIDs of the servers displays, that is expected. If no other errors display, mark the **Force** checkbox and click **OK** to proceed with the database restore.  ***Note:*** After the restore has started, the user is logged out of the XMI SOAM GUI since the restored topology is old data. The provisioning is disabled after this step.
19. ☐	**Recovered SOAM GUI**: Monitor and confirm database restoral	1. Wait for 5-10 minutes for the system to stabilize with the new topology. 2. Monitor the Info tab for **Success**. This indicates the backup is complete and the system is stabilized. ***Notes***: • Do not pay attention to alarms until all the servers in the system are completely restored. • The Configuration and Maintenance information is in the same state it was when backed up during the initial backup.
20. ☐	**NOAM VIP GUI**: Recover active SOAM server	Install the SOAM servers by executing procedure 22 **Configure the SOAM Servers**, steps 1, 3-6, from reference [1]. ***Note:*** Wait for server to reboot before continuing.

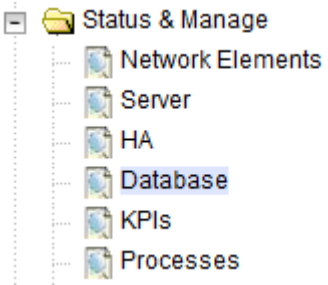
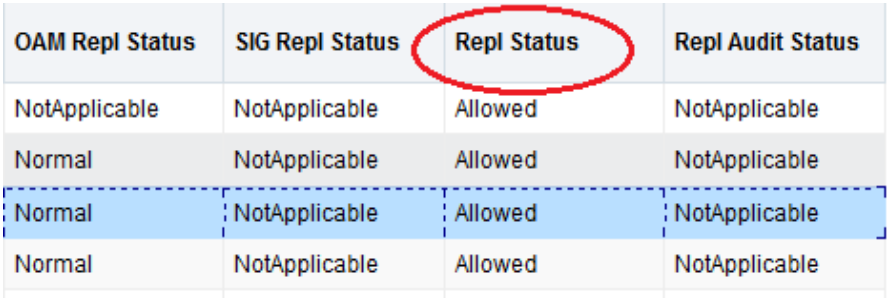
Procedure 2. Recovery Scenario 2		
21. ☐	**NOAM VIP GUI**: Start replication on the recovered SOAMs	Un-Inhibit (Start) Replication to the recovered SOAM servers 1. Navigate to **Status and Manage > Database**.  2. Click **Allow Replication** on the recovered SOAM servers. 3. Verify the replication on all SOAMs servers is allowed. This can be done by checking **Repl status** column of respective server
22. ☐	**Recovered Server**: Sync NTP	1. Navigate to **Status and Manage > Server**.  2. Select the recovered server and click **NTP Sync**.  3. Click **OK**. 

Procedure 2. Recovery Scenario 2		
23. ☐	**NOAM VIP GUI**: Set HA on SOAM servers	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. For each server whose Max Allowed HA Role is set to Standby, set it to **Active**. 4. Click **OK**.
24. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered server and click **Restart**. 

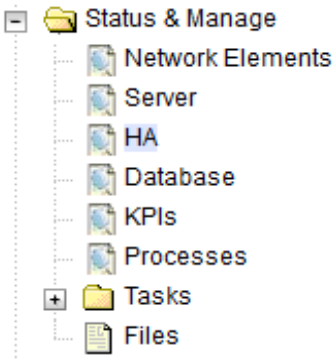
Procedure 2. Recovery Scenario 2		
25. ☐	**SOAM GUI**: Enable site provisioning	1. Navigate to **Status and Manage > Database**.  2. Click **Enable Site Provisioning**.  3. Click **OK** on the confirmation screen to enable provisioning.

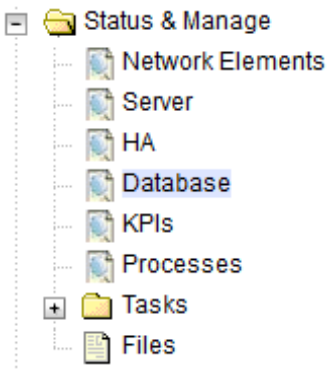
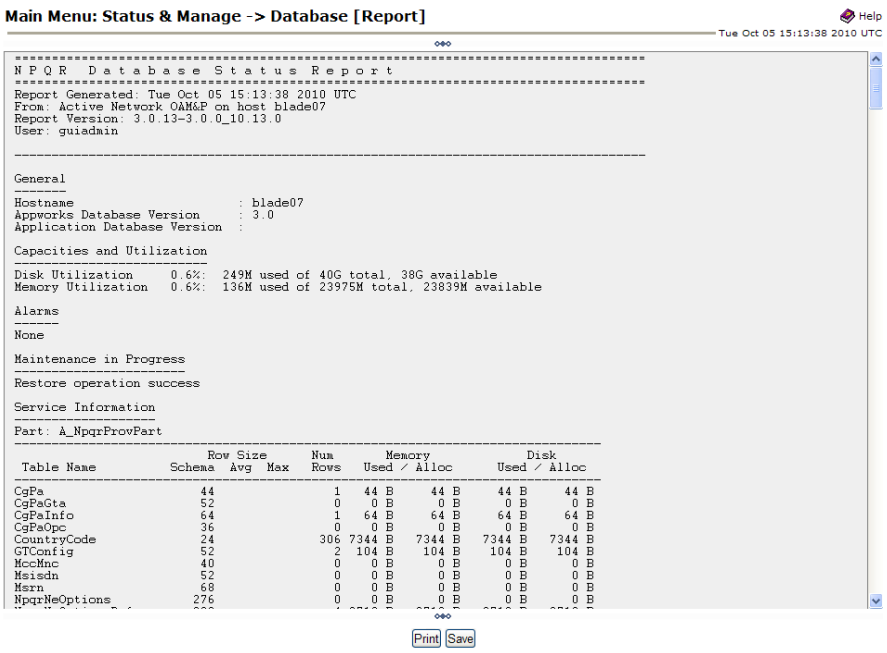
Procedure 2. Recovery Scenario 2		
26. ☐	**NOAM VIP GUI**: Start replication on working C-level servers	Un-inhibit (start) replication to the **working** C-level servers that belong to the same site as of the failed SOAM servers. **If the spare SOAM is also present in the site and lost**, execute Appendix E Un-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 Appendix C Un-Inhibit A and B Level Replication on C-Level Servers. 1. Navigate to **Status and Manage > Database**.  2. If the **Repl Status** is set to **Inhibited**, click **Allow Replication** using this order; otherwise, if none of the servers are inhibited, skip this step and continue with the next step: • Active NOAM server • Standby NOAM server • Active SOAM server • Standby SOAM server • Spare SOAM server, if applicable • Active DR NOAM server • Standby DR NOAM server • MP/IPFE servers • SBRs (if SBR servers are configured, start with the active SBR, then standby, then spare) 3. Verify the replication on all the working servers is allowed. This can be done by checking the **Repl Status** column. **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

Procedure 2. Recovery Scenario 2

27. ☐	**NOAM VIP GUI**: Recover the C-level servers (DA-MP, SBRs, IPFE, vSTP-MP)	1. Establish an SSH session to the C-level server being recovered and login as **admusr**. 2. Execute following command to set shared memory to unlimited: `$ sudo shl.set -m 0` 3. Execute the following procedure 25 **Configure the MP Virtual Machines**, steps 1, 8-14 (and 15, if required), from [1] for **EACH** server that has been recovered.
28. ☐	**NOAM VIP GUI**: Start replication on ALL C-level servers	Un-Inhibit (Start) Replication to the **ALL** C-level servers. 1. Navigate to **Status and Manage > Database**.  2. If the **Repl Status** is set to **Inhibited**, click **Allow Replication** using this order: • Active NOAMP server • Standby NOAMP server • Active SOAM server • Standby SOAM server • Spare SOAM server (if applicable) • Active DR NOAM server • Standby DR NOAM Server • MP/IPFE servers (if MPs are configured as active/standby, start with the Active MP; otherwise, the order of the MPs does not matter). 3. Verify the replication on all servers is allowed. This can be done by checking the **Repl Status** column. 

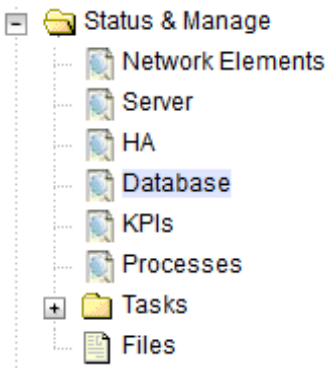
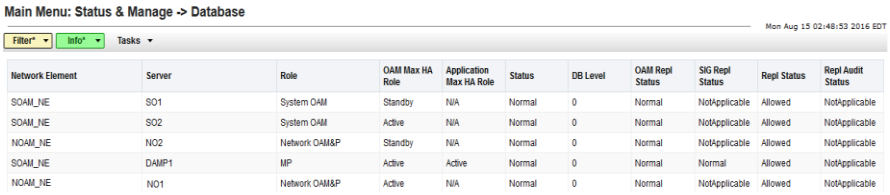
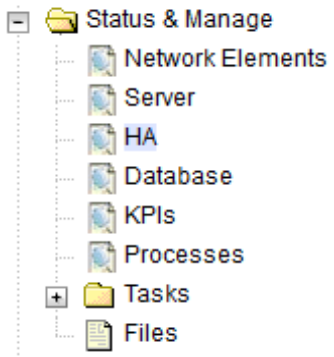
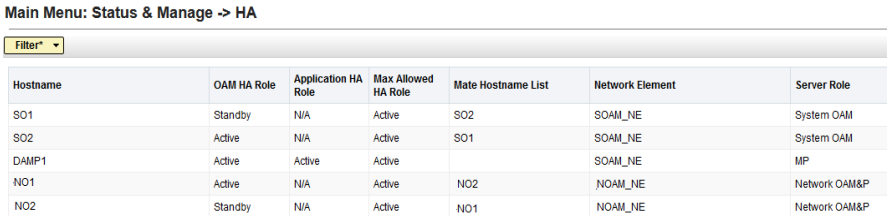
OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
NotApplicable	NotApplicable	Allowed	NotApplicable
Normal	NotApplicable	Allowed	NotApplicable
Normal	NotApplicable	Allowed	NotApplicable
Normal	NotApplicable	Allowed	NotApplicable

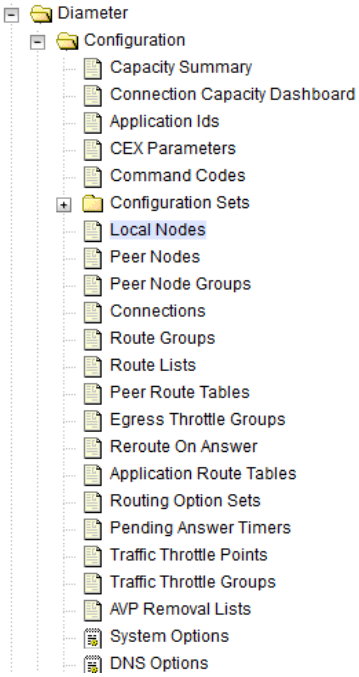
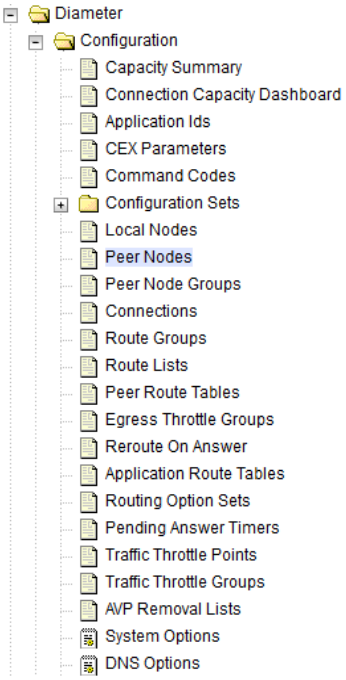
Procedure 2. Recovery Scenario 2		
29. ☐	**NOAM VIP GUI**: Set HA on all C-level servers	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. For each server whose Max Allowed HA Role is set to Standby, set it to **Active**. 4. Click **OK**.
30. ☐	**Active NOAM**: Perform key exchange between the active NOAM and recovered servers	1. Establish an SSH session to the active NOAM and login as **admusr**. 2. 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 and login as **admusr**. **Note for PCA Feature Activation:** If you have PCA installed in the system being recovered, re-activate the PCA by executing **PCA Activation on Standby NOAM server** on the recovered standby NOAM server, and **PCA Activation on Active SOAM Server** on the recovered active SOAM server from [3]. Refer to section 1.5 Optional Features to activate any features that were previously activated. ***Notes***: • While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored: `iload#31000{S/W Fault}` • If any of the MPs are failed and recovered, then these MP servers should be restarted after activation of the feature.

Procedure 2. Recovery Scenario 2		
32. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status and Manage > Database**.  2. Select the active NOAM server and click **Report**.  3. Click **Save** to save the report to your local machine.

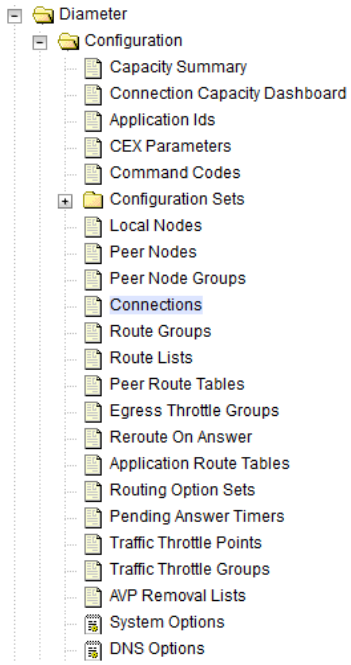
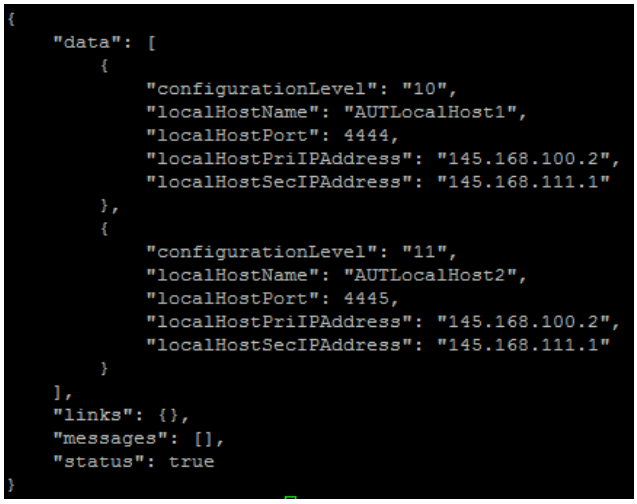
Procedure 2. Recovery Scenario 2		

33. ☐	**Active NOAM**: Verify replication between servers	1. Log into the active NOAM using SSH terminal as **admusr**.
		2. Execute this command:
		`$ sudo irepstat –m`
		Output:
		`-- Policy 0 ActStb [DbReplication] ------------------`
		`Oahu-DAMP-1 – Act/Act`
		`  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 – Act/Stb`
		`  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`

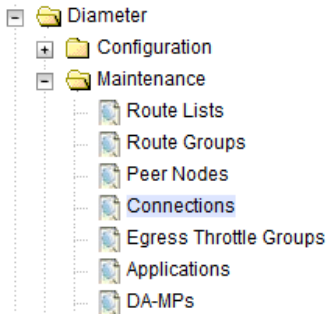
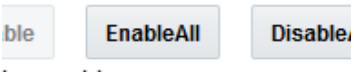
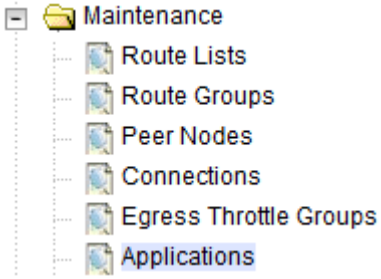
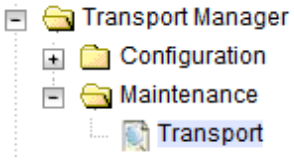
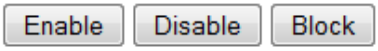
Procedure 2. Recovery Scenario 2		
34. ☐	**NOAM VIP GUI**: Verify the database states	1. Navigate to **Status and Manager > Database**.  2. Verify the OAM Max HA Role is either **Active** or **Standby** for NOAM and SOAM; Application Max HA Role for MPs is **Active**; and status is **Normal**. 
35. ☐	**NOAM VIP GUI**: Verify the HA status	1. Navigate to **Status and Manage > HA**.  2. Select the row for all of the servers. 3. Verify the HA Role is either **Active** or **Standby**. 

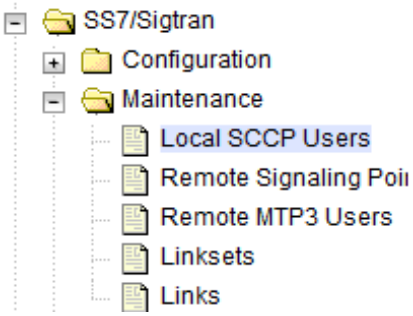
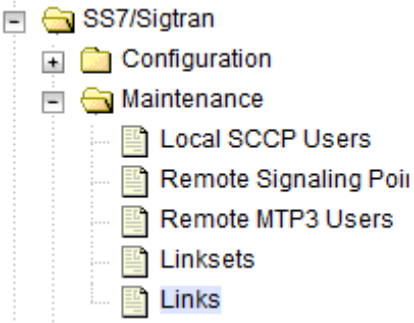
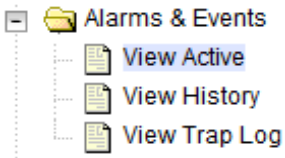
Procedure 2. Recovery Scenario 2		
36. ☐	**SOAM VIP GUI**: Verify the local node information	1. Navigate to **Diameter > Configuration > Local Node**.  2. Verify all the local nodes are shown.
37. ☐	**SOAM VIP GUI**: Verify the peer node information	1. Navigate to **Diameter > Configuration > Peer Node**.  2. Verify all the peer nodes are shown.

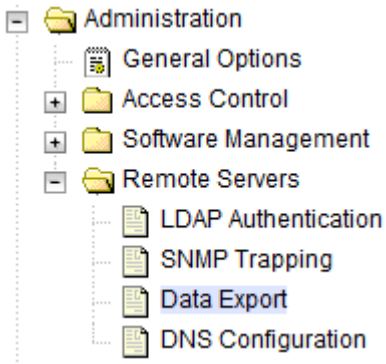
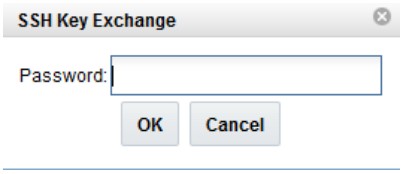
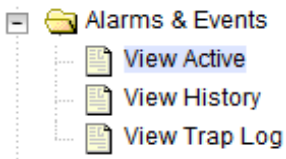
Procedure 2. Recovery Scenario 2

38. ☐	**SOAM VIP GUI**: Verify the connections information	1. Navigate to **Diameter > Configuration > Connections**.  2. Verify all the connections are shown.
39. ☐	For vSTP only **SOAM VIP Server Console**: Verify the vSTP MP local nodes information (optional)	1. Log into the SOAM VIP server console as **admusr**. 2. Execute this command: `[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts` 3. Verify output is similar to this: 

<table>
<tr><th colspan="3">Procedure 2. Recovery Scenario 2</th></tr>
<tr><td>40. ☐</td><td>For vSTP only
SOAM VIP Server Console: Verify the vSTP MP remote nodes information (optional)</td><td>1. Log into the SOAM VIP server console as admusr.
2. Execute this command:
<code>[admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts</code>
3. Verify output is similar to this:
<pre>{
    "data": [
        {
            "configurationLevel": "12",
            "remoteHostName": "AUTRemoteHost1",
            "remoteHostPort": 4444,
            "remoteHostPriIPAddress": "1.1.1.6",
            "remoteHostSecIPAddress": "1.1.1.7"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}</pre></td></tr>
<tr><td>41. ☐</td><td>For vSTP only
SOAM VIP Server Console: Verify the vSTP MP connections information (optional)</td><td>1. Log into the SOAM VIP server console as admusr.
2. Execute this command:
<code>[admusr@SOAM1 ~]$ mmiclient.py /vstp/connections</code>
3. Verify output is similar to this:
<pre>{
    "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
}</pre></td></tr>
<tr><td>42. ☐</td><td>MP Servers: Disable SCTP authorization flag</td><td>For SCTP connections without DTLS enabled, refer to the Enable/Disable DTLS appendix in reference [1].
Execute the procedure on all failed MP servers.</td></tr>
</table>

Procedure 2. Recovery Scenario 2		
43. ☐	**SOAM VIP GUI**: Enable connections, if needed	1. Navigate to **Diameter > Maintenance > Connections**.  2. Select each connection and click **Enable**. Alternatively, you can enable all the connections by clicking **EnableAll**.  3. Verify the Operational State is **Available**.
44. ☐	**SOAM VIP GUI**: Enable optional features	1. Navigate to **Diameter > Maintenance > Applications**.  2. Select the optional feature application configured in step 31. 3. Click **Enable**. 
45. ☐	**SOAM VIP GUI**: Re-enable transports, if needed	1. Navigate to **Transport Manager > Maintenance > Transport**.  2. Select each transport and click **Enable**.  3. Verify the Operational Status for each transport is **Up**.

Procedure 2. Recovery Scenario 2		
46. ☐	**SOAM VIP GUI**: Re-enable MAPIWF application, if needed	1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.  2. Click **Enable** for the corresponding to MAPIWF Application Name.  3. Verify the SSN Status is **Enabled**.
47. ☐	**SOAM VIP GUI**: Re-enable links if needed	1. Navigate to **SS7/Sigtran > Maintenance > Links**.  2. Click **Enable** for each link.  3. Verify the Operational Status for each link is **Up**.
48. ☐	**SOAM VIP GUI**: Examine all alarms	1. Navigate to **Alarms & Events > View Active**.  2. Examine all active alarms and refer to the on-line help on how to address them. If needed contact My Oracle Support (MOS).

Procedure 2. Recovery Scenario 2		
49. ☐	**SOAM VIP GUI**: Perform key exchange with export server	1. Navigate to **Administration > Remote Servers > Data Export**.  2. Click **SSH Key Exchange** at the bottom of the screen.  3. Type the **Password** and click **OK**. 
50. ☐	**NOAM VIP GUI**: Examine all alarms	1. Log into the NOAM VIP, if not already logged in. 2. Navigate to **Alarms & Events > View Active**.  3. 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:

4.1.3 Recovery Scenario 3 (Partial Server Outage with All NOAM Servers Failed and One SOAM Server Intact)

For a partial server outage with an SOAM server intact and available; NOAM servers are recovered using recovery procedures for software and then executing a database restore to the active NOAM server using a NOAM database backup file obtained from external backup sources such as customer servers. All other servers are recovered using recovery procedures for software. Database replication from the active NOAM/active SOAM server will recover the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures' detailed steps are in Procedure 3. The major activities are summarized as follows:

Recover **Active NOAM** server by recovering software and the database.

- Recover the software.
- Recover the database

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

- Recover the software.

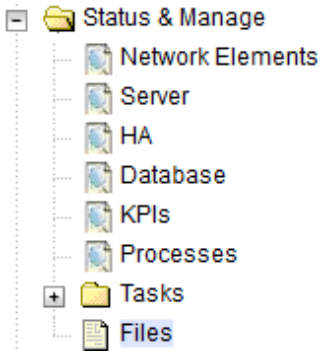
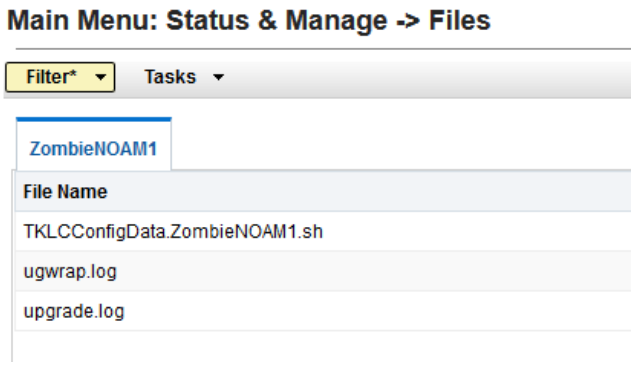
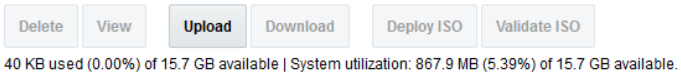
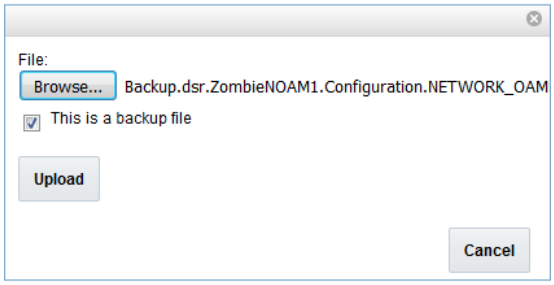
Recover any failed **SOAM and MP servers** by recovering software.

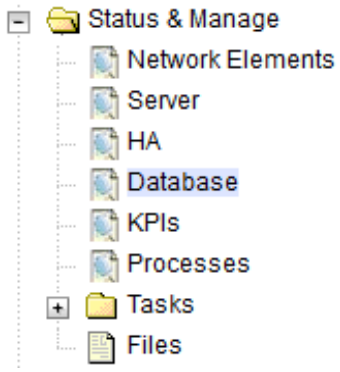
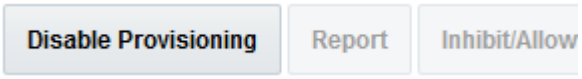
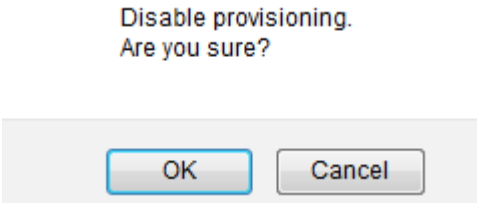
- Recover the software.
- Database is already intact at one SOAM server and does not require restoration at the other SOAM and MP servers.

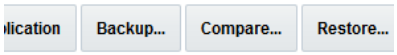
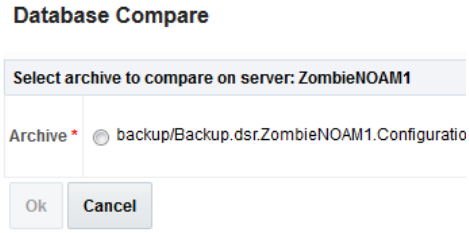
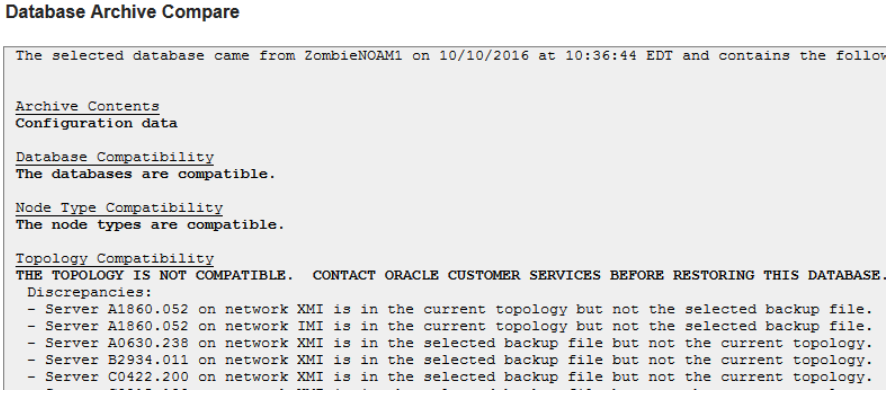
Procedure 3. Recovery Scenario 3		
This procedure performs recovery if ALL NOAM servers have failed but one or more SOAM servers are intact. This includes any SOAM server that is in another location (spare SOAM server). Check off (√) each step as it is completed. Boxes have been provided for this purpose 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/apply any workarounds required during this procedure.
2. ☐	Gather required materials	Gather the documents and required materials listed in the Required Materials section.

Procedure 3. Recovery Scenario 3		
3. ☐	Recover the failed software	For VMWare based deployments: • 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 the procedure to import OVA. b. Procedure 2 **(VMWare Only) Configure NOAM Guests Based on Resource Profile**. • For SOAMs or 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 the procedure to import OVA. b. Procedure 3 **(VMWare Only) Configure Remaining DSR Guests Based on Resource Profile**. For KVM/Openstack based deployments: • 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 the procedure to import OVA. b. Procedure 5 (**KVM/Openstack Only) Configure NOAM Guests Based on Resource Profile**. • For SOAMs or 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 the procedure to import 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]: 1. Procedure 7 **(OVM-S/OVM-M) Import DSR OVA and Prepare for VM Creation**. 2. 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 (for example, file servers) or tape backup sources. From required materials list in the Required Materials section; use site survey documents and network element report (if available), to determine network configuration data.

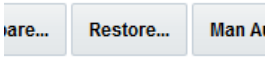
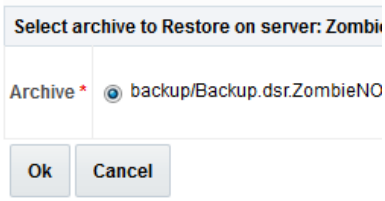
Procedure 3. Recovery Scenario 3		
5. ☐	Execute DSR installation procedure for the first NOAM	Verify the networking data for network elements. ***Note:*** Use the backup copy of network configuration data and site surveys (step 2.). Execute installation procedures for the first NOAM server from reference [1]: 1. Procedure 13 **Configure the First NOAM NE and Server**. 2. Procedure 14 **Configure the NOAM Server Group**.
6. ☐	**NOAM GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 

Procedure 3. Recovery Scenario 3		
7. ☐	**NOAM GUI**: Upload the backed up database file	1. Navigate to **Status and Manage > Files**.  2. Select the active NOAM server.  3. Click **Upload** and select the **NO Provisioning and Configuration** file backed up after initial installation and provisioning.  4. Click **Browse** and locate the backup file. 5. Mark the **This is a backup file** checkbox. 6. Click **Upload**.  The file takes a few seconds to upload depending on the size of the backup data. The file is visible on the list of entries after the upload is complete.

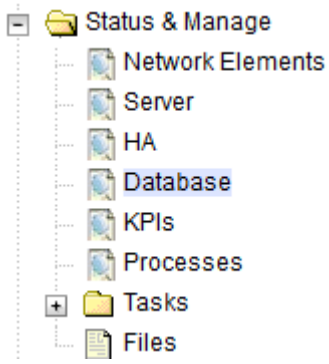
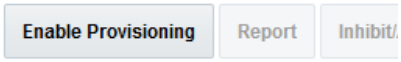
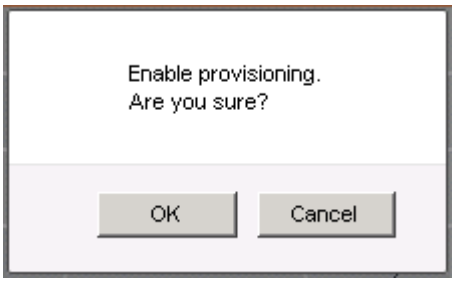
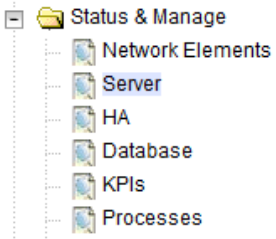
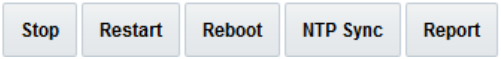
Procedure 3. Recovery Scenario 3		
8. ☐	**NOAM GUI**: Disable provisioning	1. Navigate to **Status and Manage > Database**.  2. Click **Disable Provisioning**.  3. Click **OK** on the confirmation screen to disable provisioning. 

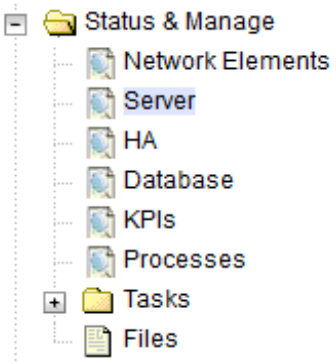
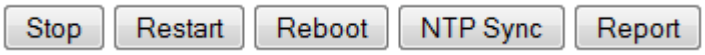
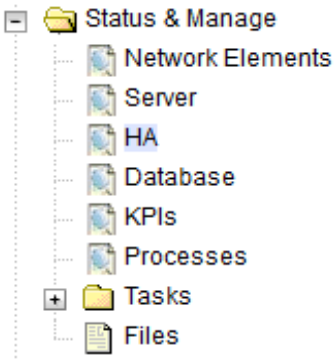
Procedure 3. Recovery Scenario 3		
9. ☐	**NOAM GUI**: Verify the archive contents and database compatibility	1. Select the active NOAM server and click **Compare**.  2. Click the button for the restored database file uploaded as a part of step 7. of this procedure.  3. Verify the output window matches the screen below. ***Note:*** A database mismatch regarding the NodeIDs of the VMs displays. That is expected. If that is the only mismatch, proceed; otherwise, stop and contact My Oracle Support (MOS).  ***Notes***: • Archive Contents and Database Compatibilities must be the following: **Archive Contents**: Configuration data. **Database Compatibility**: The databases are compatible. • The following is expected output for the Topology Compatibility Check since we are restoring from an existing backed up database to a database with just one NOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. • We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility. 4. If the verification is successful, click **Back** and continue to the next step.

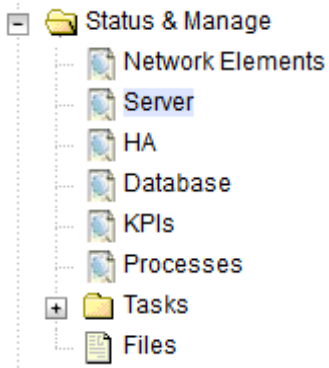
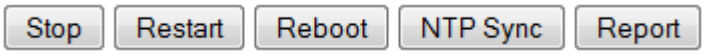
Procedure 3. Recovery Scenario 3

10. ☐	**Active NOAM**: Restore the database	1. From **Status and Manage > Database**. 2. Select the active NOAM server and click **Restore**.  3. Select the backup provisioning and configuration file.  4. Click **OK**. ***Note:*** A database mismatch regarding the NodeIDs of the VMs displays. That is expected. If that is the only mismatch, proceed; otherwise, stop and contact My Oracle Support (MOS). 5. Mark the **Force** checkbox and click **OK** to proceed with the database restore.  After the restore has started, the user is logged out of the XMI NOAM GUI since the restored topology is old data.

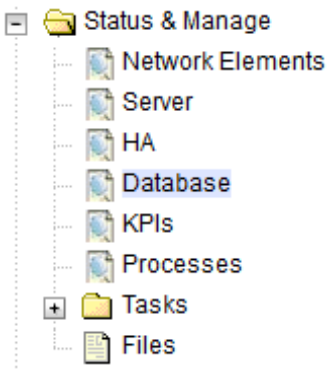
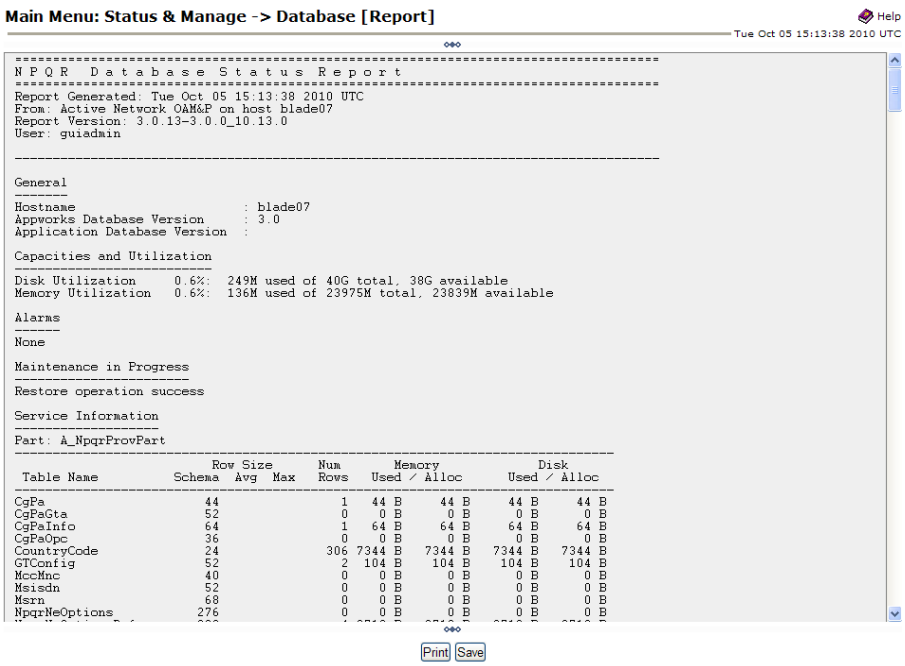
Procedure 3. Recovery Scenario 3		
11. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 
12. ☐	**NOAM VIP GUI**: Monitor and confirm database restoral	1. Wait for 5-10 minutes for the system to stabilize with the new topology. 2. Monitor the Info tab for Success. This indicates the restore is complete and the system is stabilized. Ignore these alarms 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). ***Notes***: • Do not pay attention to alarms until all the servers in the system are completely restored. • The Configuration and Maintenance information will be in the same state it was backed up during initial backup.
13. ☐	**Active NOAM**: Login	Log into the recovered active NOAM with the SSH terminal as **admusr**.

Procedure 3. Recovery Scenario 3		
14. ☐	**NOAM VIP GUI**: Re-enable provisioning	1. Navigate to **Status and Manage > Database**.  2. Click **Enable Provisioning**.  3. Click **OK** on the confirmation screen to enable provisioning. 
15. ☐	**NOAM VIP GUI**: Recover standby NOAM	Install the second NOAM server by executing procedure 15 **Configure the Second NOAM Server**, steps 1, 3-7, from reference [1].
16. ☐	**NOAM VIP GUI:** Recover standby NOAM	1. Navigate to **Status and Manage > Server**.  2. Select the second NOAM server click **Restart**.  3. 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.

Procedure 3. Recovery Scenario 3		
17. ☐	**NOAM VIP GUI**: Recover remaining failed SOAM servers	Recover the remaining SOAM servers (standby, spare) by repeating this step for each SOAM server: Install the remaining SOAM servers by executing procedure 22 **Configure the SOAM Servers**, steps 1, 3-6, from reference [1]. ***Note:*** Wait for server to reboot before continuing.
18. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered server and click **Restart**. 
19. ☐	**NOAM VIP GUI:** Set HA on all C-Level Servers	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. For each server whose Max Allowed HA Role is not set to Active, set it to **Active**. 4. Click **OK**.

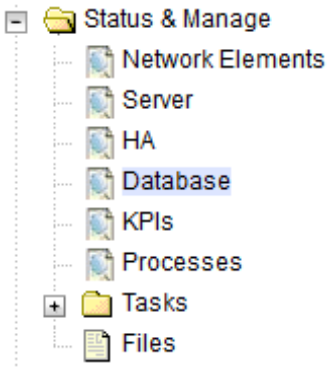
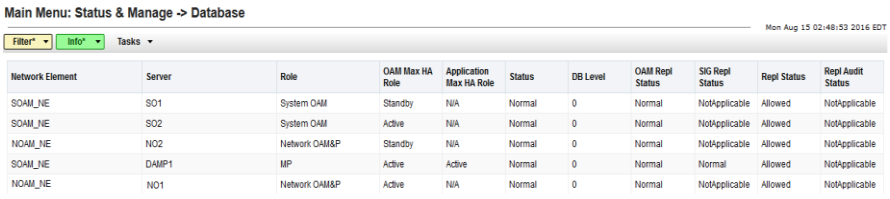
Procedure 3. Recovery Scenario 3		
20. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered server and click **Restart**. 
21. ☐	**Active NOAM**: Perform key exchange between the active NOAM and recovered servers	1. Establish an SSH session to the active NOAM and login as **admusr**. 2. 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 and login as **admusr**. **Note for PCA Feature Activation:** If you have PCA installed in the system being recovered, re-activate the PCA by executing **PCA Activation on Standby NOAM server** on the recovered standby NOAM server, and **PCA Activation on Active SOAM Server** on the recovered active SOAM server from [3]. Refer to section 1.5 Optional Features to activate any features that were previously activated. ***Notes***: • While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored: `iload#31000{S/W Fault}` • If any of the MPs are failed and recovered, then these MP servers should be restarted after activation of the feature.

Procedure 3. Recovery Scenario 3

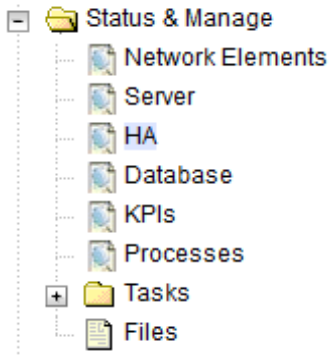
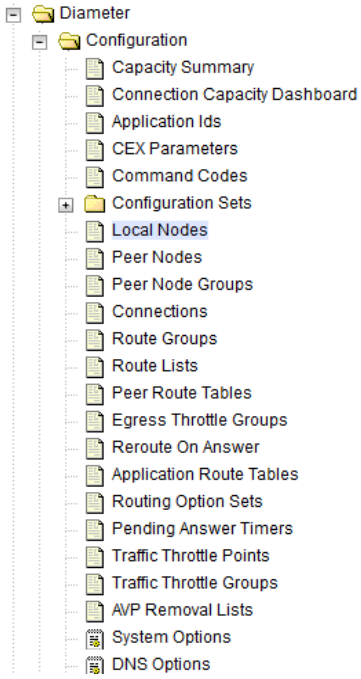
23. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status and Manage > Database**.  2. Select the active NOAM server and click **Report**.  3. Click **Save** to save the report to your local machine.

Procedure 3. Recovery Scenario 3

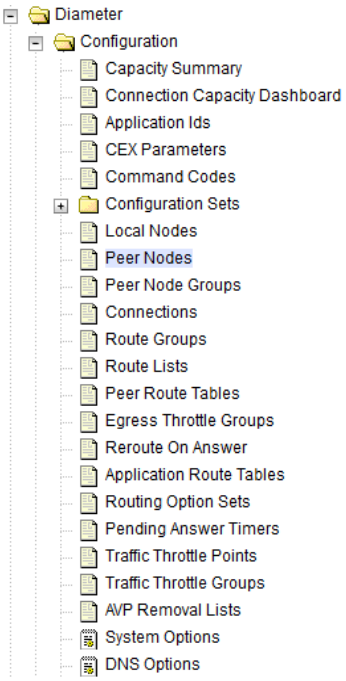
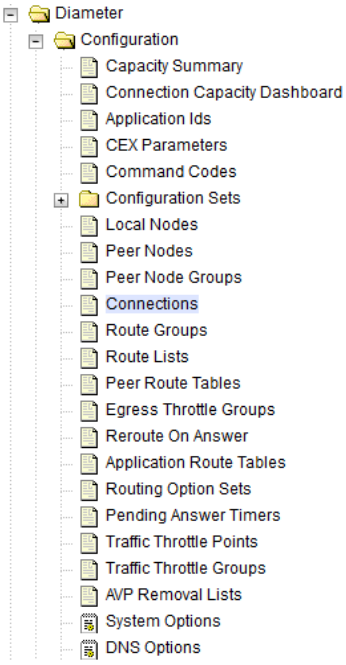
24. ☐	**Active NOAM**: Verify replication between servers	1. Log into the active NOAM using SSH terminal as **admusr**.
		2. Execute this command:
		`$ sudo irepstat –m`
		Output:
		`-- Policy 0 ActStb [DbReplication] ------------------------------`
		`RDU06-MP1 -- Stby`
		`BC From RDU06-SO1 Active 0 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	1. Navigate to **Status and Manager > Database**.  2. Verify the OAM Max HA Role is either **Active** or **Standby** for NOAM and SOAM; Application Max HA Role for MPs is **Active**; and status is **Normal**. 

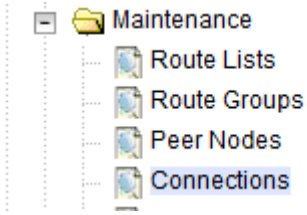
Procedure 3. Recovery Scenario 3

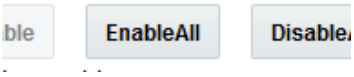
26. ☐	**NOAM VIP GUI**: Verify the HA status	1. Navigate to **Status and Manage > HA**.  2. Select the row for all of the servers. 3. Verify the HA Role is either **Active** or **Standby**. **Main Menu: Status & Manage -> HA** Filter*
27. ☐	**SOAM VIP GUI**: Verify the local node information	1. Navigate to **Diameter > Configuration > Local Node**.  2. Verify all the local nodes are shown.

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

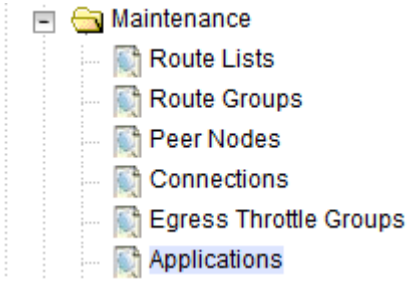
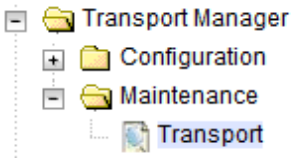
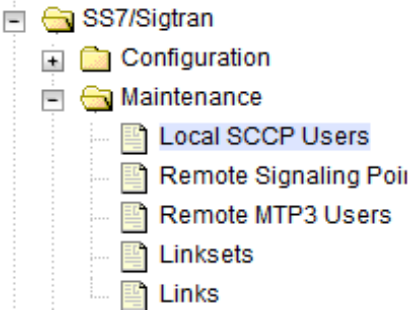
Procedure 3. Recovery Scenario 3		
28. ☐	**SOAM VIP GUI**: Verify the peer node information	1. Navigate to **Diameter > Configuration > Peer Node**.  2. Verify all the peer nodes are shown.
29. ☐	**SOAM VIP GUI**: Verify the connections information	1. Navigate to **Diameter > Configuration > Connections**.  2. Verify all the connections are shown.

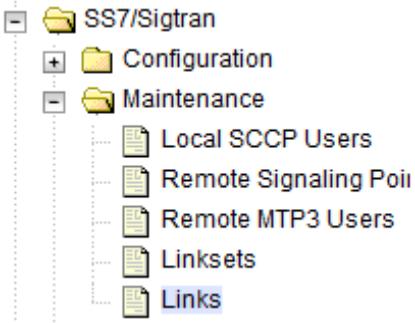
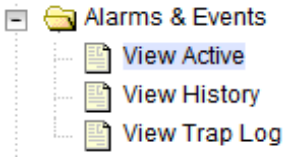
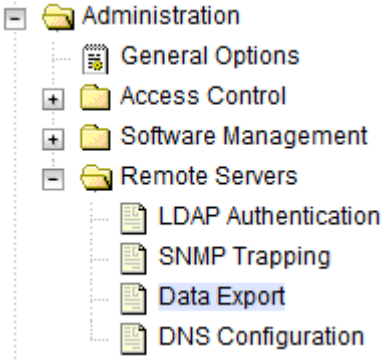
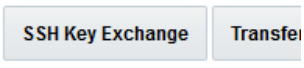
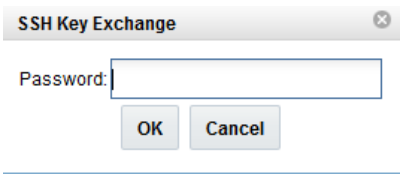
<table>
<tr><th colspan="3">Procedure 3. Recovery Scenario 3</th></tr>
<tr><td>30. ☐</td><td>For vSTP only
SOAM VIP Server Console: Verify the vSTP MP local nodes information (optional)</td><td>1. Log into the SOAM VIP server console as admusr.
2. Execute this command:
<code>[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts</code>
3. Verify output is similar to this:
<pre>{
    "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
}</pre></td></tr>
<tr><td>31. ☐</td><td>For vSTP only
SOAM VIP Server Console: Verify the vSTP MP remote nodes information (optional)</td><td>1. Log into the SOAM VIP server console as admusr.
2. Execute this command:
<code>[admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts</code>
3. Verify output is similar to this:
<pre>{
    "data": [
        {
            "configurationLevel": "12",
            "remoteHostName": "AUTRemoteHost1",
            "remoteHostPort": 4444,
            "remoteHostPriIPAddress": "1.1.1.6",
            "remoteHostSecIPAddress": "1.1.1.7"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}</pre></td></tr>
</table>

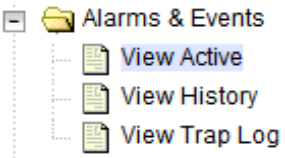
<table>
<tr><th colspan="3">Procedure 3. Recovery Scenario 3</th></tr>
<tr><td>32. ☐</td><td>For vSTP only
SOAM VIP Server Console: Verify the vSTP MP connections information (optional)</td><td>1. Log into the SOAM VIP server console as admusr.
2. Execute this command:
<code>[admusr@SOAM1 ~]$ mmiclient.py /vstp/connections</code>
3. Verify output is similar to this:
<pre>{
    "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
}</pre></td></tr>
<tr><td>33. ☐</td><td>SOAM VIP GUI: Enable connections, if needed</td><td>1. Navigate to Diameter > Maintenance > Connections.
 

2. Select each connection and click Enable. Alternatively, you can enable all the connections by clicking EnableAll.
 

3. Verify the Operational State is Available.</td></tr>
</table>

Procedure 3. Recovery Scenario 3		
34. ☐	**SOAM VIP GUI**: Enable optional features	1. Navigate to **Diameter > Maintenance > Applications**.  2. Select the optional feature application configured in step 22. 3. Click **Enable**. 
35. ☐	**SOAM VIP GUI**: Re-enable transports, if needed	1. Navigate to **Transport Manager > Maintenance > Transport**.  2. Select each transport and click **Enable**.  3. Verify the Operational Status for each transport is **Up**.
36. ☐	**SOAM VIP GUI**: Re-enable MAPIWF application, if needed	1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.  2. Click **Enable** for the corresponding to MAPIWF Application Name.  3. Verify the SSN Status is **Enabled**.

Procedure 3. Recovery Scenario 3		
37. ☐	**SOAM VIP GUI**: Re-enable links if needed	1. Navigate to **SS7/Sigtran > Maintenance > Links**.  2. Click **Enable** for each link.  3. Verify the Operational Status for each link is **Up**.
38. ☐	**SOAM VIP GUI**: Examine all alarms	1. Navigate to **Alarms & Events > View Active**.  2. Examine all active alarms and refer to the on-line help on how to address them. If needed contact My Oracle Support (MOS).
39. ☐	**SOAM VIP GUI**: Perform key exchange with export server	1. Navigate to **Administration > Remote Servers > Data Export**.  2. Click **SSH Key Exchange** at the bottom of the screen.  3. Type the **Password** and click **OK**. 

Procedure 3. Recovery Scenario 3		
40. ☐	**NOAM VIP GUI**: Examine all alarms	1. Log into the NOAM VIP, if not already logged in. 2. Navigate to **Alarms & Events > View Active**.  3. 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 5 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.

4.1.4 Recovery Scenario 4 (Partial Server Outage with One NOAM Server and One SOAM Server Intact)

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

Recover Standby NOAM server by recovering software.

- Recover the software.

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

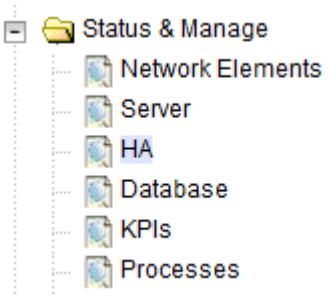
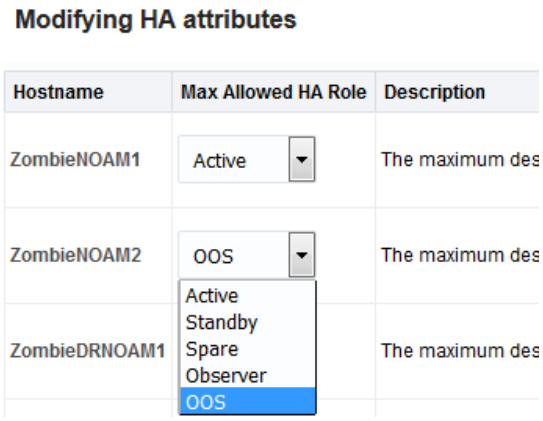
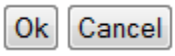
- Recover any failed SO and MP servers by recovering software.
- Recover the software.

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

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

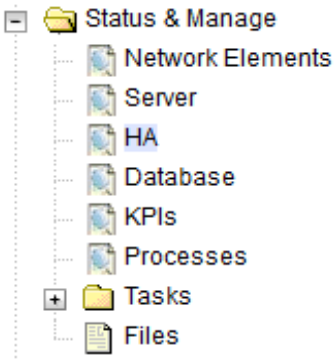
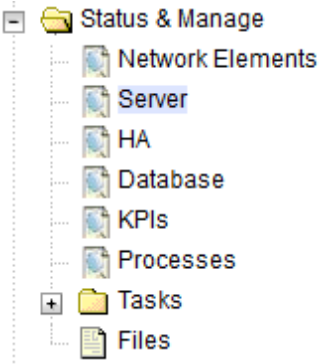
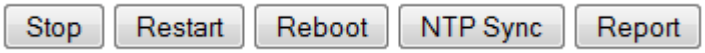
Procedure 4. Recovery Scenario 4		
This procedure performs recovery if at least 1 NOAM server is intact and available and 1 SOAM server is intact and available. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.		
1. ☐	Workarounds	Refer to Workarounds for Issues Not Fixed in this Release to understand/apply any workarounds required during this procedure.

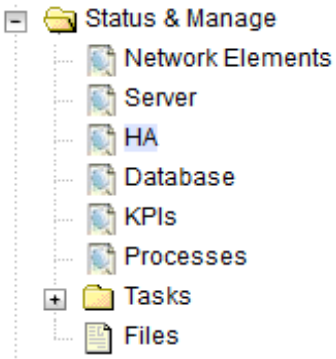
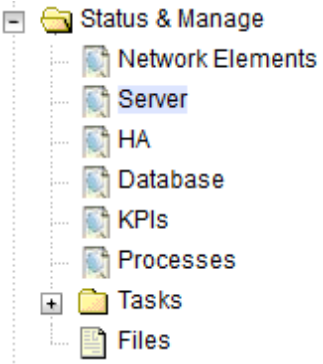
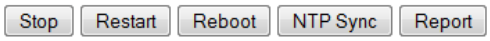
Procedure 4. Recovery Scenario 4		
2. ☐	Gather required materials	Gather the documents and required materials listed in the Required Materials section.
3. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 

Procedure 4. Recovery Scenario 4		
4. ☐	**Active NOAM**: Set failed servers to OOS	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Set the Max Allowed HA Role option to **OOS** for the failed servers.  4. Click **OK**. 

Procedure 4. Recovery Scenario 4		
5. ☐	Recover the failed software	For VMWare based deployments: • 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 the procedure to import OVA. b. Procedure 2 **(VMWare Only) Configure NOAM Guests Based on Resource Profile**. • For SOAMs or 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 the procedure to import OVA. b. Procedure 3 **(VMWare Only) Configure Remaining DSR Guests Based on Resource Profile**. For KVM/Openstack based deployments: • 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 the procedure to import OVA. b. Procedure 5 (**KVM/Openstack Only) Configure NOAM Guests Based on Resource Profile**. • For SOAMs or 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 the procedure to import 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]: 1. Procedure 7 **(OVM-S/OVM-M) Import DSR OVA and Prepare for VM Creation**. 2. 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	If necessary, repeat 5. for all remaining failed servers.

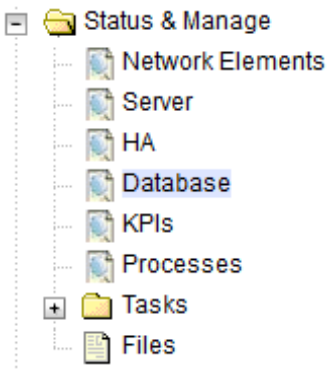
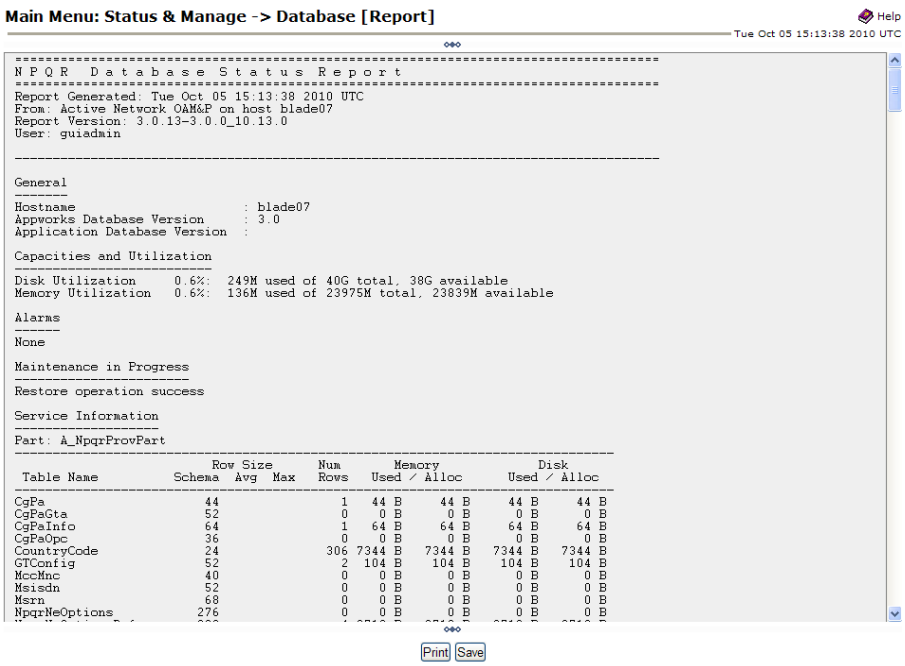
Procedure 4. Recovery Scenario 4		
7. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 
8. ☐	**NOAM VIP GUI:** Recover standby NOAM	Install the second NOAM server by executing procedures from reference [1]: 1. Procedure 15 **Configure the Second NOAM Server**, steps 1, 3-7. 2. 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.
9. ☐	**NOAM VIP GUI**: Recover remaining failed SOAM servers (optional)	Recover the remaining SOAM servers (standby, spare) by repeating this step for each SOAM server: Install the remaining SOAM servers by executing procedure 22 **Configure the SOAM Servers**, steps 1, 3-6, from reference [1]. ***Note:*** Wait for server to reboot before continuing.

Procedure 4. Recovery Scenario 4		
10. ☐	**NOAM VIP GUI**: Set HA on recovered servers (optional)	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. For each server whose Max Allowed HA Role is set to Standby, set it to **Active**. 4. Click **OK**.
11. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**. 
12. ☐	**NOAM VIP GUI:** Recover the C-Level Server (DA-MP, SBRs, IPFE, vSTP-MP)	1. Establish an SSH session to the C-level server being recovered and login as **admusr**. 2. Execute the procedure 25 **Configure the MP Virtual Machines**, steps 1, 8-14 (and 15, if required), from [1] for **EACH** server that has been recovered.

Procedure 4. Recovery Scenario 4		
13. ☐	**NOAM VIP GUI**: Set HA on all C-level servers	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. For each server whose Max Allowed HA Role is set to Standby, set it to **Active**. 4. Click **OK**.
14. ☐	**NOAM VIP GUI**: Restart DSR application on recovered C-level servers	1. Navigate to **Status and Manage > Server**.  2. Select the recovered server and click **Restart**. 
15. ☐	**Active NOAM**: Perform key exchange between the active NOAM and recovered servers	1. Establish an SSH session to the active NOAM and login as **admusr**. 2. Perform a keyexchange from the active NOAM to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>`

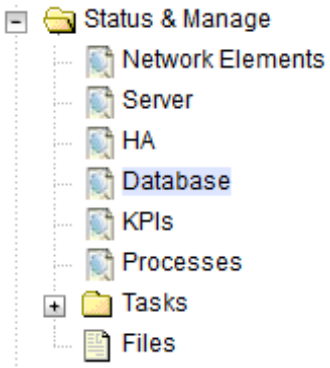
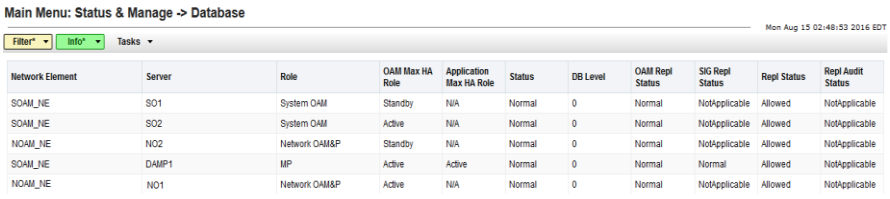
Procedure 4. Recovery Scenario 4		
16. ☐	**Active NOAM**: Activate optional features	Establish an SSH session to the active NOAM and login as **admusr**. **Note for PCA Feature Activation:** If you have PCA installed in the system being recovered, re-activate the PCA by executing the **PCA Activation on Standby NOAM Server** procedure on the recovered standby NOAM servers, and the **PCA Activation on Active SOAM Server** procedure on the recovered active SOAM server from [3]. Refer to section 1.5 Optional Features to activate any features that were previously activated. ***Notes***: • While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored: `iload#31000{S/W Fault}` • If any of the MPs are failed and recovered, then these MP servers should be restarted after activation of the feature.

Procedure 4. Recovery Scenario 4

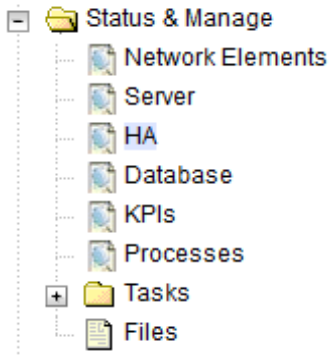
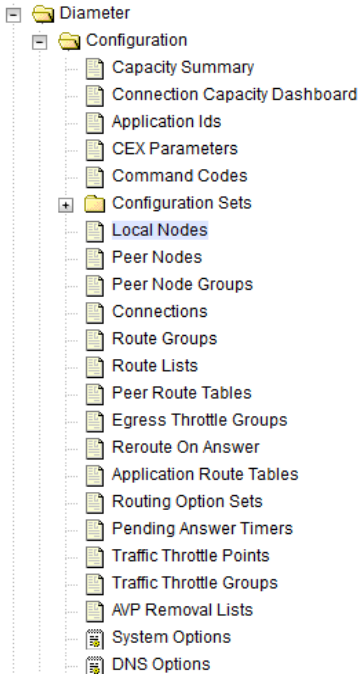
17. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status and Manage > Database**.  2. Select the active NOAM server and click **Report**.  3. Click **Save** to save the report to your local machine.

Procedure 4. Recovery Scenario 4

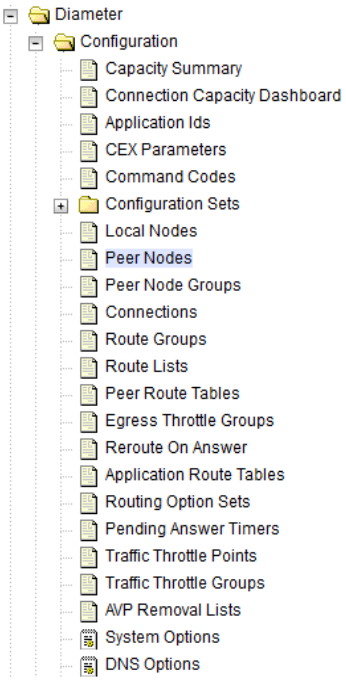
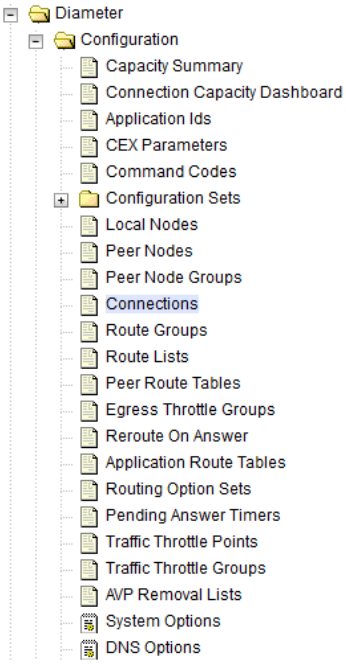
18. ☐	**Active NOAM**: Verify replication between servers	1. Log into the active NOAM using SSH terminal as **admusr**.
		2. Execute this command:
		`$ sudo irepstat –m`
		Output:
		`-- Policy 0 ActStb [DbReplication] ------------------------------`
		`RDU06-MP1 -- Stby`
		`BC From RDU06-SO1 Active 0 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`

19. ☐	**NOAM VIP GUI**: Verify the database states	1. Navigate to **Status and Manager > Database**.  2. Verify the OAM Max HA Role is either **Active** or **Standby** for NOAM and SOAM; Application Max HA Role for MPs is **Active**; and status is **Normal**. 

Procedure 4. Recovery Scenario 4

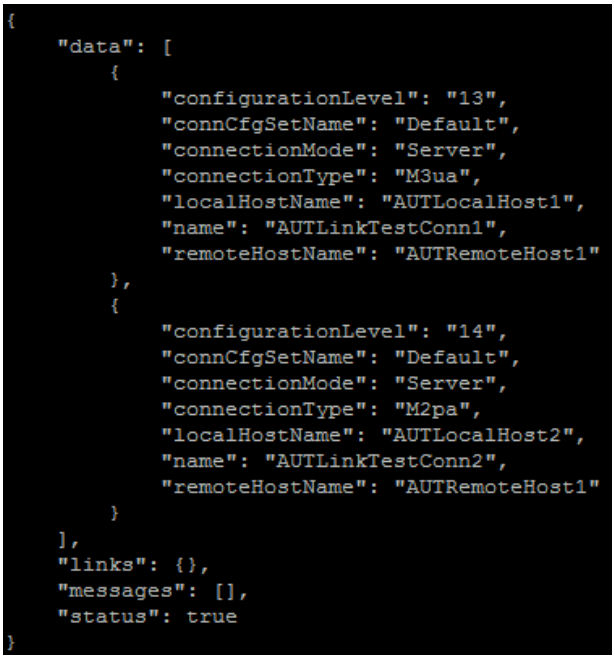
20. ☐	**NOAM VIP GUI**: Verify the HA status	1. Navigate to **Status and Manage > HA**.  2. Select the row for all of the servers. 3. Verify the HA Role is either **Active** or **Standby**. **Main Menu: Status & Manage -> HA** Filter*
21. ☐	**SOAM VIP GUI**: Verify the local node information	1. Navigate to **Diameter > Configuration > Local Node**.  2. Verify all the local nodes are shown.

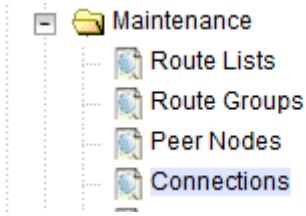
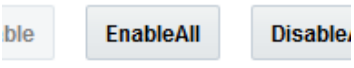
Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role	Mate Hostname List	Network Element	Server Role
SO1	Standby	N/A	Active	SO2	SOAM_NE	System OAM
SO2	Active	N/A	Active	SO1	SOAM_NE	System OAM
DAMP1	Active	Active	Active		SOAM_NE	MP
NO1	Active	N/A	Active	NO2	NOAM_NE	Network OAM&P
NO2	Standby	N/A	Active	NO1	NOAM_NE	Network OAM&P

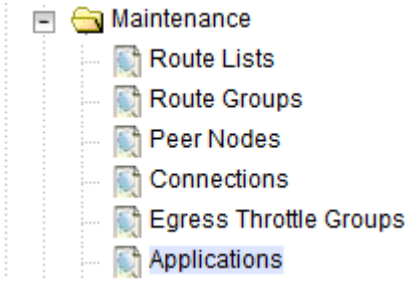
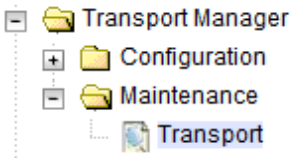
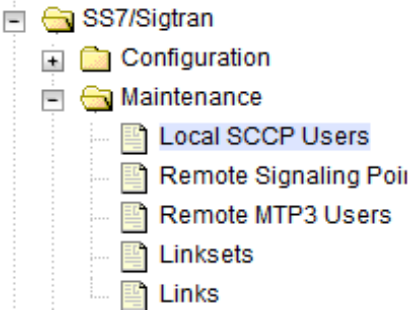
Procedure 4. Recovery Scenario 4		
22. ☐	**SOAM VIP GUI**: Verify the peer node information	1. Navigate to **Diameter > Configuration > Peer Node**.  2. Verify all the peer nodes are shown.
23. ☐	**SOAM VIP GUI**: Verify the connections information	1. Navigate to **Diameter > Configuration > Connections**.  2. Verify all the connections are shown.

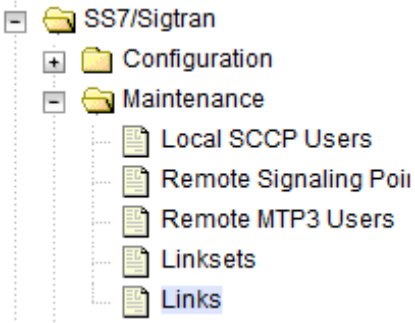
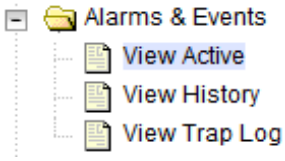
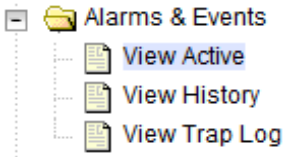
<table>
<tr><th colspan="3">Procedure 4. Recovery Scenario 4</th></tr>
<tr><td>24. ☐</td><td>For vSTP only
SOAM VIP Server Console: Verify the vSTP MP local nodes information (optional)</td><td>1. Log into the SOAM VIP server console as admusr.
2. Execute this command:
<code>[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts</code>
3. Verify output is similar to this:
<pre>{
    "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
}</pre></td></tr>
<tr><td>25. ☐</td><td>For vSTP only
SOAM VIP Server Console: Verify the vSTP MP remote nodes information (optional)</td><td>1. Log into the SOAM VIP server console as admusr.
2. Execute this command:
<code>[admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts</code>
3. Verify output is similar to this:
<pre>{
    "data": [
        {
            "configurationLevel": "12",
            "remoteHostName": "AUTRemoteHost1",
            "remoteHostPort": 4444,
            "remoteHostPriIPAddress": "1.1.1.6",
            "remoteHostSecIPAddress": "1.1.1.7"
        }
    ],
    "links": {},
    "messages": [],
    "status": true
}</pre></td></tr>
</table>

Procedure 4. Recovery Scenario 4		

26. ☐	For vSTP only
	SOAM VIP Server Console: Verify the vSTP MP connections information (optional)
		1. Log into the SOAM VIP server console as **admusr**.
		2. Execute this command:
		`[admusr@SOAM1 ~]$ mmiclient.py /vstp/connections`
		3. Verify output is similar to this:
		  {
		"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
		}

27. ☐	**MP Servers**: Disable SCTP authorization flag	For SCTP connections without DTLS enabled, refer to the **Enable/Disable DTLS** appendix in reference [1]. Execute the procedure on all failed MP servers.
28. ☐	**SOAM VIP GUI**: Enable connections, if needed	1. Navigate to **Diameter > Maintenance > Connections**.  2. Select each connection and click **Enable**. Alternatively, you can enable all the connections by clicking **EnableAll**.  3. Verify the Operational State is **Available**.

Procedure 4. Recovery Scenario 4		
29. ☐	**SOAM VIP GUI**: Enable optional features	1. Navigate to **Diameter > Maintenance > Applications**.  2. Select the optional feature application configured in step 16. 3. Click **Enable**. 
30. ☐	**SOAM VIP GUI**: Re-enable transports, if needed	1. Navigate to **Transport Manager > Maintenance > Transport**.  2. Select each transport and click **Enable**.  3. Verify the Operational Status for each transport is **Up**.
31. ☐	**SOAM VIP GUI**: Re-enable MAPIWF application, if needed	1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.  2. Click **Enable** for the corresponding to MAPIWF Application Name.  3. Verify the SSN Status is **Enabled**.

Procedure 4. Recovery Scenario 4		
32. ☐	**SOAM VIP GUI**: Re-enable links if needed	1. Navigate to **SS7/Sigtran > Maintenance > Links**.  2. Click **Enable** for each link.  3. Verify the Operational Status for each link is **Up**.
33. ☐	**SOAM VIP GUI**: Examine all alarms	1. Navigate to **Alarms & Events > View Active**.  2. Examine all active alarms and refer to the on-line help on how to address them. If needed contact My Oracle Support (MOS).
34. ☐	**NOAM VIP GUI**: Examine all alarms	1. Log into the NOAM VIP, if not already logged in. 2. Navigate to **Alarms & Events > View Active**.  3. Examine all active alarms and refer to the on-line help on how to address them. If needed contact My Oracle Support (MOS)

35. ☐	Restart oampAgent, if needed	***Note:*** ***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.
		1. Establish an SSH session to each server that has the alarm and login as **admusr**.
		2. Execute these commands:
		`$ sudo pm.set off oampAgent`
		`$ sudo pm.set on oampAgent`

Procedure 4. Recovery Scenario 4		
36. ☐	Backup and archive all the databases from the recovered system	Execute DSR Database Backup to back up the configuration databases.

4.1.5 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.

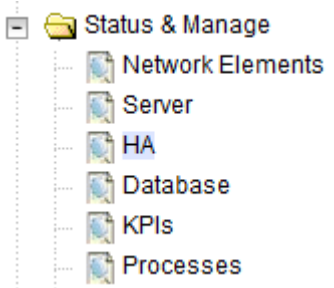
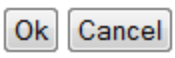
- Recover the base hardware.
- Recover the software.
- The database is intact at the newly active NOAM server and does not require restoration.

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 5. Recovery Scenario 5		
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/apply any workarounds required during this procedure.
2. ☐	Gather required materials	Gather the documents and required materials listed in the Required Materials section.
3. ☐	Switch DR NOAM to primary	Refer to DSR/SDS NOAM Failover User's Guide [2].

Procedure 5. Recovery Scenario 5		
4. ☐	Recover the failed software	For VMWare based deployments: • 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 the procedure to import OVA. b. Procedure 2 **(VMWare Only) Configure NOAM Guests Based on Resource Profile**. • For SOAMs or 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 the procedure to import OVA. b. Procedure 3 **(VMWare Only) Configure Remaining DSR Guests Based on Resource Profile**. For KVM/Openstack based deployments: • 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 the procedure to import OVA. b. Procedure 5 (**KVM/Openstack Only) Configure NOAM Guests Based on Resource Profile**. • For SOAMs or 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 the procedure to import 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]: 1. Procedure 7 **(OVM-S/OVM-M) Import DSR OVA and Prepare for VM Creation**. 2. 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.

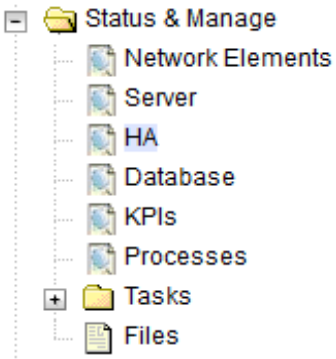
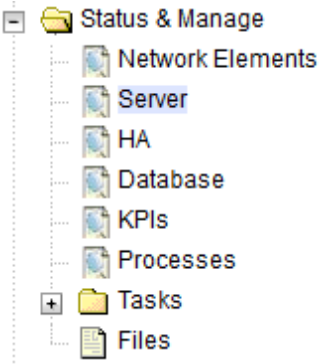
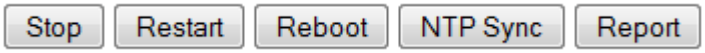
Procedure 5. Recovery Scenario 5		
6. ☐	**DR NOAM VIP GUI**: Login	1. Establish a GUI session on the DR NOAM server by using the VIP IP address of the DR NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 
7. ☐	**DR-NOAM VIP GUI**: Set failed NOAM servers to standby	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Set the Max Allowed HA Role option to **Standby** for the failed NOAM servers. 4. Click **OK**. 

Procedure 5. Recovery Scenario 5		
8. ☐	**DR-NOAM VIP GUI**: Export the initial configuration	1. Navigate **to Configuration > Servers**. 2. Select the failed NOAM server and click **Export** to generate the initial configuration data for that server. 
9. ☐	**DR-NOAM VIP GUI**: Copy configuration file to failed NOAM server	1. Obtain a terminal session to the DR-NOAM VIP, login as **admusr**. 2. Execute this 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`

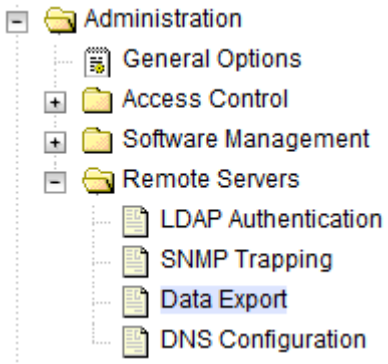
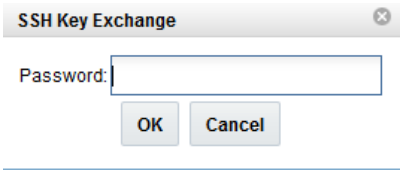
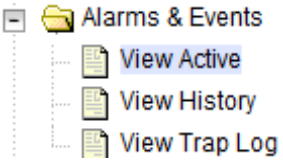
10. ☐	**Recovered NOAM Server**: Verify configuration was called and reboot the server	1. Establish an SSH session to the recovered NOAM server (Recovered_NOAM_xmi_IP_address) and login as **admusr**.
		2. The automatic configuration daemon looks for the file named **TKLCConfigData.sh** in the **/var/tmp** directory, implements the configuration in the file, and asks the user to reboot the server.
		3. 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!`
		4. Reboot the server:
		`$ sudo init 6`
		5. Wait for the server to reboot,

11. ☐	**Recovered NOAM Server**: Verify server health	Execute this command on the failed NOAM server and make sure 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 second failed NOAM server.
13. ☐	**Active NOAM**: Perform key exchange between the active NOAM and recovered servers	1. Establish an SSH session to the active NOAM and login as **admusr**. 2. Perform a keyexchange from the active NOAM to each recovered server using the host names of the recovered NOAMs `$ keyexchange admusr@<Recovered NOAM Server Hostname>`

Procedure 5. Recovery Scenario 5		
14. ☐	**NOAM VIP GUI**: Set HA on recovered servers	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. For each server whose Max Allowed HA Role is set to Standby, set it to **Active**. 4. Click **OK**.
15. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**. 

Procedure 5. Recovery Scenario 5		
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 Feature Activation:** 1. Establish SSH sessions to the all the recovered NOAM servers and login as **admusr**. 2. Execute the **PCA Activation on Standby NOAM Server** procedure on the recovered standby NOAM servers from [3]. 3. Establish SSH session to the recovered active NOAM, login as **admusr**. **For MAP-IWF Activation:** 1. Establish SSH session to the recovered active NOAM and login as **admusr**. 2. Refer [4] to activate Map-Diameter Interworking (MAP-IWF). ***Notes***: • While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored: `iload#31000{S/W Fault}` • 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 has been recovered, refer to the DSR/SDS NOAM Failover User's Guide procedure in [2].

Procedure 5. Recovery Scenario 5		
18. ☐	**NOAM VIP GUI**: Perform key exchange with export server	1. Navigate to **Administration > Remote Servers > Data Export**.  2. Click **SSH Key Exchange** at the bottom of the screen.  3. Type the **Password** and click **OK**. 
19. ☐	**Recovered Servers**: Verify alarms	1. Navigate to **Alarms & Events > View Active**.  2. 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 and C-Level servers.

4.1.6 Recovery Scenario 6 (Database Recovery)

4.1.6.1 Recovery Scenario 6: Case 1

For a partial outage with

- Server having a corrupted database
- Replication channel from parent is inhibited because of upgrade activity or
- Server is in a different release then that of its Active parent because of upgrade activity.
- Verify that the Server Runtime backup files, performed at the start of the upgrade, are present in /var/TKLC/db/filemgmt area in the following format

- Backup.DSR.HPC02-NO2.FullDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2
- Backup.DSR.HPC02-NO2.FullRunEnv.NETWORK_OAMP.20140524_223507.UPG.tar.bz2

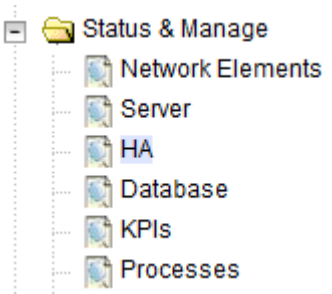
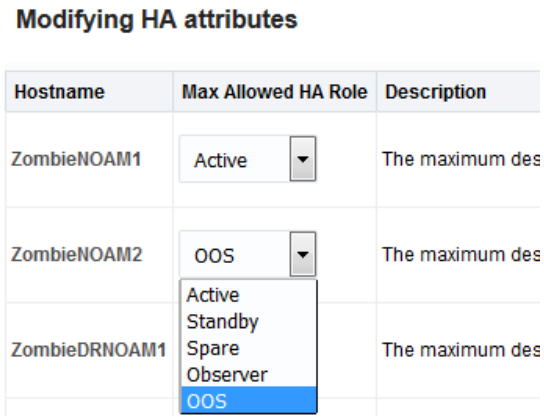
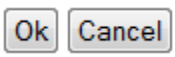
Note: During recovery, the corrupted Database will get replaced by the sever Runtime backup. Any configuration done after taking the backup will not be visible post recovery.

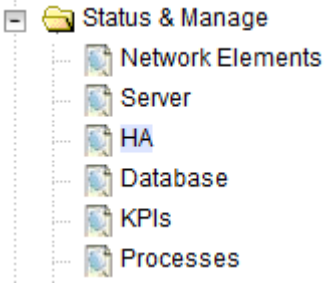
Procedure 6. Recovery Scenario 6 (Case 1)

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 any workarounds required during this procedure.
2. ☐	**Active NOAM**: Set failed servers to OOS	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Set the Max Allowed HA Role option to **OOS** for the failed servers.  4. Click **OK**. 
3. ☐	**Server in Question**: Login and change runlevel to 3	1. Establish an SSH session to the server in question and login as **admusr**. 2. Execute this command to bring the system to runlevel 3: `$ sudo init 3`

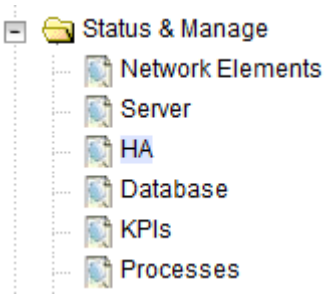
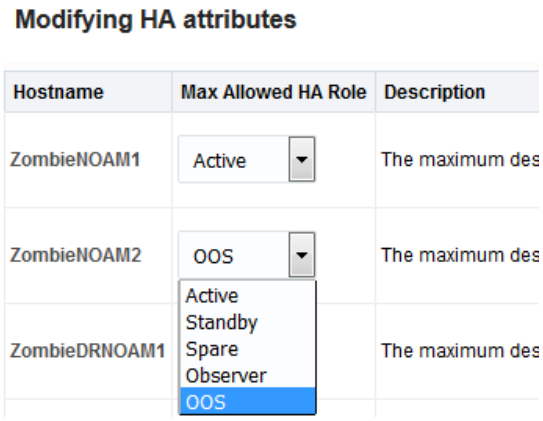
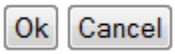
Procedure 6. Recovery Scenario 6 (Case 1)		
4. ☐	**Server in Question**: Recover system	Execute this command and follow the instructions appearing the console prompt: `$ sudo /usr/TKLC/appworks/sbin/backout_restore`
5. ☐	**Server in Question**: Login and change runlevel to 4	Execute this command to bring the system to runlevel 4: `$ sudo init 4`
6. ☐	**Server in Question**: Verify the server	Execute this command to verify if the processes are up and running: `$ sudo pm.getprocs`
7. ☐	**NOAM VIP GUI:** Set failed servers to active	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. For each failed server whose Max Allowed HA Role is set to OOS, set it to **Active**. 4. Click **OK**.
8. ☐	Backup and archive all the databases from the recovered system	Execute DSR Database Backup to back up the configuration databases.

4.1.6.2 Recovery Scenario 6: Case 2

For a partial outage with

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

Procedure 7. Recovery Scenario 6 (Case 2)		
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 Workarounds for Issues Not Fixed in this Release to understand any workarounds required during this procedure.

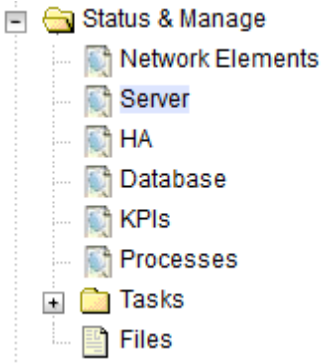
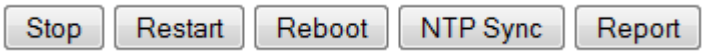
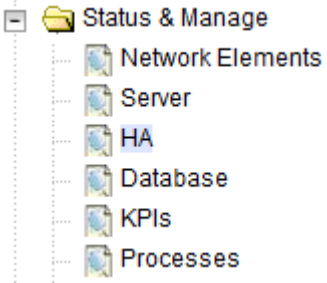
Procedure 7. Recovery Scenario 6 (Case 2)		
2. ☐	**Active NOAM**: Set failed servers to OOS	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Set the Max Allowed HA Role option to **OOS** for the failed servers.  4. Click **OK**. 
3. ☐	**Server in Question**: Login	Establish an SSH session to the server in question and login as **admusr**.

4. ☐	**Server in Question**: Take server out of service	Execute this 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 these commands to take the server to Dbup and start the DSR application:
		`$ sudo bash -l`
		`$ sudo prod.start`

Procedure 7. Recovery Scenario 6 (Case 2)		

6. ☐	**Server in Question**: Verify the server state	1. Verify the processes are up and running:
		`$ sudo pm.getprocs`
		2. Verify replication channels are up and running:
		`$ sudo irepstat`
		3. Verify merging channels are up and running:
		`$ sudo inetmstat`

7. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**. 
8. ☐	**NOAM VIP GUI:** Set failed servers to active	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. For each failed server whose Max Allowed HA Role is set to OOS, set it to **Active**. 4. Click **OK**.
9. ☐	Backup and archive all the databases from the recovered system	Execute DSR Database Backup to back up the configuration databases.

5. Resolve 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 the restoration does not impact security or accessibility.

5.1 Restore a Deleted User

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

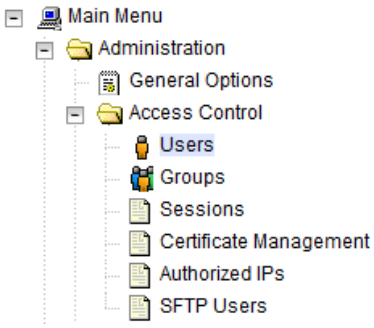
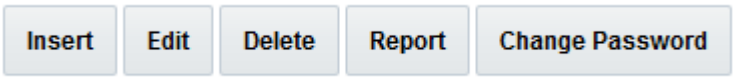
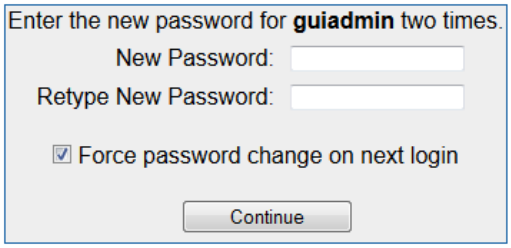
These users were removed before creation of the backup and archive file. They are reintroduced by system restoration of that file.

5.2 Keep a Restored User

Procedure 8. Keep a Restored User		
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 affected before the restoration and notify them that you will reset their password during this maintenance operation.

Procedure 8. Keep a Restored User		
2. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 

Procedure 8. Keep a Restored User

3. ☐	**After Restoration:** Reset User Passwords	1. Navigate to **Administration > Access Control > Users**.  2. Select the user. 3. Click **Change Password**.  4. Type a new password.  5. Click **Continue**.

5.3 Remove a Restored User

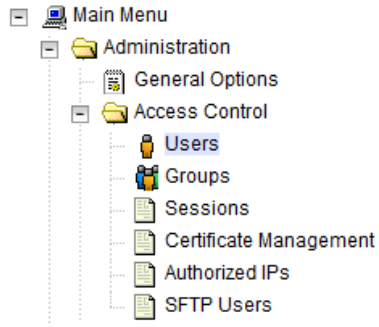
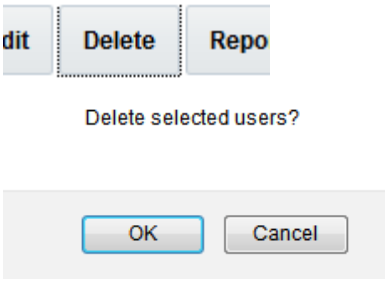
Procedure 9. Remove the Restored User

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. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user:

Procedure 9. Remove the Restored User		
2. ☐	**After Restoration**: Reset user passwords	1. Navigate to **Administration > Access Control > Users**.  2. Select the user. 3. Click **Delete**.  4. Click **OK** to confirm.

5.4 Restore a Modified User

These users have had a password change before creation of the backup and archive file. They are 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 you have access to a user with administrator permissions that is not affected.

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

After Restoration:

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

5.5 Restore an Archive that Does Not Contain a Current User

These users have been created after the creation of the backup and archive file. They are deleted by system restoration of that file.

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

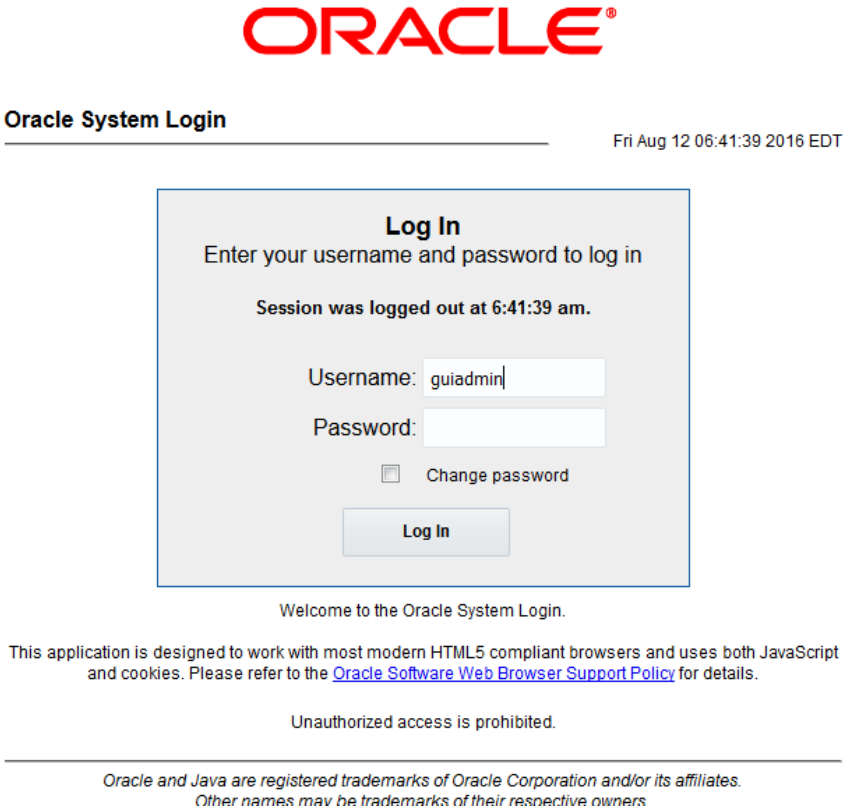
If the user is no longer desired, do not perform any additional steps. The user is permanently removed.

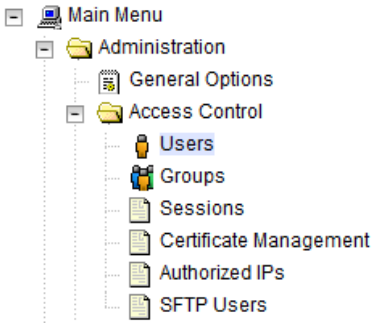
Procedure 10. Restore an Archive that Does Not Contain a Current User

Perform this procedure to remove users that will be restored by system restoration

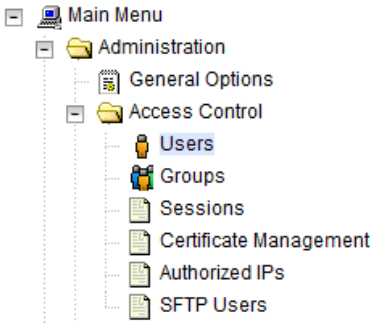
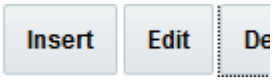
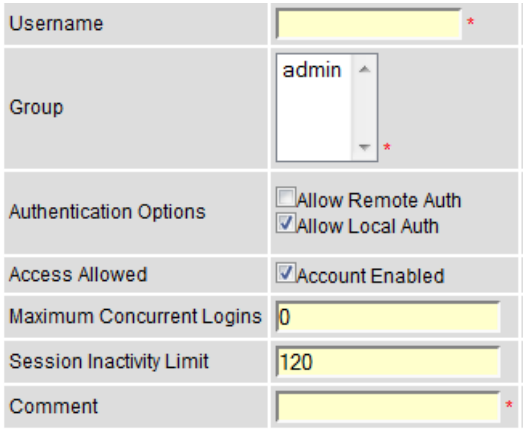
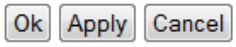
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

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.
2. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 

Procedure 10. Restore an Archive that Does Not Contain a Current User		
3. ☐	**Before Restoration**: Record user settings	1. Navigate to **Administration > Access Control > Users**.  2. Under each affected user, record the following: • Username • Account status • Remote Auth • Local Auth • Concurrent Logins Allowed • Inactivity Limit • Comment • Groups

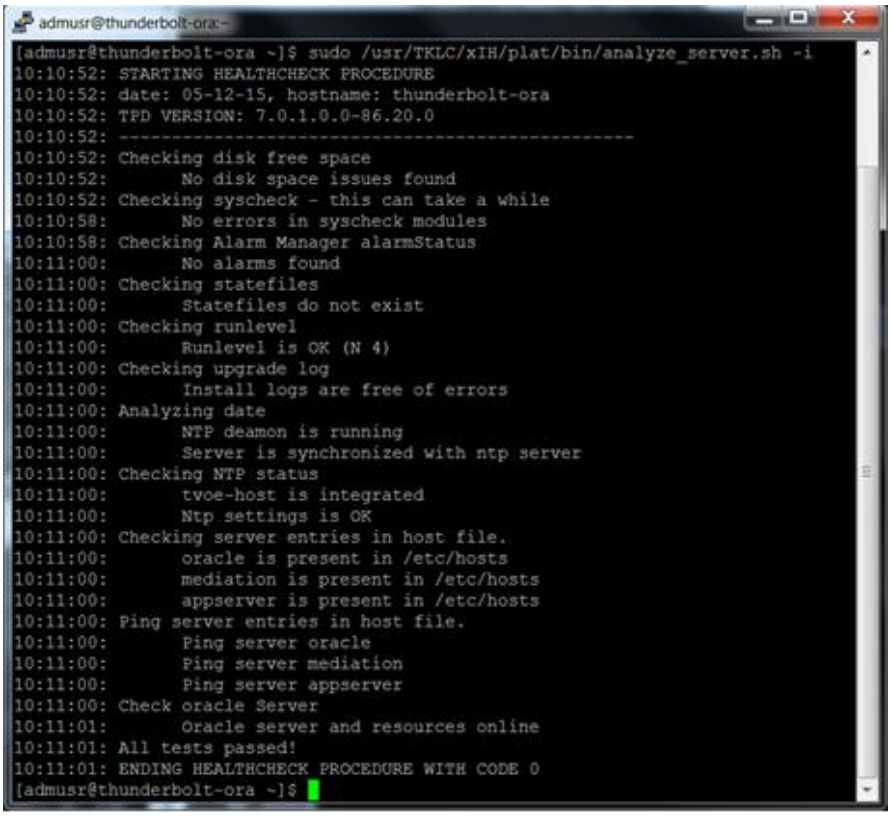
Procedure 10. Restore an Archive that Does Not Contain a Current User		
4. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 

Procedure 10. Restore an Archive that Does Not Contain a Current User		
5. ☐	**After Restoration:** Recreate affected user and required group	1. Navigate to **Administration > Access Control > Users**.  2. Click **Insert**.  3. Recreate the user using the data collected from step 3.  4. Click **OK**. 
6. ☐	**After Restoration**: Repeat for additional users	Repeat step 5. to recreate additional users.
7. ☐	**After Restoration**: Reset the passwords	See Procedure 8 for resetting passwords for a user.

6. IDIH Disaster Recovery

Procedure 11. IDIH Disaster Recovery Preparation		
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 and login as **admusr**.

Procedure 11. IDIH Disaster Recovery Preparation

2. ☐	**Oracle Guest**: Perform database health check	Perform a database health check: `$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i` Output:  ***Note:*** If this step fails, re-install using these procedures from reference [1]: **For VMware based deployments:** • Section 5.6 procedure 34, **(VMware Only) Create iDIH Oracle, Mediation and Application VMs**. • Section 5.9 procedures 37 – 40, **Configure iDIH Virtual Machines**. **For KVM/Openstack based deployments:** • Section 5.7 procedure 35, **(KVM/OpenStack only) Create iDIH Oracle, Mediation and Application VMs**. • Section 5.9 procedures 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 OVAs and Create and Configure a VM for Each**. • Section 5.9 procedures 37 – 40, **Configure iDIH Virtual Machines**.

Procedure 12. IDIH Disaster Recovery (Re-Install Mediation and Application Servers)		
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 and mediation VMs	Execute these procedures 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.** **For OVM-S/OVM-M based deployments:** • Procedure 36, **(OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for Each**.
2. ☐	Configure iDIH VM networks	Execute procedure 37, **Configure iDIH VM Networks**, from [1] to configure the VM networks on the Application and Mediation VMs only.
3. ☐	Configure VMs	Execute procedure 38, **Run Post Installation scripts on iDIH VMs**, steps 3 – 7, from [1]:
4. ☐	Integrate into DSR (optional)	If integration is needed execute the following procedure 41, **Integrate iDIH into DSR**, from [1]

Appendix A. DSR Database Backup

Procedure 13. Back Up the Provision and Configuration Data

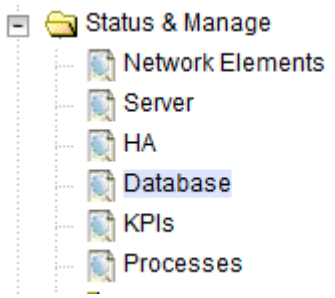
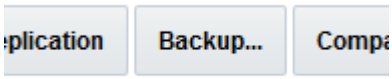
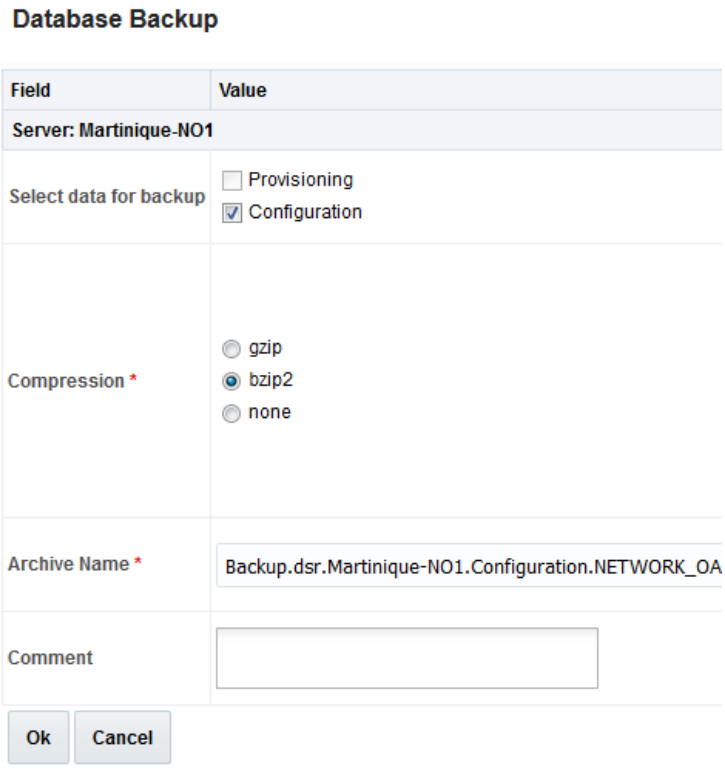
The intent of this procedure is to back up the provision and configuration information from an NOAM or SOAM server after the disaster recovery is complete

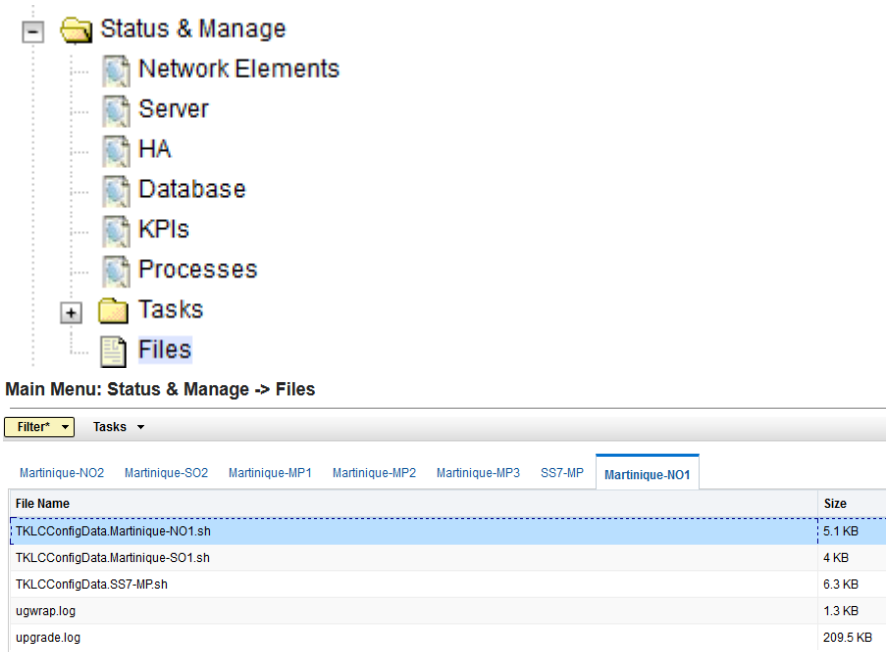
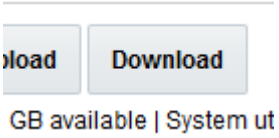
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.

1. ☐	**NOAM/SOAM VIP**: Login	1. Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM/SOAM_VIP_IP_Address>` 3. Login as the **guiadmin** user: 

Procedure 13. Back Up the Provision and Configuration Data

2. ☐	**NOAM/SOAM VIP:** Back up configuration data for the system	1. Navigate to **Status and Manage > Database**.  2. Select the active NOAM server and click **Backup**.  3. Make sure that the **Configuration** checkbox is marked.  4. Type a filename for the backup and click **OK**.

Procedure 13. Back Up the Provision and Configuration Data		
3. ☐	**NOAM/SOAM VIP**: Verify the backup file exists	1. Navigate to **Status and Manage > Files**.  2. Select the active NOAM or SOAM tab. 3. The files on this server display. Verify the existence of the backup file.
4. ☐	**NOAM/SOAM VIP**: Download the file to a local machine	1. From the previous step, select the backup file. 2. Click **Download**.  3. Click **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 located in case of system disaster recovery.
6. ☐	Backup active SOAM	Repeat steps 2. through 5. to back up the active SOAM.

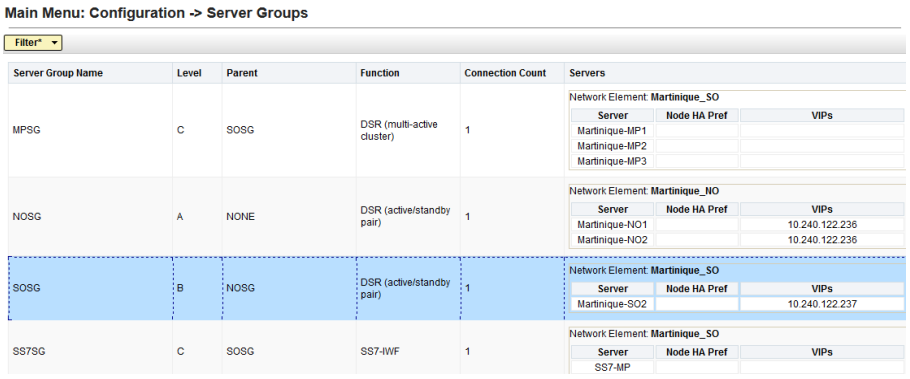
Appendix B. Inhibit A and B Level Replication on C-Level Servers

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

This procedure inhibits 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	Log into the active NOAM server using SSH as **admusr**.
2. ☐	**Active NOAM**: Inhibit replication on all C-level servers	Execute this 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 navigating to **Configuration > Server Groups**. This snapshot shows more details. 

3. ☐	**Active NOAM**: Verify replication has been Inhibited	After inhibiting replication on MP(s), no alarms on the GUI should display about replication on MP being disabled.
		Verify replication inhibition on MPs by analyzing NodeInfo output. The InhibitRepPlans field for all MP servers for the selected site, for example, Site SO_HPC03 is set as **A B**.
		Execute this command:
		`$ sudo iqt NodeInfo`
		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 15. Un-Inhibit A and B Level Replication on C-Level Servers

This procedure un-inhibits 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	Log into the active NOAM server using SSH as **admusr**.
2. ☐	**Active NOAM:** Un-Inhibit replication on all C-level servers	Execute this 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 navigating to **Configuration > Server Groups**. This snapshot shows 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 / Node HA Pref / VIPs): Martinique-MP1, Martinique-MP2, Martinique-MP3 NOSG — A — NONE — DSR (active/standby pair) — 1 — Network Element: Martinique_NO (Server / Node HA Pref / VIPs): 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 / Node HA Pref / VIPs): Martinique-SO2 10.240.122.237 SS7SG — C — SOSG — SS7-IWF — 1 — Network Element: Martinique_SO (Server / Node HA Pref / VIPs): SS7-MP

3. ☐	**Active NOAM**: Verify replication has been Inhibited	After un-inhibiting replication on MP(s), no alarms on the GUI should display about replication on MP being disabled.
		Verify replication un-inhibition on MPs by analyzing NodeInfo output. InhibitRepPlans field for all MP servers for the selected site, for example, Site SO_HPC03 is set as empty.
		Execute this command:
		`$ sudo iqt NodeInfo`
		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 16. Inhibit A and B Level Replication on C-Level Servers

This procedure inhibits 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	Log into the active NOAM server using SSH as **admusr**.

2. ☐	**Active NOAM**: Inhibit replication on all C-level servers	Execute the script from **/usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh**, if available.
		If the **/usr/TKLC/dsr/tools/** path does not have the **InhibitReplicationToCLevel.sh** script, then use this manual command.
		`/usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh --replication=inhibit --SO_SG_Name=<SOAM server group name>`
		Alternatively to the above script, if the script is not 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_NAME is the name of the server group found by logging into the active NOAM GUI and navigating to **Configuration > Server Groups**.
		This snapshot shows more details.
		 

Procedure 16. Inhibit A and B Level Replication on C-Level Servers		

3. ☐	**Active NOAM**: Verify replication has been inhibited	After executing above steps to inhibit replication on MP(s), no alarms on GUI should display about replication on MP being disabled.
		Verify replication inhibition on MPs by analyzing NodeInfo output. The InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO_SG is set as **A B**.
		Execute this command::
		`$ sudo iqt NodeInfo`
		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 17. Un-Inhibit A and B Level Replication on C-Level Servers		
This procedure un-inhibits 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	Log into the active NOAM server using SSH as **admusr**.

Procedure 17. Un-Inhibit A and B Level Replication on C-Level Servers

2. ☐	**Active NOAM**: Un-Inhibit replication on all C-level servers	Execute the script from **/usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh**, if available.
		If the **/usr/TKLC/dsr/tools/** path does not have the **InhibitReplicationToCLevel.sh** script, then use this manual command.
		`/usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh --replication=allow --SO_SG_Name=<SOAM server group name>`
		Alternatively to the above script, if the script is not 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 is the name of the server group found by logging into the active NOAM GUI and navigating to **Configuration > Server Groups**.
		This snapshot shows more details.
		 

Procedure 17. Un-Inhibit A and B Level Replication on C-Level Servers		

3. ☐	**Active NOAM**: Verify replication has been un-inhibited	After un-inhibiting replication on MP(s), no alarms on the GUI should display about replication on MP is disabled.
		Verify replication inhibition on MPs by analyzing NodeInfo output. The Un-InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO_SG is set as <**blank>**.
		Execute this 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 18. Backup Directory		
This procedure checks and creates a 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 exists	1. Execute this command an active NOAM/SOAM server console (accessed using the VIP) and compare the output.
		`$ cd /var/TKLC/db/filemgmt/`
		`$ ls -ltr`
		2. Look for the backup directory in the output.
		3. Make sure the directory is already created with correct permission. The directory looks like this:
		`drwxrwx--- 2 awadmin awadm 4096 Dec 19 02:15 backup`
		4. If the directory is already there with correct permissions, then skip steps 2 and 3.
		5. If directory does not have the correct permissions, then go to step 3.

Procedure 18. Backup Directory		

2. ☐	**NOAM/SOAM VIP Console**: Create backup directory	1. Go to the backup directory location.
		`cd /var/TKLC/db/filemgmt/`
		2. Create backup directory.
		`$ mkdir backup`
		3. Verify directory has been created.
		`$ ls -ltr /var/TKLC/db/filemgmt/backup`
		Note: A **No such file or directory** error message should not display. The directory should show as empty with the total as 0 for content.

3. ☐	**NOAM/SOAM VIP Console**: Change permissions of backup directory	1. Verify directory has been created.
		`$ ls -ltr /var/TKLC/db/filemgmt/backup`
		Note: A **No such file or directory** error message should not display. The directory should show as empty with the total as 0 for content.
		2. Change permissions for the backup directory.
		`$ chmod 770 /var/TKLC/db/filemgmt/backup`
		3. Change ownership of backup directory.
		`$ sudo chown –R awadmin:awadm /var/TKLC/db/filemgmt/backup`
		4. Directory displays as follows:
		`drwxrwx--- 2 awadmin awadm 4096 Dec 22 02:15 backup`

4. ☐	**NOAM/SOAM VIP Console**: Copy the backup file to the backup directory	1. Copy the backup file to the backup directory.
		`$ cp BACKUPFILE /var/TKLC/db/filemgmt/backup`
		2. Change permissions of files in the backup directory.
		`$ chmod 666 Backup.*`
		3. Change ownership of files in the 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 are 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, 365 days a year.

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.

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.
2. Click **Industries**.
3. 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.
4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release displays.
5. 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.