Oracle® Communications

Diameter Signaling Router

Cloud Disaster Recover Guide

Release 8.2

E88974 Revision 01

March 2018

Oracle Communications Diameter Signaling Router Cloud Disaster Recover Guide, Release 8.2

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

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

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

Change History

Date	Version	Author	Description	Approved (Yes/No)
09/07/2017	1	Kawal Sapra	Initial Release	No
12/25/2017	2	Kawal Sapra	Bug 27294758 fix	No
01/02/2018	3	Kawal Sapra	Review comments	No
01/10/2018	4	Kawal Sapra	Approved for 8.2	Yes
04/01/2018	5	J. Carlino	Format, Edit, and Post to OTN	Yes

Table of Contents

List of Tables

List of Figures

List of Procedures

1. Introduction

This document is a guide to describe procedures used to execute disaster recovery (DR) for Diameter Signaling Router (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 may also need to be recovered, for example, SDS and IDIH.

Note: Note that failures can happen from the host or Infrastructure level. 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 8.2 Cloud Installation Guide

[2] DSR/SDS 8.2 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
DR	Disaster Recovery
DSR	Diameter Signaling Router
ESXi	Elastic Sky X Integrated
FABR	Full Address Based Resolution
iDIH	Integrated Diameter Intelligence Hub
IPFE	IP Front End
IWF	Inter Working Function
NAPD	Network Architecture Planning Diagram
NOAM	Network Operations, Administration & Maintenance
OS	Operating System
OVA	Open Virtualization Appliance
OVM-M	Oracle Virtual Machine Manager
OVM-S	Oracle Virtual Machine Server

Acronym	Definition
PCA	Policy and Charging Application
RBAR	Range Based Address Resolution
SNMP	Simple Network Management Protocol
SOAM	Systems Operations, Administration & Maintenance
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 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	Documents
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. Installation Overview

The DSR disaster recovery procedure falls into the categories. It is primarily dependent on the state of the NOAM servers and SOAM servers.

Table 4. Recovery Scenarios

Category	When to Use
Recovery of the entire network from a total outage 4.1 Recovery Scenario 1 — Complete Server Outage	• All NOAM servers failed • All SOAM servers failed • 1 or more MP servers failed
Recovery of one or more servers with at least one NOAM server intact Recovery Scenario 2 — Partial Server Outage with One NOAM Server Intact and ALL 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 4.5 Recovery Scenario 5 — Both 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 4.6 Recovery Scenario 6 — Database Recovery	• Server has a corrupted database
4.6 Recovery Scenario 6 — Database Recovery — Case 1	• Server is intact • Database gets corrupted on the server • Replication is occurring to the server with corrupted database
4.7 Recovery Scenario 6 — Database Recovery — Case 2	• Server is intact • Database gets corrupted on the server • Latest Database backup of the corrupt server is NOT present • Replication is inhibited (either manually or because of Comcol upgrade barrier)

Executing a disaster recovery procedure depends on the failure conditions in the network. The severity of the failure determines the recovery scenario for the network. Use Table 4. Recovery Scenarios 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 1

Scenario:

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

This is the worst case scenario where all the servers in the network have suffered complete software failure. The servers are recovered using OVA images then restoring database backups to the active NOAM and SOAM servers.

Database backups will be taken from customer offsite backup storage locations (assuming these were performed and stored offsite prior to the outage). If no backup files are available, the only option is to rebuild the entire network from scratch. The network data must be reconstructed from whatever sources are available, including entering all data manually.

2.2 Partial Server Outage with One NOAM Server Intact and Both SOAMs Failed — Recovery Scenario 2

Scenario:

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

This case assumes that at least one NOAM servers intact. All SOAM servers have failed and are recovered using OVA images. Database is restored on the SOAM server and replication will recover the database of the remaining servers.

2.3 Partial Server Outage with Both NOAM Servers Failed and One SOAM Server Intact — Recovery Scenario 3

Scenario:

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

Database is restored on the NOAM and replication will recover the database of the remaining.

2.4 Partial Server Outage with NOAM and One SOAM Server Intact — Recovery Scenario 4

Scenario:

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

The simplest case of disaster recovery is with at least one NOAM and at least one SOAM servers intact. All servers are recovered using base recovery of software. Database replication from the active NOAM and SOAM servers will recover the database to all servers.

2.5 Partial Server Outage with Corrupt Database

Case 1: Database is corrupted, replication channel is inhibited (either manually or because of Comcol upgrade barrier) and database backup is available.

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

3. Procedure Overview

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

3.1 Required Materials

The following items are needed for disaster recovery:

1. A hardcopy of this document and hard copies 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 hard copy 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 Installation Overview.
2. Read and review the content in this document.
3. Gather required materials in section 3.1 Required Materials.
4. From the failure conditions, determine the Recovery Scenario and procedure to follow (using Figure 1. Determine Recovery Scenario).
5. Execute appropriate recovery procedures (listed in section 4 Disaster Recovery Procedure).

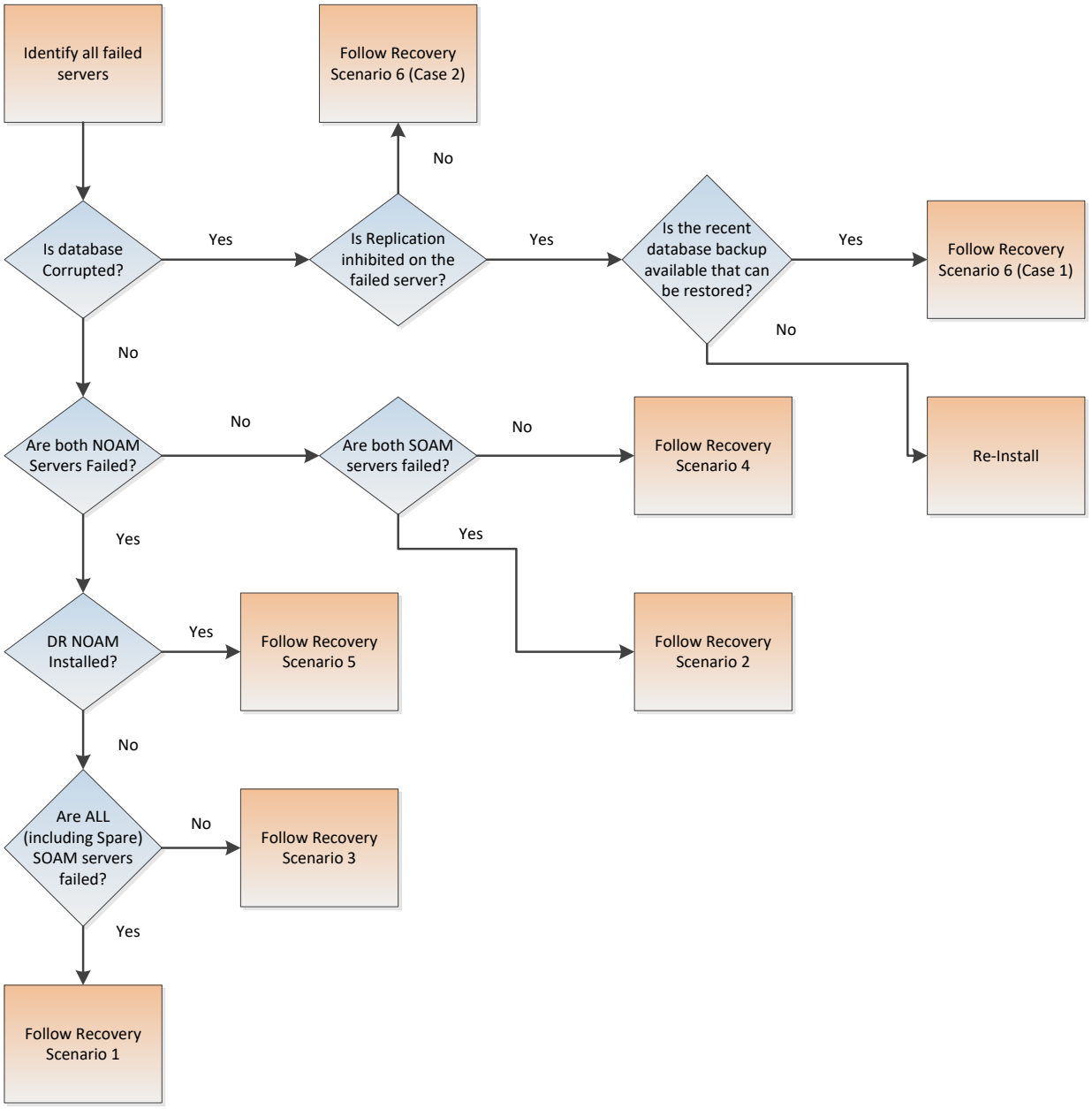


Figure 1. Determine Recovery Scenario

4. Disaster Recovery Procedure

!!WARNING!!

Contact My Oracle Support (MOS) before executing this procedure to ensure the proper recovery planning is performed.

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

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 the disaster, it may be necessary to deviate from the documented process.

Disaster recovery requires configuring the system as it was before the disaster and restoring operational information. There are eight (8) distinct procedures to choose from depending on the type of recovery needed. Only one of these should be followed (not all).

!!WARNING!!

When you need to restore the database backup for NOAM and SOAM servers in any of the recovery scenarios, the backup directory may not exist in the system since it is in DRed.

In this case, refer to Appendix F Check and Create Backup Directory for issues not fixed in this release for the steps to check and create the backup directory.

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

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

4.1 Recovery Scenario 1 — Complete Server Outage

For a complete server outage, NOAM servers are recovered using recovery procedures for software and then executing a database restore to the active NOAM server. All other servers are recovered using recovery procedures for software.

Database replication from the active NOAM server will recover the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual detailed steps are in Procedure 1. The major activities are summarized as follows:

- Recover base software for all VMs
  - Recover the **virtual machines** hosting the NOAMs and SOAMs
  - Recover the **active NOAM** server by recovering the NOAMs base software
  - Recover the NOAM database
  - Reconfigure the application
- Recover the **standby NOAM** server by recovering base software. For a non-HA deployment, this can be skipped
  - Reconfigure the DSR application

- Recover all SOAM and MP servers by recovering software. In a non-HA deployment, the standby/spare SOAM servers can be skipped
  - Recover the SOAM database
  - Reconfigure the DSR Application
  - Reconfigure the signaling interface and routes on the MPs. The DSR software automatically reconfigures 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

S T E P #	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. ☐	Workaround	Refer to Appendix F to Check and Create Backup Directory.
2. ☐	Gather required materials	Gather the documents and required materials listed in section 3.1 Required Materials.
3. ☐	Recover the failed software	**For VMWare based deployments**: 1. For NOAMs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 2 (VMWare Only) Configure NOAM Guests Based On Resource Profile 2. For SOAMs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile 3. For failed MPs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile **For KVM/OpenStack based deployments**: 1. For NOAMs, execute the following procedures from reference [1]:

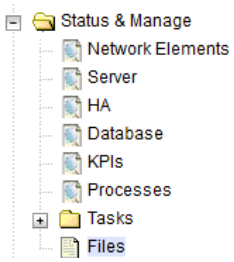
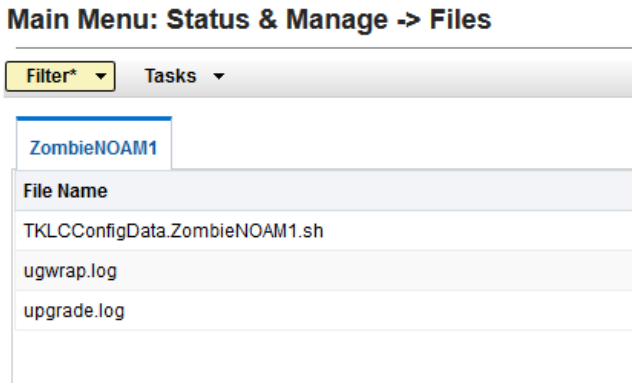
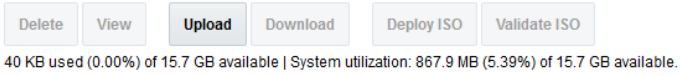
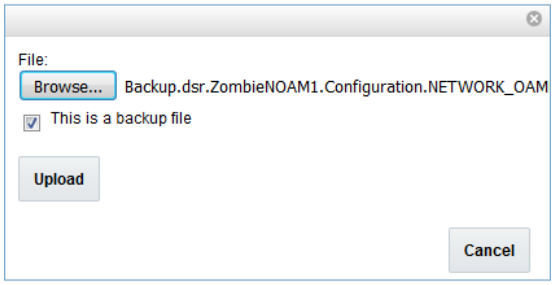
Procedure 1. Recovery Scenario 1

		a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 5 (KVM/OpenStack Only) Configure NOAM Guests Based On Resource Profile 2. For SOAMs, execute the following procedures from reference [1]: a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile 3. For failed MPs, execute the following procedures from reference [1]: a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this 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**: 1. Execute the following procedures from reference [1]: a. Procedure 7 (OVM-S/OVM-M) Import DSR OVA and Prepare for VM creation b. Procedure 8 (OVM-S/OVM-M) Configure each DSR VM While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs).
4. ☐	Obtain latest database backup and network configuration data	1. Obtain the most recent database backup file from external backup sources (for example, file servers) or tape backup sources. 2. From required materials list in section 3.1 Required Materials; use site survey documents and Network Element report (if available) to determine network configuration data.
5. ☐	Execute DSR installation procedure for the first NOAM	Verify the network data for network elements. ***Note***: Use the backup copy of network configuration data and site surveys (Step 2). • Execute Configure the First NOAM NE and Server from reference [1]. • Execute Configure the NOAM Server Group from reference [1].

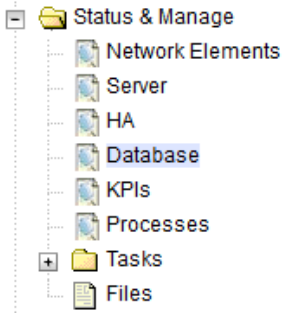
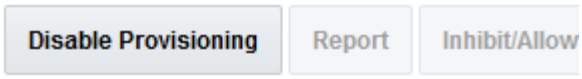
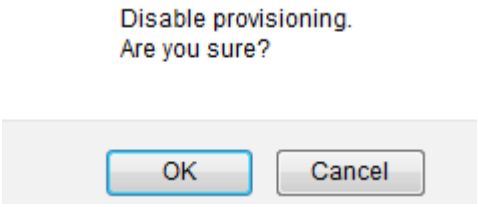
Procedure 1. Recovery Scenario 1

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

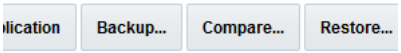
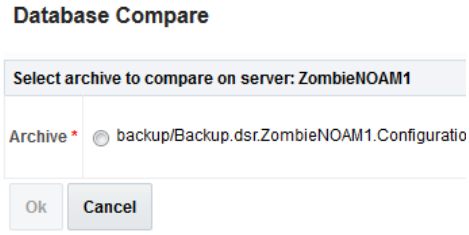
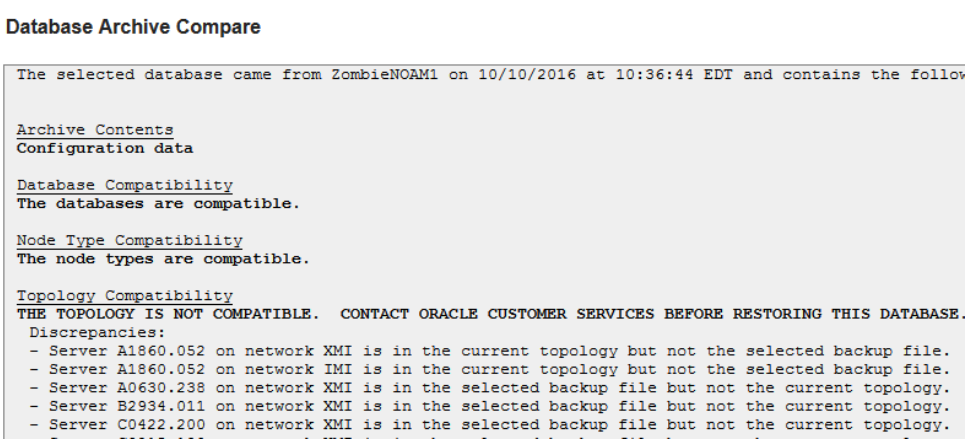
Procedure 1. Recovery Scenario 1

7. ☐	**NOAM GUI**: Upload the backed up database file	1. Navigate to **Status & 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. Check **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.

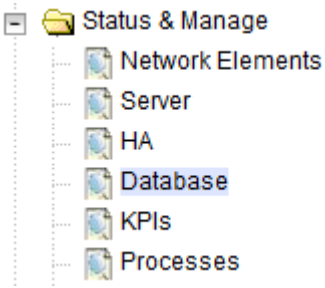
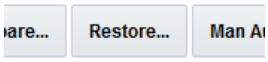
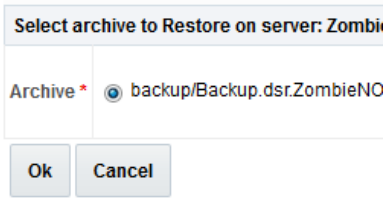
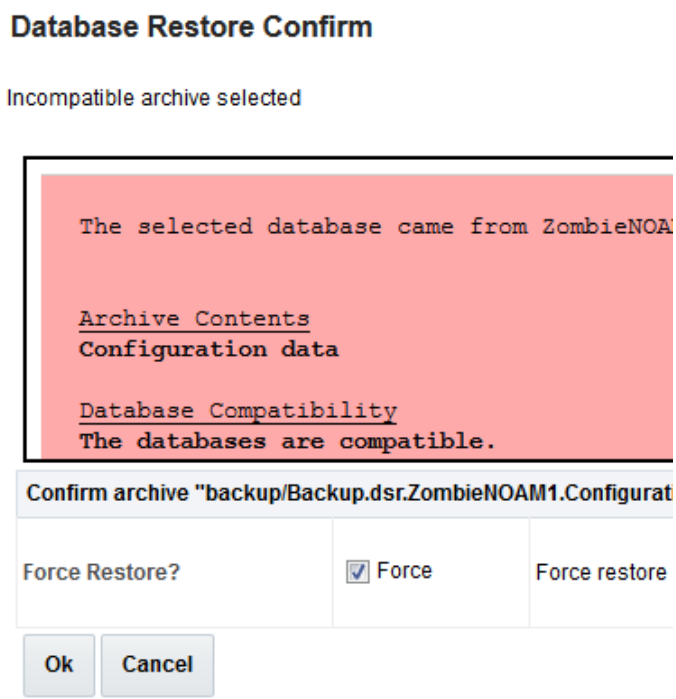
Procedure 1. Recovery Scenario 1

8. ☐	**NOAM GUI**: Disable provisioning	1. Navigate to **Status & Manage > Database**.  2. Click **Disable Provisioning**.  3. A confirmation window displays. Click **OK** 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 Topology Compatibility and possibly User compatibility (due to authentication) display. These warnings are expected. If these are the only mismatches, proceed; otherwise, stop and contact My Oracle Support (MOS) to ask for assistance.  ***Note***: Archive Contents and Database Compatibilities must be the following: **Archive Contents**: Configuration data. **Database Compatibility**: The databases are compatible. ***Note***: The following is expected output for Topology Compatibility Check since we are restoring from an existing backed up database to a database with just one NOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. ***Note***: We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility. 4. If the verification is successful, click **Back**.

Procedure 1. Recovery Scenario 1

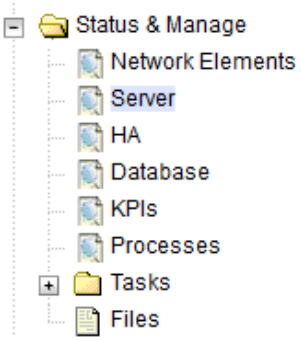
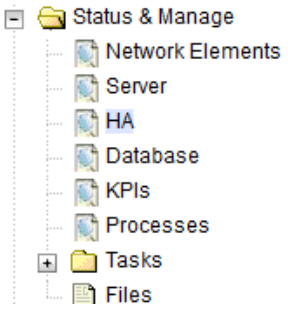
10. ☐	**Active NOAM**: Restore the database	1. From **Status & Manage > Database**.  2. Select the **Active NOAM** server and click **Restore**.  3. Select the proper backup provisioning and configuration file.  4. Click **OK**.  5. If you get errors related to the warnings highlighted in the previous step, that is expected. If no other errors are displayed, mark the **Force** checkbox as shown above and Click **OK** to proceed with the DB restore. ***Note***: After the restore has started, the user is logged out of XMI NO GUI since the restored topology is old data.

Procedure 1. Recovery Scenario 1

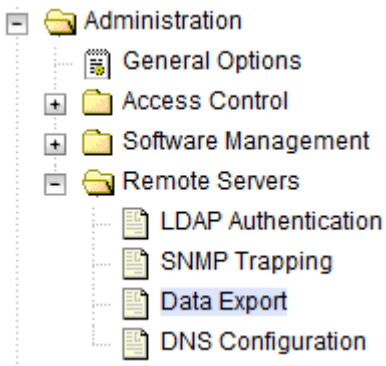
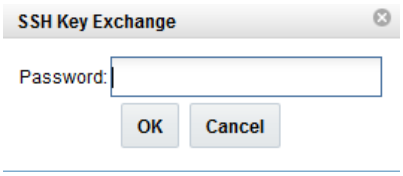
11. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 
12. ☐	**NOAM VIP GUI**: Monitor and confirm database restoral	1. 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). ***Note***: Do not pay attention to alarms until all the servers in the system are completely restored. ***Note***: The Configuration and Maintenance information is in the same state it was when backed up during initial backup.
13. ☐	**Active NOAM**: Login	Log into the recovered active NOAM using SSH terminal as **admusr** user.
14. ☐	**NOAM VIP GUI**: Recover standby NOAM	Install the second NOAM server by executing these procedures from reference [1]: • Execute Configure the Second NOAM Server, steps 3-5 and 7 • Execute Configure the NOAM Server Group, step 4

Procedure 1. Recovery Scenario 1

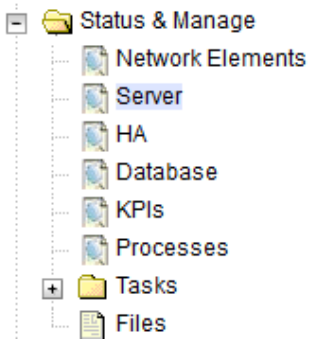
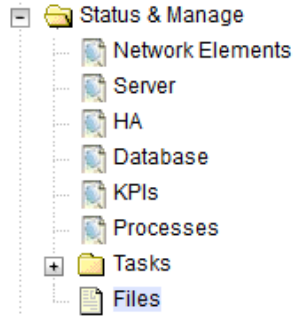
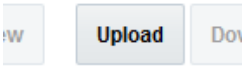
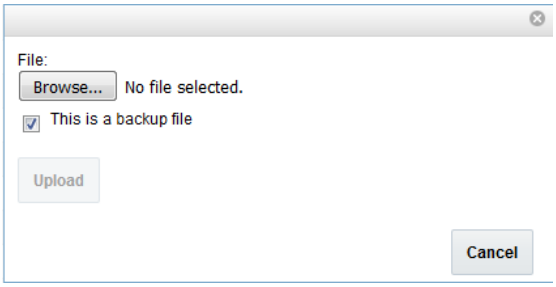
15. ☐	**Active NOAM:** Correct the RecognizedAuthority table	1. Establish an SSH session to the active NOAM and login as **admusr**.
		2. Execute the following command:
		`$ sudo top.setPrimary`
		`- Using my cluster: A1789`
		`- New Primary Timestamp: 11/09/15 20:21:43.418`
		`- Updating A1789.022: <DSR_NOAM_B_hostname>`
		`- Updating A1789.144: <DSR_NOAM_A_hostname>`

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

Procedure 1. Recovery Scenario 1

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. ☐	**NOAM VIP GUI**: Stop replication to the C-level servers of this site 	**!!Warning!!** Before continuing this procedure, replication to C-level servers at the SOAM site being recovered MUST be inhibited. Failure to inhibit replication to the working C-level servers results in the database being destroyed! If the spare SOAM is also present in the site and lost, execute Appendix A 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 C Inhibit A and B Level Replication on C-level Servers to inhibit replication to working C-level servers before continuing.
20. ☐	Recover active SOAM server	Install the SOAM servers by executing Configure the SOAM Servers, steps 1 and 3-7 from reference [1]. ***Note***: Wait for the server to reboot.

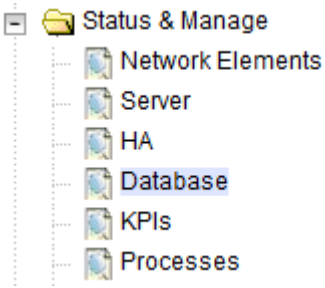
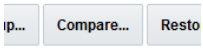
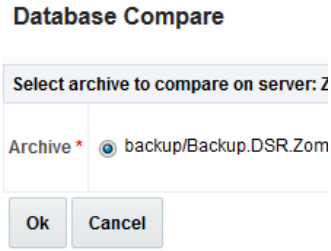
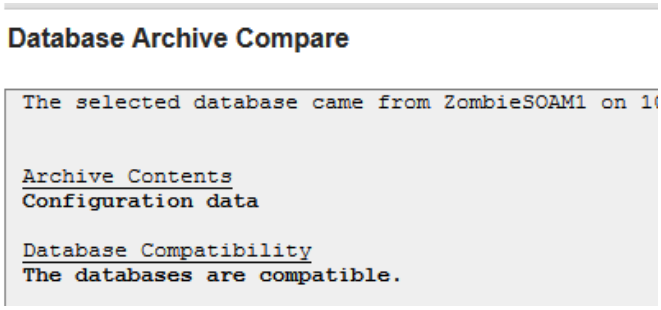
Procedure 1. Recovery Scenario 1

21. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered active SOAM server and click **Restart**. 
22. ☐	**NOAM VIP GUI**: Upload the backed up SOAM database file	3. Navigate to **Status & Manage > Files**.  4. Select the active SOAM server tab. Click **Upload** and select the file **SO Provisioning and Configuration** file backed up after initial installation and provisioning.  5. Click **Browse** and locate the backup file. 6. Check This is a backup file checkbox. 7. Click **Upload**.  The file takes a few seconds to upload depending on the size of the backup data.

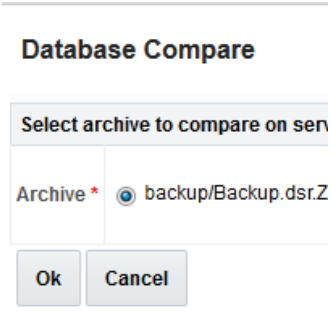
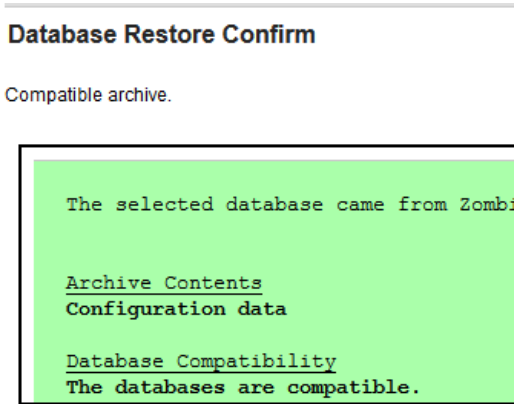
Procedure 1. Recovery Scenario 1

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

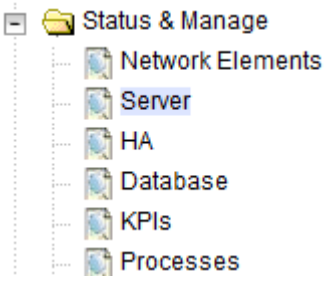
Procedure 1. Recovery Scenario 1

24. ☐	**Recovered SOAM GUI**: Verify the archive contents and database compatibility	1. Navigate to **Status & 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 22. of this procedure.  4. **Verify** the output window matches the screen below.  ***Note***: Archive Contents and Database Compatibilities must be the following: **Archive Contents**: Configuration data. **Database Compatibility**: The databases are compatible. ***Note***: The following is expected output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM: **Topology Compatibility** The topology should be compatible minus the nodeID. ***Note***: We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in topology compatibility. 5. If the verification is successful, click **Back**.

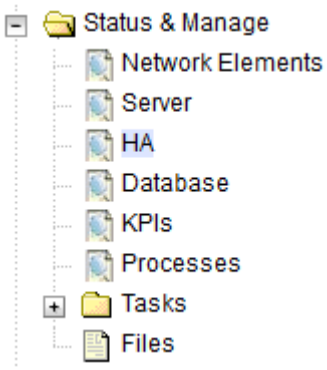
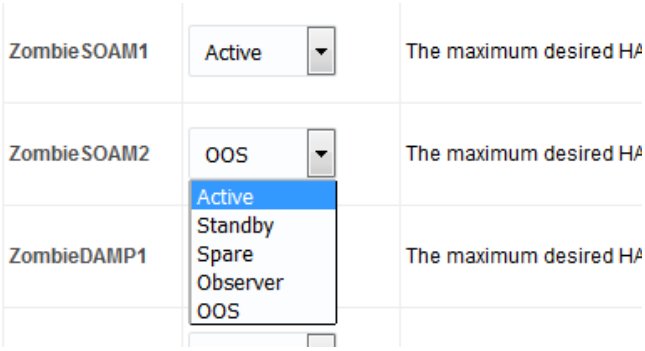
Procedure 1. Recovery Scenario 1

25. ☐	**Recovered SOAM GUI**: Restore the database	1. Select the **Active SOAM** server and click **Restore**. 2. Select the proper back up provisioning and configuration file.  3. Click **OK**. The following confirmation screen displays.  4. If you receive an error for Node Type Compatibility, that is expected. If no other errors are displayed, mark the **Force** checkbox and click **OK** to proceed with the DB restore. ***Note***: After the restore has started, the user is logged out of XMI SOAM GUI since the restored Topology is old data.
26. ☐	**Recovered SOAM GUI**: Monitor and confirm database restoral	Wait for **5-10 minutes** for the system to stabilize with the new topology: Monitor the Info tab for **Success**. This indicates the restore is complete and the system is stabilized. ***Note***: Do not pay attention to alarms until all the servers in the system are completely restored. ***Note***: The Configuration and Maintenance information is in the same state it was when backed up during initial backup.

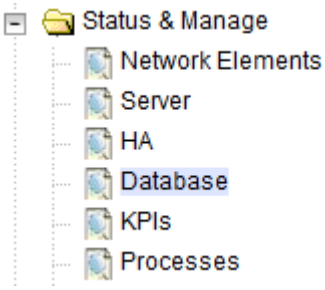
Procedure 1. Recovery Scenario 1

27. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 
28. ☐	**NOAM VIP GUI**: Recover the remaining SOAM servers	Executing Configure the SOAM Servers, steps 1 and 3-6, from reference [1]. ***Note***: Wait for server to reboot before continuing.
29. ☐	**NOAM VIP GUI**: Restart DSR application on remaining SOAM server(s)	1. Navigate to **Status & Manage > Server**.  2. Select the recovered standby SOAM server and click **Restart**. 

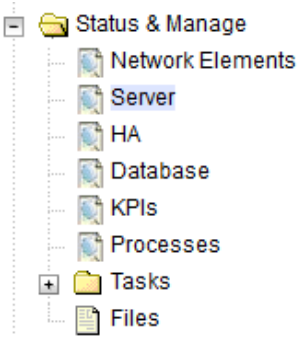
Procedure 1. Recovery Scenario 1

30. ☐	**NOAM VIP GUI**: Set HA on recovered standby SOAM server, if applicable ***Note***: For non-HA sites, skip this step	1. Navigate to **Status & Manage > HA**.  2. Click **Edit** at the bottom of the screen. 3. Select the recovered SOAM server and set it to **Active**.  4. Click **OK**.

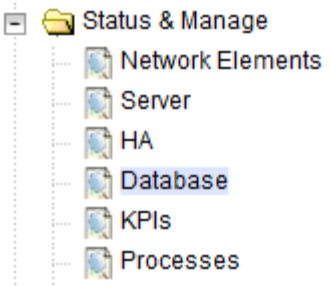
Procedure 1. Recovery Scenario 1

31. ☐	**NOAM VIP GUI**: Start replication on working C-level servers	Un-Inhibit (Start) Replication to the **working** C-level Servers which belongs to the same site as of the failed SOAM servers. If the spare SOAM is also present in the site and lost, execute Appendix A If the spare SOAM is also present in the site and lost, execute Appendix A 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 B Inhibit A and B Level Replication on C-level Servers. 1. Navigate to **Status & 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)** • MP/IPFE servers (if MPs are configured as active/standby, start with the Active MP; otherwise, the order of the MPs does not matter) • SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare) 3. Verify the replication on all the working servers is allowed. This can be done by examining the Repl Status table as shown here: **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

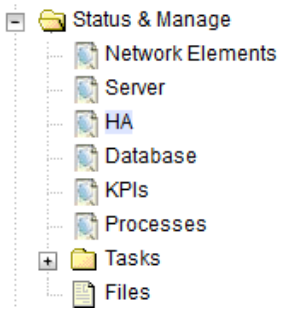
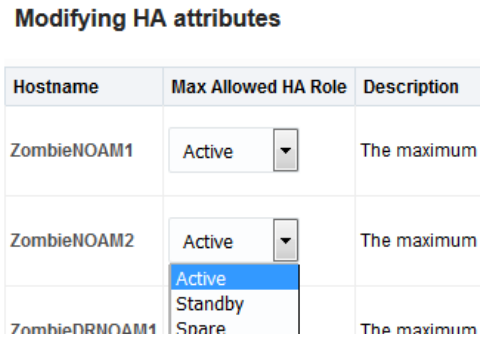
Procedure 1. Recovery Scenario 1

32. ☐	**Active NOAM**: Perform key exchange between the active-NOAM and recovered servers (DA-MP, SBRs, IPFE, SS7-MP, and 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 Configure the MP Virtual Machines, steps 1, 11-14 (and 15 if required) of reference [1] for each server that has been recovered.
33. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**. 

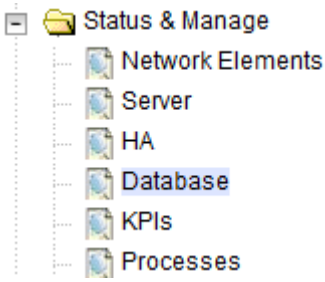
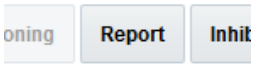
Procedure 1. Recovery Scenario 1

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 & Manage > Database.  2. If the **Repl Status** is set to **Inhibited**, click **Allow Replication** using this order: • Active NOAM Server • Standby NOAM Server • Active SOAM Server • Standby SOAM Server • Spare SOAM Server (if applicable) • MP/IPFE servers (if MPs are configured as active/standby, start with the Active MP; otherwise, the order of the MPs does not matter) 3. Verify the replication on all the working servers is allowed. This can be done by examining the Repl Status table as shown here: **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

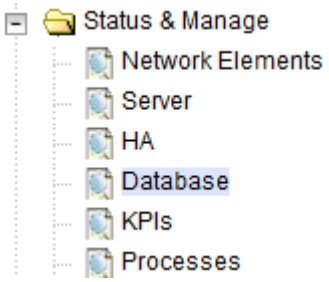
Procedure 1. Recovery Scenario 1

35. ☐	**NOAM VIP GUI**: Set HA on all C-level servers	1. Navigate to **Status & Manage > HA**.  2. Click **Edit** at the bottom of the screen. 3. For each server with a Max Allowed HA Role 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	**Note for PCA Activation:** If you have PCA installed in the system being recovered, re-activate PCA by executing PCA Activation on Entire Server on Recovered NOAM Server and PCA Activation on Active SOAM Server from [3]. ***Note***: While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: `iload#31000{S/W Fault}` ***Note***: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature. Refer to section 1.4 Optional Features to activate any features previously activated.

Procedure 1. Recovery Scenario 1

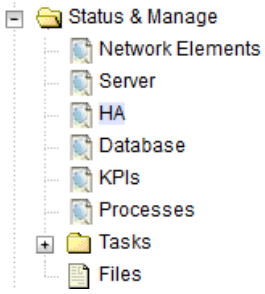
38. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status & Manage > Database**.
		 
		2. Select the active NOAM server and click **Report**.
		 
		The following screen displays:
		Main Menu: Status & Manage -> Database [Report]
		`dsr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

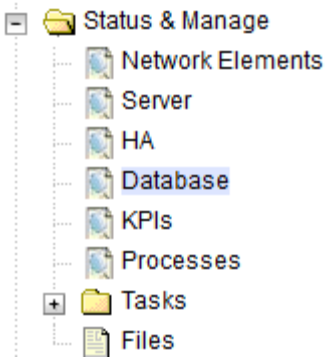
Procedure 1. Recovery Scenario 1

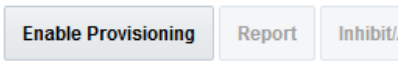
<table>
<tr>
<td>39. ☐</td>
<td>Active NOAM: Verify replication between servers</td>
<td>1. Log into the active NOAM using SSH terminal as admusr.
2. Execute this command:
<pre>$ sudo irepstat –m</pre>
Output:
<pre>-- Policy 0 ActStb [DbReplication] ---------------------
RDU06-MP1 -- Stby
  BC From RDU06-SO1 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</pre>
</td>
</tr>
<tr>
<td>40. ☐</td>
<td>NOAM VIP GUI: Verify the database states</td>
<td>1. Navigate to Status & Manage > 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 the status is Normal:
Main Menu: Status & Manage -> Database
Filter* Info* Tasks
<table>
<tr><th>Network Element</th><th>Server</th><th>Role</th><th>OAM Max HA Role</th><th>Application Max HA Role</th><th>Status</th></tr>
<tr><td>SOAM_NE</td><td>SO1</td><td>System OAM</td><td>Standby</td><td>N/A</td><td>Normal</td></tr>
<tr><td>SOAM_NE</td><td>SO2</td><td>System OAM</td><td>Active</td><td>N/A</td><td>Normal</td></tr>
<tr><td>NOAM_NE</td><td>NO2</td><td>Network OAM&P</td><td>Standby</td><td>N/A</td><td>Normal</td></tr>
<tr><td>SOAM_NE</td><td>DAMP1</td><td>MP</td><td>Active</td><td>Active</td><td>Normal</td></tr>
<tr><td>NOAM_NE</td><td>NO1</td><td>Network OAM&P</td><td>Active</td><td>N/A</td><td>Normal</td></tr>
</table>
</td>
</tr>
</table>

Procedure 1. Recovery Scenario 1

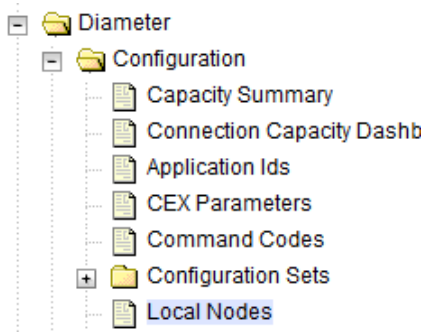
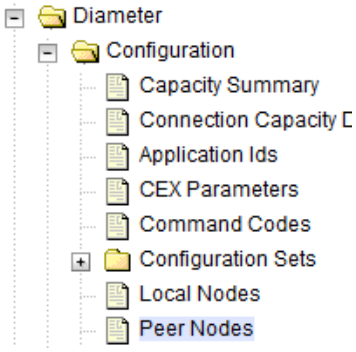
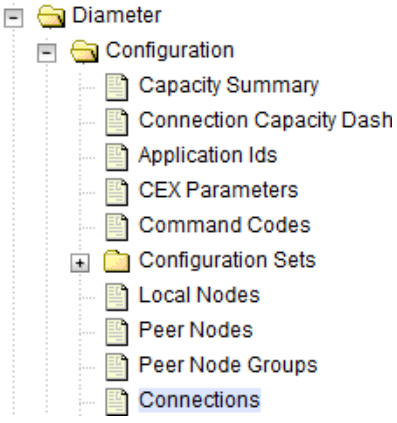
<table>
<tr>
<td>41. ☐</td>
<td>NOAM VIP GUI:
Verify the HA status</td>
<td>
1. Navigate to Status and Manage > HA.


2. Select the row for all of the servers.
3. Verify the HA Role is either Active or Standby.
<table>
<tr><th>Hostname</th><th>OAM HA Role</th><th>Application HA Role</th><th>Max Allowed HA Role</th></tr>
<tr><td>ZombieNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieDRNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieDRNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieSOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieSOAM2</td><td>Standby</td><td>N/A</td><td>Standby</td></tr>
</table>
</td>
</tr>
<tr>
<td>42. ☐</td>
<td>NOAM GUI:
Enable provisioning</td>
<td>
1. Navigate to Status & Manage > Database.


2. Click Enable Provisioning.


3. A confirmation window displays. Click OK to enable provisioning.
</td>
</tr>
</table>

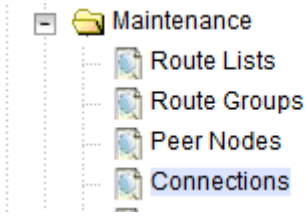
Procedure 1. Recovery Scenario 1

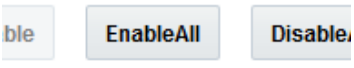
43. ☐	**SOAM VIP GUI**: Verify the local node info	1. Navigate to **Diameter > Configuration > Local Node**.  2. Verify all the local nodes are shown.
44. ☐	**SOAM VIP GUI**: Verify the peer node info	1. Navigate to **Diameter > Configuration > Peer Node**.  2. Verify all the peer nodes are shown.
45. ☐	**SOAM VIP GUI**: Verify the connections info	1. Navigate to **Diameter > Configuration > Connections**.  2. Verify all the connections are shown.

Procedure 1. Recovery Scenario 1

<table>
<tr>
<td>46.
☐</td>
<td>For vSTP Only
SOAM VIP Server Console (Optional): Verify vSTP MP local node information</td>
<td>1. Log into the SOAM VIP server console as admusr.
2. Execute the following command:
<code>[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts</code>
3. Verify the output similar to this output.
<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>47.
☐</td>
<td>For vSTP Only
SOAM VIP Server Console (Optional): Verify vSTP MP remote nodes information</td>
<td>1. Log into the SOAM VIP server console as admusr.
2. Execute the following command
<code>[admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts</code>
3. Verify the output similar to this output.
<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>

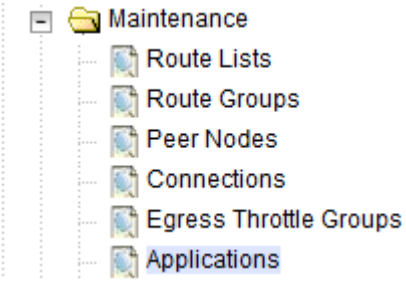
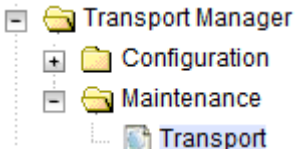
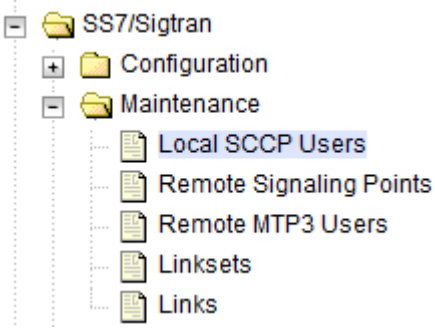
Procedure 1. Recovery Scenario 1

<table>
<tr>
<td>48.
☐</td>
<td>For vSTP Only
SOAM VIP Server Console (Optional): Verify the vSTP MP connections information</td>
<td>1. Log into the SOAM VIP server console as admusr.
2. Execute the following command
<pre>[admusr@SOAM1 ~]$ mmiclient.py /vstp/connections</pre>3. Verify the output similar to this output.
<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>49.
☐</td>
<td>MP Servers: Disable SCTP Auth Flag</td>
<td>For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [1].
Execute this procedure on all failed MP servers.</td>
</tr>
<tr>
<td>50.
☐</td>
<td>SOAM VIP GUI: Enable connections, if needed</td>
<td>1. Navigate to Diameter > Maintenance > Connections.
 

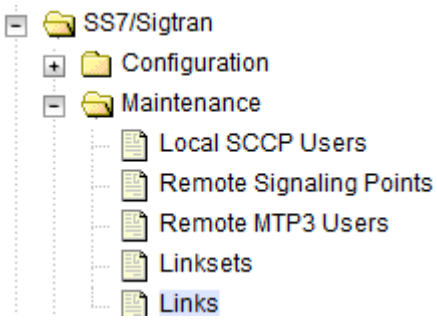
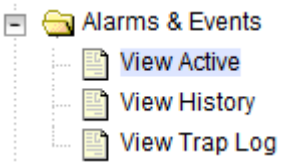
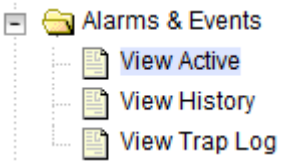
2. Select each connection and click Enable. Alternatively, you can enable all the connections by clicking EnableAll.
 

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

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. This step is applicable when the MAP-IWF is activated.	1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.  2. Click the **Enable** button 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. This step is applicable when the MAP-IWF is activated.	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 Appendix E DSR Database Backup to back up the Configuration databases.

4.2 Recovery Scenario 2 — Partial Server Outage with One NOAM Server Intact and ALL SOAMs Failed

For a partial server outage with an NOAM server intact and available; SOAM servers are recovered using recovery procedures for software and then executing a database restore to the active SOAM server using a database backup file obtained from the SOAM servers. All other servers are recovered using recovery procedures for software. Database replication from the active NOAM server will recover the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures' detailed steps are in Procedure 2. The major activities are summarized as follows:

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

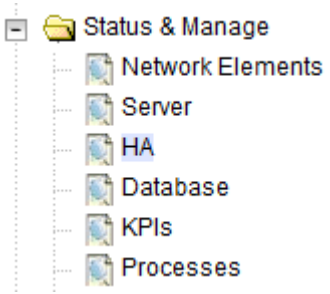
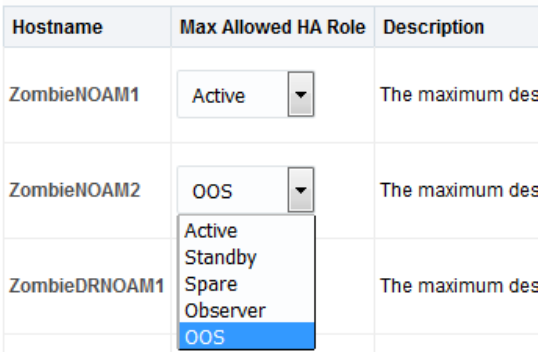
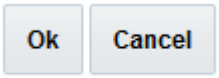
Procedure 2. Recovery Scenario 2

S T E P #	This procedure performs recovery if at least 1 NOAM server is available, but all SOAM servers in a site have failed. This includes any SOAM server that is in another location. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Workaround	Refer to Appendix F to Check and Create Backup Directory.
2. ☐	Gather required materials	Gather the documents and required materials listed in section 3.1 Required Materials.

Procedure 2. Recovery Scenario 2

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

Procedure 2. Recovery Scenario 2

4. ☐	**Active NOAM**: Set failed servers to OOS	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. **Modifying HA attributes**  3. Set the Max Allowed HA Role to **OOS** for the failed servers. 4. Click **OK**. 
5. ☐	Recover the failed software	**For VMWare based deployments**: 1. For NOAMs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 2 (VMWare Only) Configure NOAM Guests Based On Resource Profile 2. For SOAMs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile 3. For failed MPs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager,

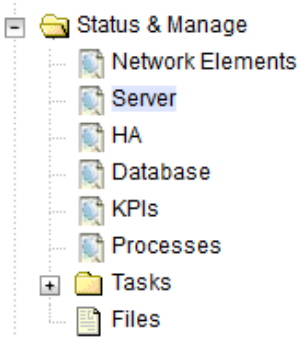
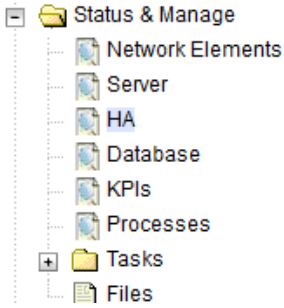
Procedure 2. Recovery Scenario 2

		skip this procedure to import OVA. b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile **For KVM/OpenStack based deployments**: 1. For NOAMs, execute the following procedures from reference [1]: a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 5 (KVM/OpenStack Only) Configure NOAM Guests Based On Resource Profile 2. For SOAMs, execute the following procedures from reference [1]: a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile 3. For failed MPs, execute the following procedures from reference [1]: a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this 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**: 1. Execute the following procedures from reference [1]: a. Procedure 7 (OVM-S/OVM-M) Import DSR OVA and Prepare for VM creation b. Procedure 8 (OVM-S/OVM-M) Configure each DSR VM While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs).
6. ☐	Repeat	If necessary, repeat step 5. for all remaining servers.

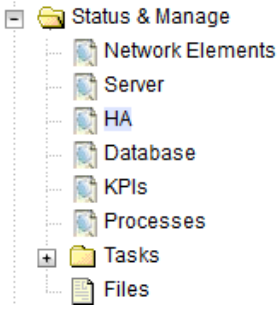
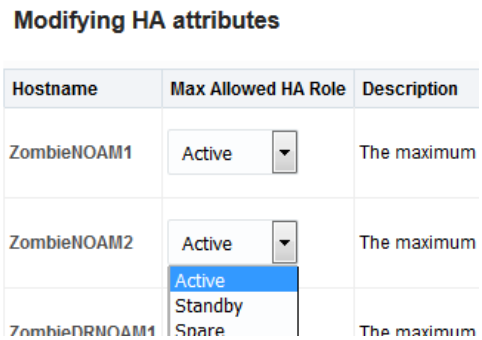
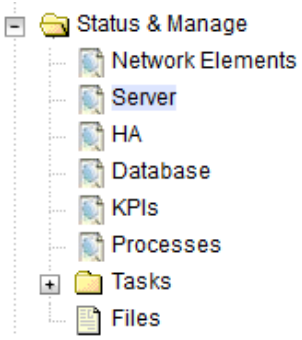
Procedure 2. Recovery Scenario 2

7. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 
8. ☐	**NOAM VIP GUI**: Recover standby NOAM	Install the second NOAM server by executing these procedures from reference [1]: • Execute Configure the Second NOAM Server, steps 3-5 and 7 • Execute Configure the NOAM Server Group, step 4 ***Note***: If topology or nodeID alarms are persistent after the database restore, refer to Appendix F to Check and Create Backup Directory.

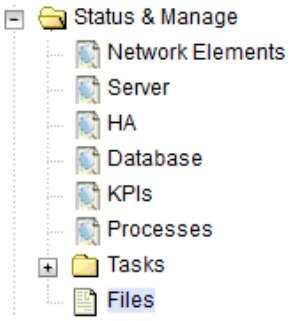
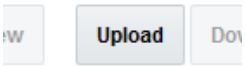
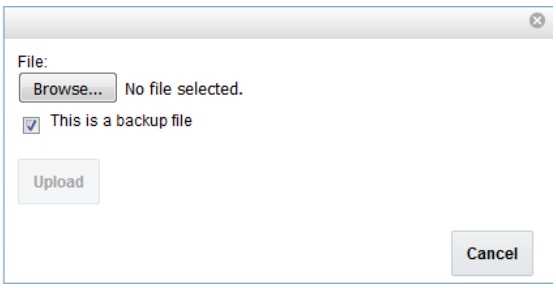
Procedure 2. Recovery Scenario 2

9. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**.  3. Click **OK** on confirmation screen.
10. ☐	**NOAM VIP GUI**: Set HA on standby NOAM	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Select the standby NOAM server and set it to **Active**. Click **OK**.
11. ☐	**NOAM VIP GUI**: Stop replication to the C-level servers of this site 	**!!Warning!!** Before continuing this procedure, replication to C-level servers at the SOAM site being recovered MUST be inhibited. Failure to inhibit replication to the working C-level servers results in the database being destroyed! If the spare SOAM is also present in the site and lost, execute Appendix A 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 C Inhibit A and B Level Replication on C-level Servers to inhibit replication to working C-level servers before continuing.
12. ☐	Recover active SOAM server	Install the SOAM servers by executing Configure the SOAM Servers, steps 1 and 3-7 from reference [1]. ***Note***: Wait for the server to reboot.

Procedure 2. Recovery Scenario 2

13. ☐	**NOAM VIP GUI**: Set HA on active NOAM	1. Navigate to **Status & Manage > HA**.  2. Click **Edit** at the bottom of the screen. 3. Select the active NOAM server and set it to **Active**.  4. Click **OK**.
14. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered active SOAM server and click **Restart**. 

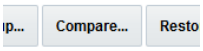
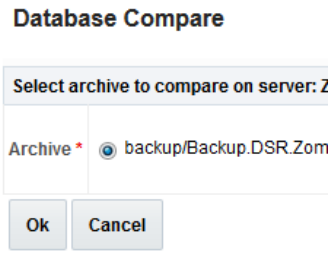
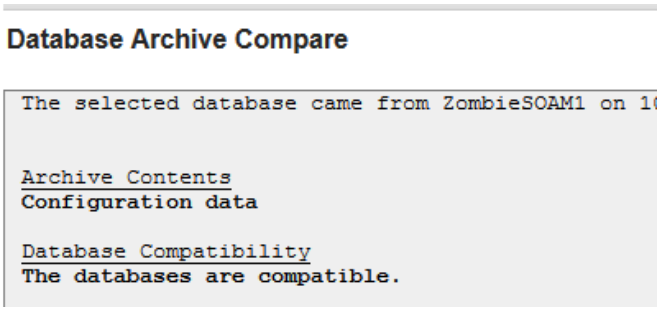
Procedure 2. Recovery Scenario 2

15. ☐	**NOAM VIP GUI**: Upload the backed up SOAM database file	3. Navigate to **Status & Manage > Files**.  4. Select the active SOAM server tab. Click **Upload** and select the file **SO Provisioning and Configuration** file backed up after initial installation and provisioning.  5. Click **Browse** and locate the backup file. 6. Check This is a backup file checkbox. 7. Click **Upload**.  The file takes a few seconds to upload depending on the size of the backup data.

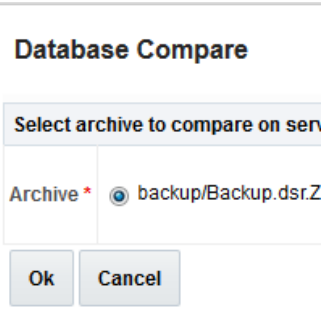
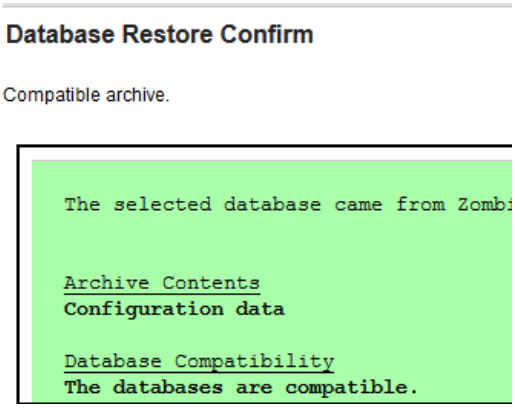
Procedure 2. Recovery Scenario 2

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

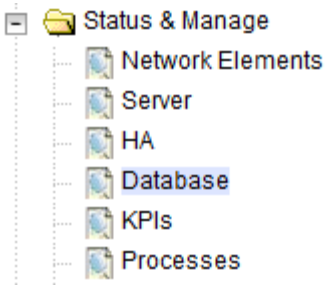
Procedure 2. Recovery Scenario 2

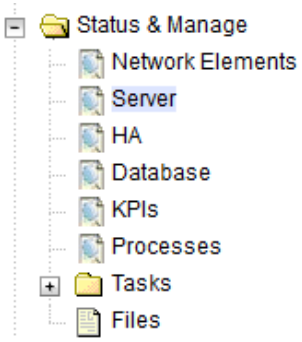
17. ☐	**Recovered SOAM GUI**: Verify the archive contents and database compatibility	1. Navigate to **Status & Manage > Database**. 2. Select the **Active SOAM** server and click **Compare**.  3. Click the button for the restored database file uploaded as a part of step 15. of this procedure.  4. **Verify** the output window matches the screen below.  ***Note***: Archive Contents and Database Compatibilities must be the following: **Archive Contents**: Configuration data. **Database Compatibility**: The databases are compatible. ***Note***: The following is expected output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM: **Topology Compatibility** The topology should be compatible minus the nodeID. ***Note***: We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in topology compatibility. 5. If the verification is successful, click **Back**.

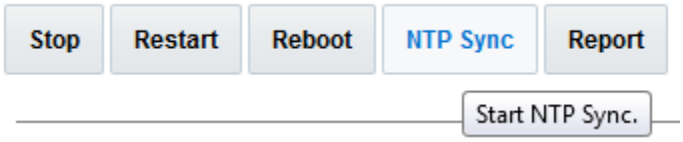
Procedure 2. Recovery Scenario 2

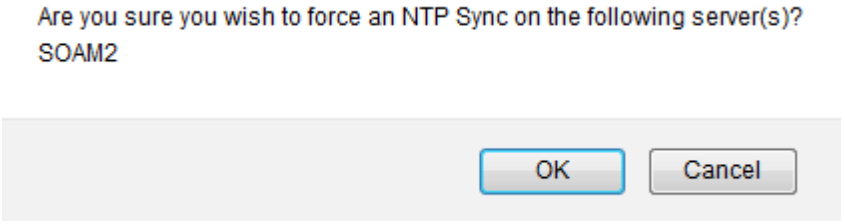
18. ☐	**Recovered SOAM GUI**: Restore the database	1. Select the **Active SOAM** server and click **Restore**. 2. Select the proper back up provisioning and configuration file.  3. Click **OK**. The following confirmation screen displays.  4. If you receive an error for Node Type Compatibility, that is expected. If no other errors are displayed, mark the **Force** checkbox and click **OK** to proceed with the DB restore. ***Note***: After the restore has started, the user is logged out of XMI SOAM GUI since the restored Topology is old data.
19. ☐	**Recovered SOAM GUI**: Monitor and confirm database restoral	Wait for **5-10 minutes** for the system to stabilize with the new topology: Monitor the Info tab for **Success**. This indicates the restore is complete and the system is stabilized. ***Note***: Do not pay attention to alarms until all the servers in the system are completely restored. ***Note***: The Configuration and Maintenance information is in the same state it was when backed up during initial backup.
20. ☐	**NOAM VIP GUI**: Recover the remaining SOAM servers	Execute Configure the SOAM Servers, steps 1 and 3-6, from reference [1]. ***Note***: Wait for server to reboot before continuing.

Procedure 2. Recovery Scenario 2

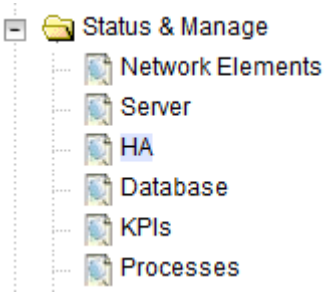
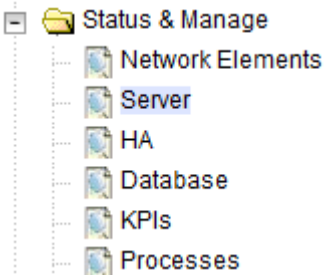
<table>
<tr>
<td>21. ☐</td>
<td>NOAM VIP GUI: Start replication on the recovered SOAMs</td>
<td>Un-Inhibit (Start) Replication to the recovered SOAM servers.
1. Navigate to Status & Manage > Database.
 

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</td>
</tr>
<tr>
<td>22. ☐</td>
<td>Recovered Server: Synchronize NTP</td>
<td>1. Navigate to Status & Manage > Server.
 

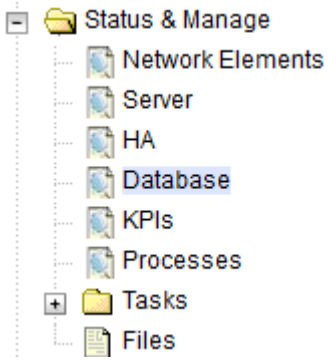
2. Select the recovered server and click NTP Sync.
 

3. Click OK to confirm.
 
</td>
</tr>
</table>

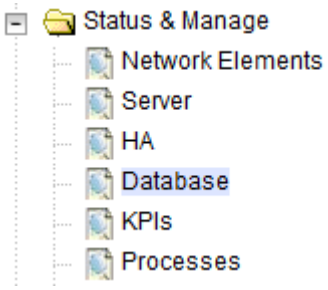
Procedure 2. Recovery Scenario 2

23. ☐	**NOAM VIP GUI**: Restart DSR application on recovered C-level servers	1. Navigate to **Status & Manage > HA**.  2. Click **Edit** at the bottom of the screen. 3. For each SOAM server with a Max Allowed HA Role set to **Standby**, set it to **Active**.  4. Click **OK**.
24. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**. 

Procedure 2. Recovery Scenario 2

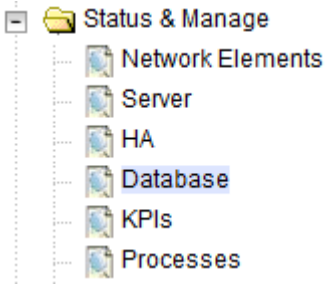
25. ☐	**SOAM GUI**: Enable provisioning	1. Navigate to **Status & Manage > Database**.  2. Click **Enable Site Provisioning**.  3. A confirmation window displays. Click **OK** to enable Provisioning.

Procedure 2. Recovery Scenario 2

<table>
<tr>
<td>26. ☐</td>
<td>NOAM VIP GUI: Start replication on working C-level servers</td>
<td>
Un-Inhibit (Start) Replication to the working C-level Servers which belongs to the same site as of the failed SOAM servers.
If the spare SOAM is also present in the site and lost, execute Appendix A If the spare SOAM is also present in the site and lost, execute Appendix A 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 B Inhibit A and B Level Replication on C-level Servers.
1. Navigate to Status & Manage > Database.


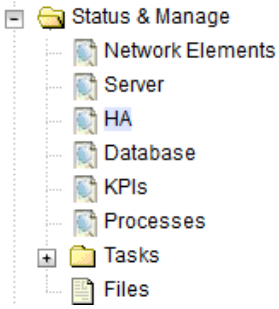
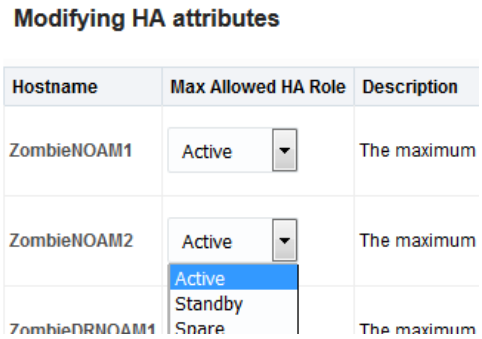
2. If the Repl Status is set to Inhibited, click Allow Replication using this order; otherwise, if none of the servers are inhibited, skip this step and continue with the next step:
• Active NOAM Server
• Standby NOAM Server
• Active SOAM Server
• Standby SOAM Server
• Spare SOAM Server (if applicable)
• MP/IPFE servers (if MPs are configured as active/standby, start with the Active MP; otherwise, the order of the MPs does not matter)
• SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare)
3. Verify the replication on all the working servers is allowed. This can be done by examining the Repl Status table as shown here:
<table>
<tr><th>OAM Repl Status</th><th>SIG Repl Status</th><th>Repl Status</th><th>Repl Audit Status</th></tr>
<tr><td>NotApplicable</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
</table>
</td>
</tr>
</table>

Procedure 2. Recovery Scenario 2

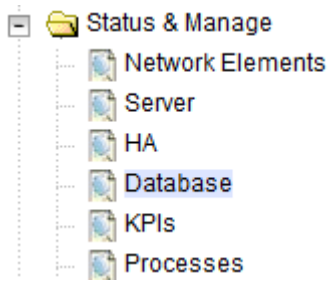
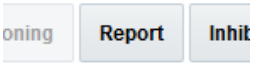
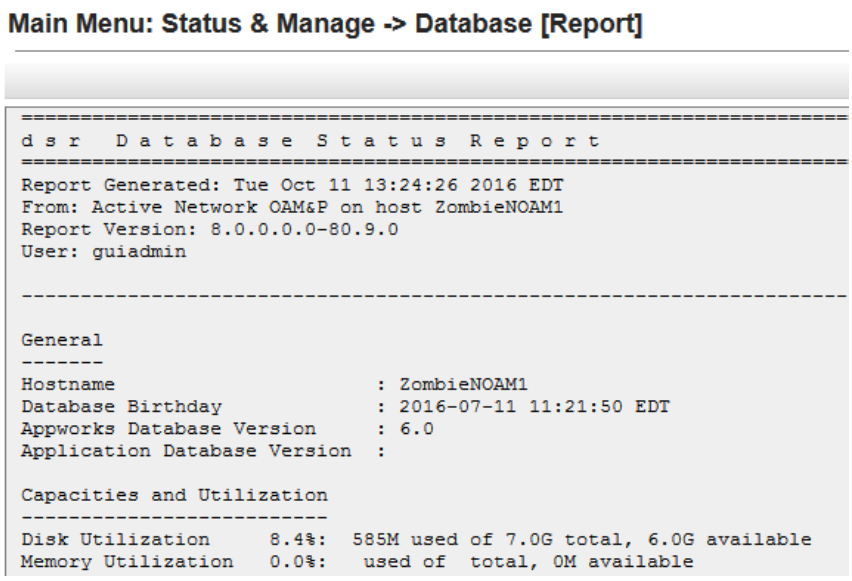
<table>
<tr>
<td>27. ☐</td>
<td>Active NOAM: Perform key exchange between the active-NOAM and recovered servers (DA-MP, SBRs, IPFE, SS7-MP, and vSTP-MP)</td>
<td>1. Establish an SSH session to the C-level server being recovered and login as admusr.
2. Execute following command to set shared memory to unlimited:
<code>$ sudo shl.set -m 0</code>
3. Execute Configure the MP Virtual Machines, steps 1, 11-14 (and 15 if required) of reference [1] for each server that has been recovered.</td>
</tr>
<tr>
<td>28. ☐</td>
<td>NOAM VIP GUI: Start replication on all C-level servers</td>
<td>Un-inhibit (start) replication to the ALL C-level servers.
1. Navigate to Status & Manage > Database.
 

2. If the Repl Status is set to Inhibited, click Allow Replication using this order:
• Active NOAM Server
• Standby NOAM Server
• Active SOAM Server
• Standby SOAM Server
• Spare SOAM Server (if applicable)
• MP/IPFE servers (if MPs are configured as active/standby, start with the Active MP; otherwise, the order of the MPs does not matter)
3. Verify the replication on all the working servers is allowed. This can be done by examining the Repl Status table as shown here:
<table>
<tr><th>OAM Repl Status</th><th>SIG Repl Status</th><th>Repl Status</th><th>Repl Audit Status</th></tr>
<tr><td>NotApplicable</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
<tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr>
</table>
</td>
</tr>
</table>

Procedure 2. Recovery Scenario 2

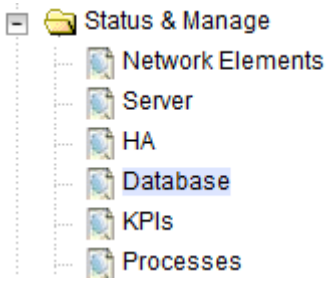
29. ☐	**NOAM VIP GUI**: Set HA on all C-level servers	1. Navigate to **Status & Manage > HA**.  2. Click **Edit** at the bottom of the screen. 3. For each server with a Max Allowed HA Role set to OOS, set it to **Active**.  Click **OK**.
30. ☐	**Active NOAM**: Perform key exchange between the active-NOAM 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	**Note for PCA Activation:** If you have PCA installed in the system being recovered, re-activate PCA by executing PCA Activation on Entire Server on Recovered NOAM Server and PCA Activation on Active SOAM Server from [3]. ***Note***: While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: `iload#31000{S/W Fault}` ***Note***: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature. Refer to section 1.4 Optional Features to activate any features previously activated.

Procedure 2. Recovery Scenario 2

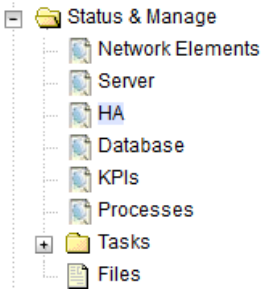
32. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status & Manage > Database**.  2. Select the active NOAM server and click **Report**.  The following screen displays:  3. Click **Save** and save the report to your local machine.

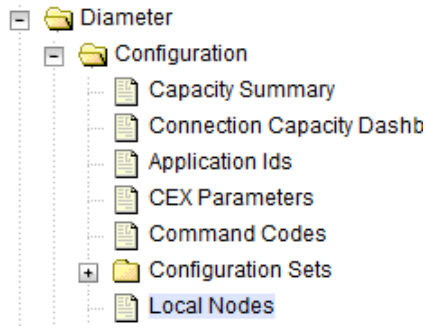
Procedure 2. Recovery Scenario 2

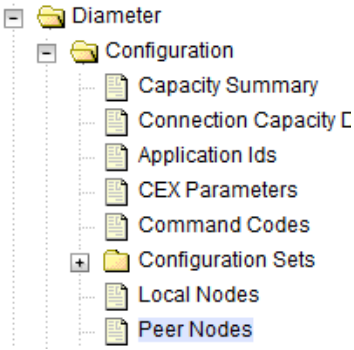
33. ☐	**Active NOAM**: Verify replication between servers	1. Log into the active NOAM using SSH terminal as **admusr**.
		2. Execute this command:
		`$ sudo irepstat -m`
		Output:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`RDU06-MP1 -- Stby`
		`  BC From RDU06-SO1 Active  0  0.50 ^0.17%cpu 42B/s  A=none`
		`  CC From RDU06-MP2 Active  0  0.10 ^0.17 0.88%cpu 32B/s  A=none`
		`RDU06-MP2 -- Active`
		`  BC From RDU06-SO1 Active  0  0.50 ^0.10%cpu 33B/s  A=none`
		`  CC To  RDU06-MP1 Active  0  0.10  0.08%cpu 20B/s  A=none`
		`RDU06-NO1 -- Active`
		`  AB To  RDU06-SO1 Active  0  0.50 1%R 0.03%cpu 21B/s`
		`RDU06-SO1 -- Active`
		`  AB From RDU06-NO1 Active  0  0.50 ^0.04%cpu 24B/s`
		`  BC To  RDU06-MP1 Active  0  0.50 1%R 0.04%cpu 21B/s`
		`  BC To  RDU06-MP2 Active  0  0.50 1%R 0.07%cpu 21B/s`

34. ☐	**NOAM VIP GUI**: Verify the database states	1. Navigate to **Status & Manage > 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 the status is **Normal**: **Main Menu: Status & Manage -> Database** Filter* Info* Tasks Network Element / Server / Role / OAM Max HA Role / Application Max HA Role / Status SOAM_NE / SO1 / System OAM / Standby / N/A / Normal SOAM_NE / SO2 / System OAM / Active / N/A / Normal NOAM_NE / NO2 / Network OAM&P / Standby / N/A / Normal SOAM_NE / DAMP1 / MP / Active / Active / Normal NOAM_NE / NO1 / Network OAM&P / Active / N/A / Normal

Procedure 2. Recovery Scenario 2

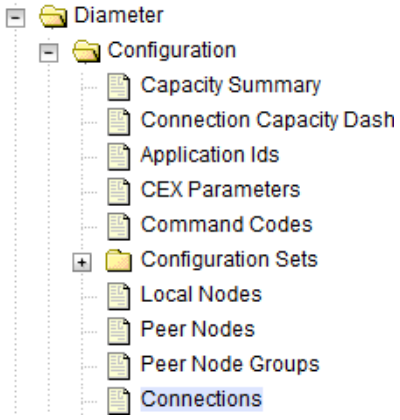
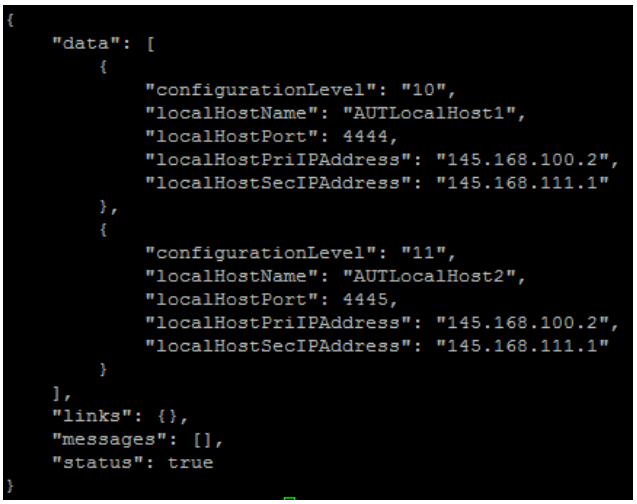
<table>
<tr>
<td>35. ☐</td>
<td>NOAM VIP GUI: Verify the HA status</td>
<td>
1. Navigate to Status and Manage > HA.


2. Select the row for all of the servers.
3. Verify the HA Role is either Active or Standby.
<table>
<tr><th>Hostname</th><th>OAM HA Role</th><th>Application HA Role</th><th>Max Allowed HA Role</th></tr>
<tr><td>ZombieNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieDRNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieDRNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieSOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieSOAM2</td><td>Standby</td><td>N/A</td><td>Standby</td></tr>
</table>
</td>
</tr>
<tr>
<td>36. ☐</td>
<td>SOAM VIP GUI: Verify the local node info</td>
<td>
1. Navigate to Diameter > Configuration > Local Node.


2. Verify all the local nodes are shown.
</td>
</tr>
<tr>
<td>37. ☐</td>
<td>SOAM VIP GUI: Verify the peer node info</td>
<td>
1. Navigate to Diameter > Configuration > Peer Node.


2. Verify all the peer nodes are shown.
</td>
</tr>
</table>

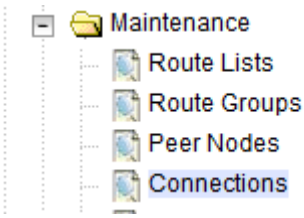
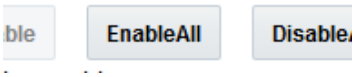
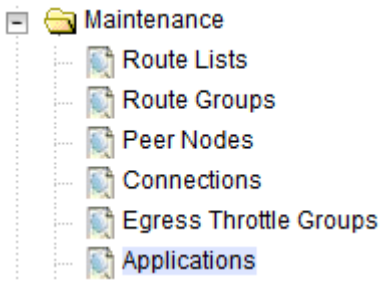
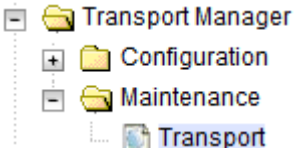
Procedure 2. Recovery Scenario 2

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

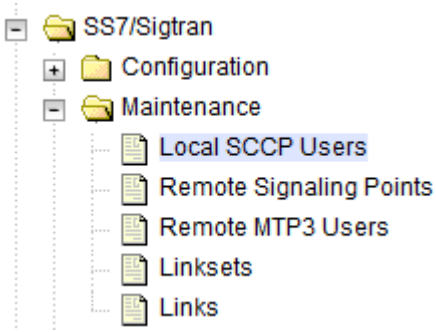
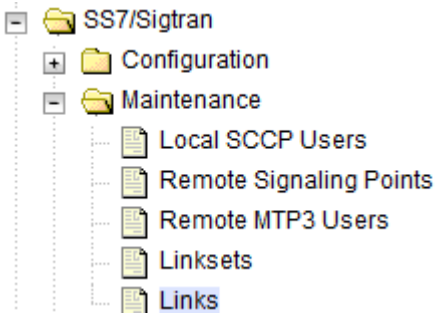
Procedure 2. Recovery Scenario 2

<table>
<tr><td>40.
☐</td><td>For vSTP Only
SOAM VIP Server Console (Optional): Verify vSTP MP remote nodes information</td><td>1. Log into the SOAM VIP server console as admusr.
2. Execute the following command
<code>[admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts</code>
3. Verify the output similar to this output.
<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 (Optional): Verify the vSTP MP connections information</td><td>1. Log into the SOAM VIP server console as admusr.
2. Execute the following command
<code>[admusr@SOAM1 ~]$ mmiclient.py /vstp/connections</code>
3. Verify the output similar to this output.
<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 Auth Flag</td><td>For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [1].
Execute this procedure on all failed MP servers.</td></tr>
</table>

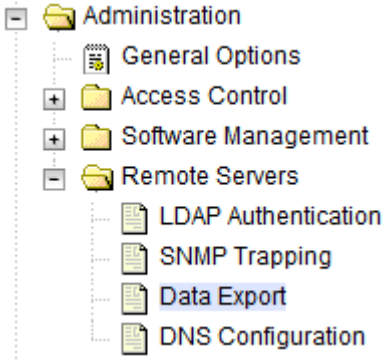
Procedure 2. Recovery Scenario 2

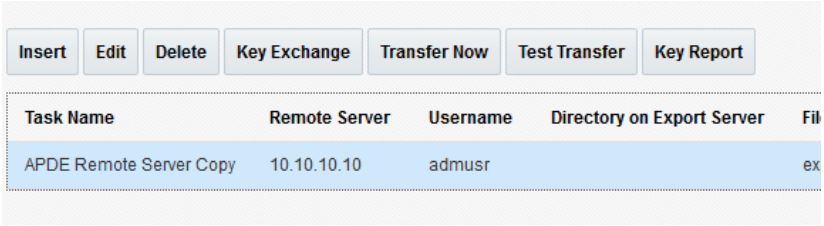
43. ☐	**SOAM VIP GUI**: Enable connections, if needed	1. Navigate to **Diameter > Maintenance > Connections**.  2. Select each connection and click **Enable**. Alternatively, you can enable all the connections by clicking **EnableAll**.  3. Verify the Operational State is **Available**.
44. ☐	**SOAM 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**.  Verify the Operational Status for each transport is **Up**.

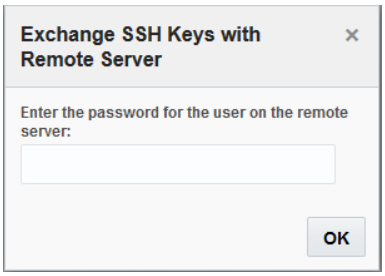
Procedure 2. Recovery Scenario 2

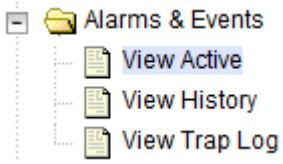
46. ☐	**SOAM VIP GUI**: Re-enable MAPIWF application, if needed. This step is applicable when the MAP-IWF is activated.	1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.  2. Click the **Enable** button corresponding to MAPIWF Application Name.  Verify the SSN Status is **Enabled**.
47. ☐	**SOAM VIP GUI**: Re-enable links, if needed. This step is applicable when the MAP-IWF is activated.	1. Navigate to **SS7/Sigtran > Maintenance > Links**.  2. Click **Enable** for each link.  Verify the Operational Status for each link is **Up**.

Procedure 2. Recovery Scenario 2

<table>
<tr>
<td>48. ☐</td>
<td>NOAM VIP GUI: Perform Keyexchange with export server</td>
<td>1. Navigate to Administration > Remote Servers > Data Export.
 

2. Click the Task Name and click Key Exchange.
 

3. Type the Password and click OK.
 

Repeat for each task.</td>
</tr>
<tr>
<td>49. ☐</td>
<td>SOAM VIP GUI: Examine all alarms</td>
<td>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).</td>
</tr>
<tr>
<td>50. ☐</td>
<td>Backup and archive all the databases from the recovered system</td>
<td>Execute Appendix E DSR Database Backup to back up the Configuration databases.</td>
</tr>
</table>

4.3 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 NOAM servers by recovering software
  - Recover the software
- Recover any failed SOAM and MP servers by recovering software
  - Recover the software
  - Database is already intact at one SOAM server and does not require restoration at the other SOAM and MP servers

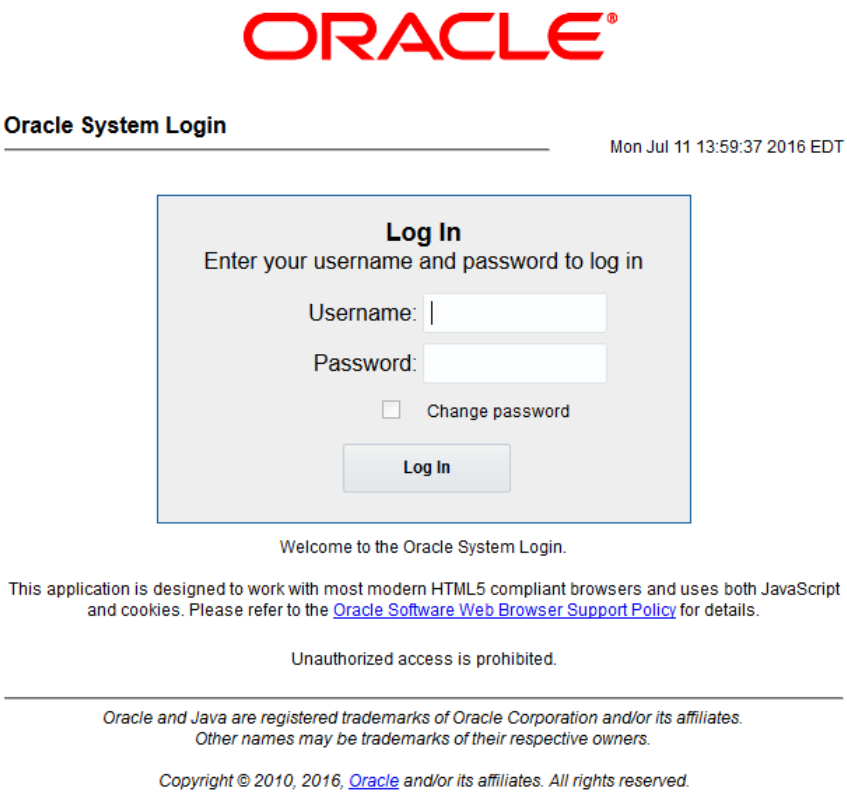
Procedure 3. Recovery Scenario 3

S T E P #	This procedure performs recovery if ALL NOAM servers are failed but 1 or more SOAM servers are intact. This includes any SOAM server that is in another location (spare SOAM server). Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Workaround	Refer to Appendix F to Check and Create Backup Directory.
2. ☐	Gather required materials	Gather the documents and required materials listed in section 3.1 Required Materials.
3. ☐	Recover the failed software	**For VMWare based deployments**: 1. For NOAMs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 2 (VMWare Only) Configure NOAM Guests Based On Resource Profile 2. For SOAMs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based

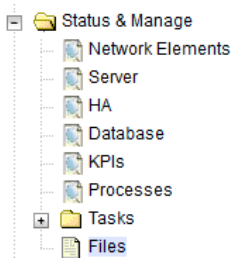
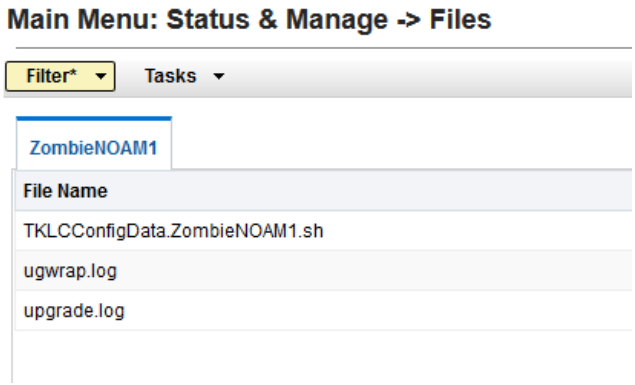
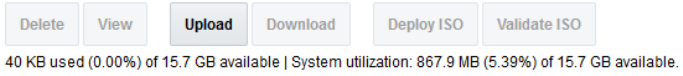
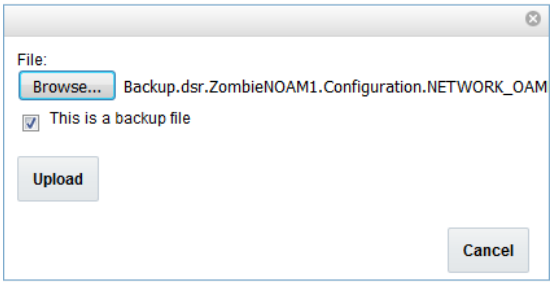
Procedure 3. Recovery Scenario 3

		On Resource Profile 3. For failed MPs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile **For KVM/OpenStack based deployments**: 1. For NOAMs, execute the following procedures from reference [1]: a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 5 (KVM/OpenStack Only) Configure NOAM Guests Based On Resource Profile 2. For SOAMs, execute the following procedures from reference [1]: a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile 3. For failed MPs, execute the following procedures from reference [1]: a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this 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**: 1. Execute the following procedures from reference [1]: a. Procedure 7 (OVM-S/OVM-M) Import DSR OVA and Prepare for VM creation b. Procedure 8 (OVM-S/OVM-M) Configure each DSR VM While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs).
4. ☐	Obtain latest database backup and network configuration data	1. Obtain the most recent database backup file from external backup sources (for example, file servers) or tape backup sources. 2. From required materials list in section 3.1 Required Materials; use site survey documents and Network Element report (if available) to determine network configuration data.

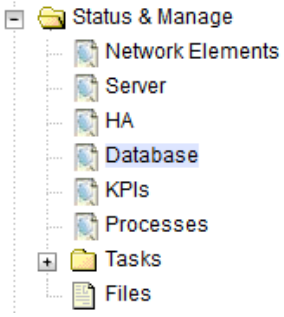
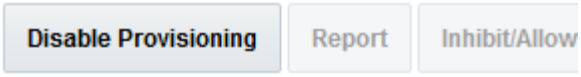
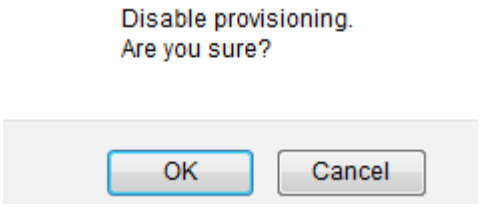
Procedure 3. Recovery Scenario 3

5. ☐	Execute DSR installation procedure for the first NOAM	Verify the network data for network elements. ***Note***: Use the backup copy of network configuration data and site surveys (Step 2). • Execute Configure the First NOAM NE and Server from reference [1]. • Execute Configure the NOAM Server Group from reference [1].
6. ☐	**NOAM GUI**: Login	1. Establish a GUI session on the recovered NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Recovered_NOAM_IP_Address>` 2. Log into the NOAM GUI as the **guiadmin** user: 

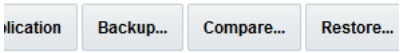
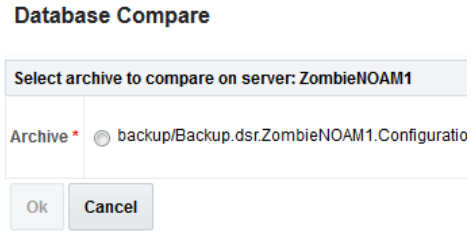
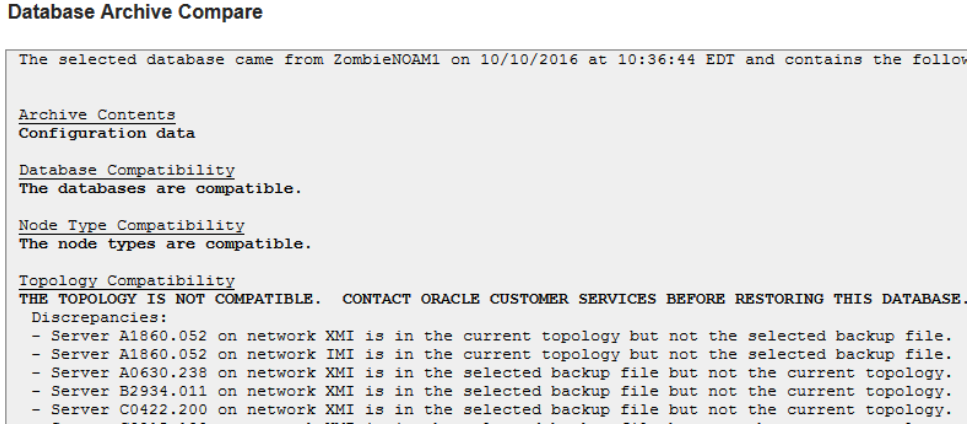
Procedure 3. Recovery Scenario 3

7. ☐	**NOAM GUI**: Upload the backed up database file	1. Navigate to **Status & 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. Check **This is a backup file** checkbox. 6. Click **Upload**.  7. 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.

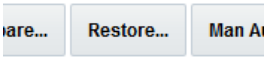
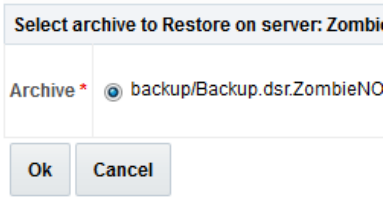
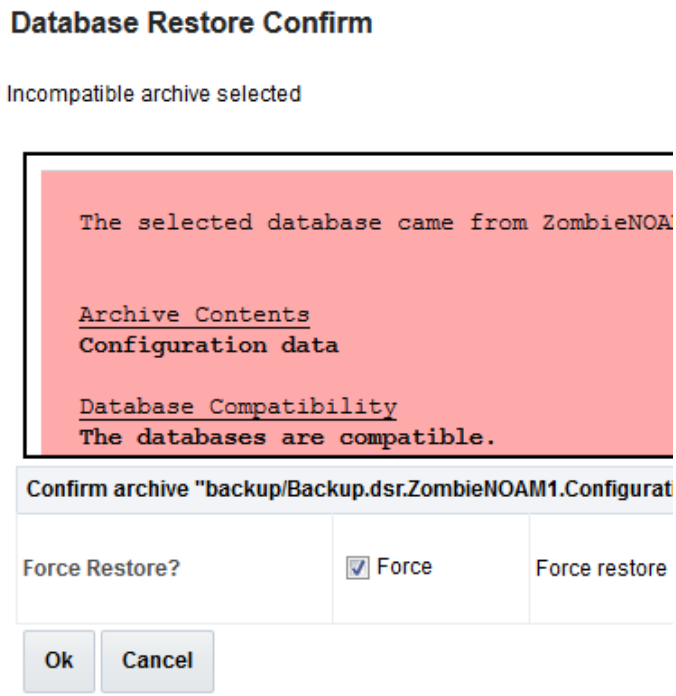
Procedure 3. Recovery Scenario 3

8. ☐	**NOAM GUI**: Disable provisioning	1. Navigate to **Status & Manage > Database**.  2. Click **Disable Provisioning**.  3. A confirmation window displays. Click **OK** 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 Topology Compatibility and possibly User compatibility (due to authentication) display. These warnings are expected. If these are the only mismatches, proceed; otherwise, stop and contact My Oracle Support (MOS) to ask for assistance.  ***Note***: Archive Contents and Database Compatibilities must be the following: **Archive Contents**: Configuration data. **Database Compatibility**: The databases are compatible. ***Note***: The following is expected output for Topology Compatibility Check since we are restoring from an existing backed up database to a database with just one NOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. ***Note***: We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility. 4. If the verification is successful, click **Back**.

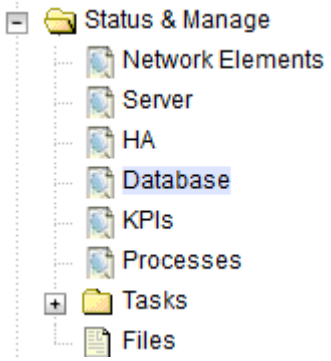
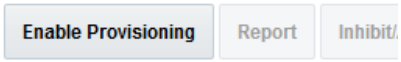
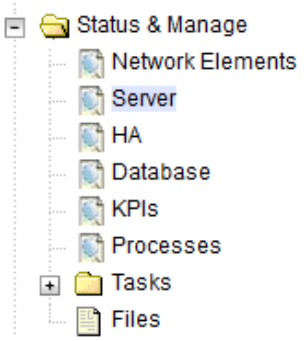
Procedure 3. Recovery Scenario 3

10. ☐	**Active NOAM**: Restore the database	1. From **Status & Manage > Database**. 2. Select the **Active NOAM** server and click **Restore**.  3. Select the proper backup provisioning and configuration file.  4. Click **OK**.  5. If you get errors related to the warnings highlighted in the previous step, that is expected. If no other errors are displayed, mark the **Force** checkbox as shown above and Click **OK** to proceed with the DB restore. ***Note***: After the restore has started, the user is logged out of XMI NO GUI since the restored topology is old data.

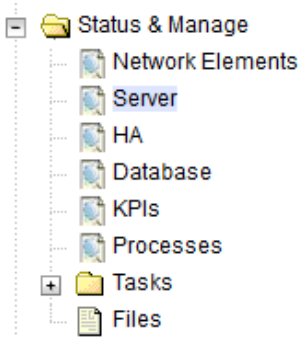
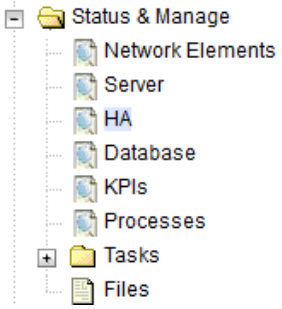
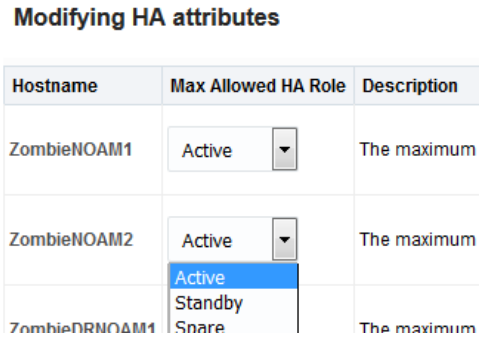
Procedure 3. Recovery Scenario 3

11. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. 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). ***Note***: Do not pay attention to alarms until all the servers in the system are completely restored. ***Note***: The Configuration and Maintenance information is in the same state it was when backed up during initial backup.
13. ☐	**Active NOAM**: Login	Log into the recovered active NOAM using SSH terminal as **admusr** user.

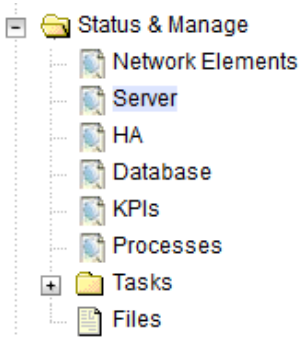
Procedure 3. Recovery Scenario 3

14. ☐	**NOAM GUI**: Enable provisioning	1. Navigate to **Status & Manage > Database**.  2. Click **Enable Provisioning**.  A confirmation window displays. Click **OK** to enable provisioning.
15. ☐	**NOAM VIP GUI**: Recover standby NOAM	Install the second NOAM server by executing these procedures from reference [1]: • Execute Configure the Second NOAM Server, steps 3-5 and 7 ***Note***: If topology or nodeID alarms are persistent after the database restore, refer to Appendix F to Check and Create Backup Directory.
16. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**.  3. Click **OK** on confirmation screen.
17. ☐	Recover remaining failed SOAM server(s), if needed	1. Install the SOAM servers by executing Configure the SOAM Servers, steps 1 and 3-7 from reference [1]. ***Note***: Wait for the server to reboot. 2. Repeat for each remaining SOAM server (standby, spare).

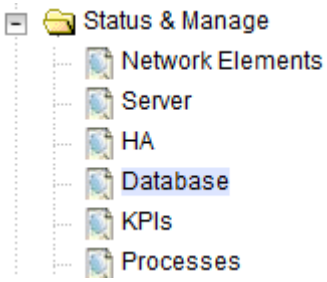
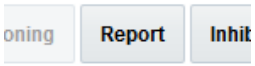
Procedure 3. Recovery Scenario 3

18. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**. 
19. ☐	**NOAM VIP GUI**: Set HA on all C-level servers	1. Navigate to **Status & Manage > HA**.  2. Click **Edit** at the bottom of the screen. 3. For each server with a Max Allowed HA Role set to not active, set it to **Active**.  4. Click **OK**.

Procedure 3. Recovery Scenario 3

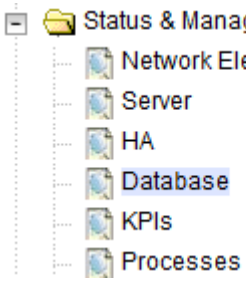
20. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select each recovered server and click **Restart**. 
21. ☐	**Active NOAM**: Perform key exchange between the active-NOAM and recovered servers	1. Establish an SSH session to the active NOAM and login as **admusr**. 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	**Note for PCA Activation:** If you have PCA installed in the system being recovered, re-activate PCA by executing PCA Activation on Entire Server on Recovered NOAM Server and PCA Activation on Active SOAM Server from [3]. ***Note***: While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: `iload#31000{S/W Fault}` ***Note***: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature. Refer to section 1.4 Optional Features to activate any features previously activated.

Procedure 3. Recovery Scenario 3

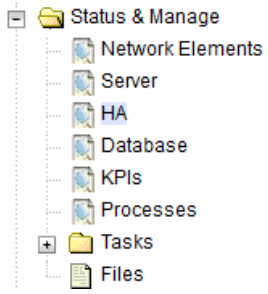
23. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status & Manage > Database**.
		 
		2. Select the active NOAM server and click **Report**.
		 
		The following screen displays:
		Main Menu: Status & Manage -> Database [Report]
		`dsr Database Status Report`
		`Report Generated: Tue Oct 11 13:24:26 2016 EDT`
		`From: Active Network OAM&P on host ZombieNOAM1`
		`Report Version: 8.0.0.0.0-80.9.0`
		`User: guiadmin`
		`General`
		`Hostname : ZombieNOAM1`
		`Database Birthday : 2016-07-11 11:21:50 EDT`
		`Appworks Database Version : 6.0`
		`Application Database Version :`
		`Capacities and Utilization`
		`Disk Utilization 8.4%: 585M used of 7.0G total, 6.0G available`
		`Memory Utilization 0.0%: used of total, 0M available`
		Click **Save** and save the report to your local machine.

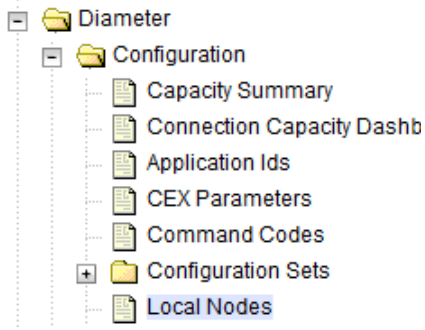
Procedure 3. Recovery Scenario 3

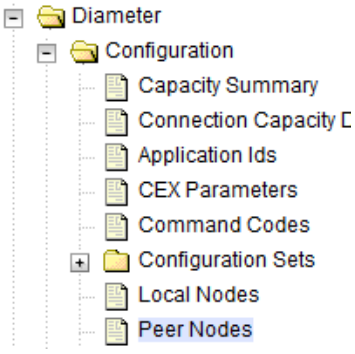
24. ☐	**Active NOAM**: Verify replication between servers	1. Log into the active NOAM using SSH terminal as **admusr**.
		2. Execute this command:
		`$ sudo irepstat –m`
		Output:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`RDU06-MP1 -- Stby`
		`  BC From RDU06-SO1 Active  0  0.50 ^0.17%cpu 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 & Manage > 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 the status is **Normal**: **Main Menu: Status & Manage -> Database** Filter* Info* Tasks Network Element / Server / Role / OAM Max HA Role / Application Max HA Role / Status SOAM_NE / SO1 / System OAM / Standby / N/A / Normal SOAM_NE / SO2 / System OAM / Active / N/A / Normal NOAM_NE / NO2 / Network OAM&P / Standby / N/A / Normal SOAM_NE / DAMP1 / MP / Active / Active / Normal NOAM_NE / NO1 / Network OAM&P / Active / N/A / Normal

Procedure 3. Recovery Scenario 3

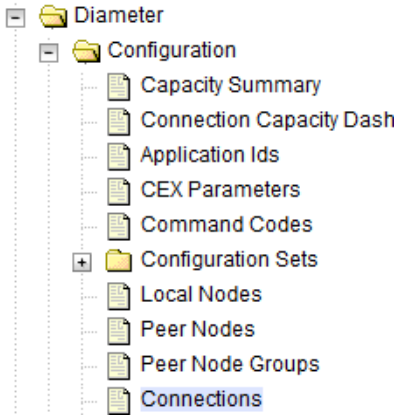
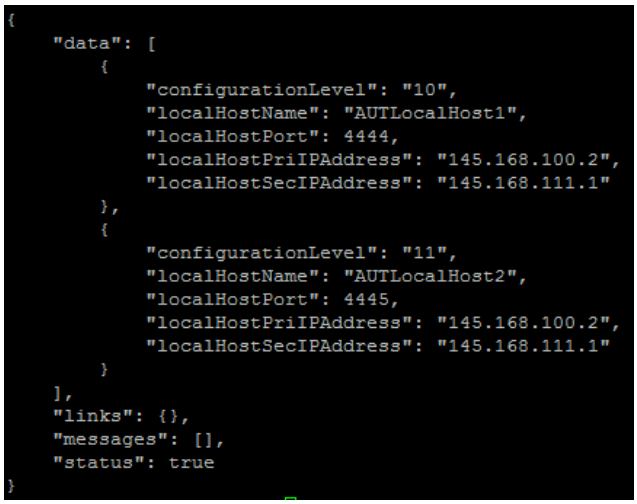
<table>
<tr>
<td>26. ☐</td>
<td>NOAM VIP GUI: Verify the HA status</td>
<td>
1. Navigate to Status and Manage > HA.


2. Select the row for all of the servers.
3. Verify the HA Role is either Active or Standby.
<table>
<tr><th>Hostname</th><th>OAM HA Role</th><th>Application HA Role</th><th>Max Allowed HA Role</th></tr>
<tr><td>ZombieNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieDRNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieDRNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieSOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieSOAM2</td><td>Standby</td><td>N/A</td><td>Standby</td></tr>
</table>
</td>
</tr>
<tr>
<td>27. ☐</td>
<td>SOAM VIP GUI: Verify the local node info</td>
<td>
1. Navigate to Diameter > Configuration > Local Node.


2. Verify all the local nodes are shown.
</td>
</tr>
<tr>
<td>28. ☐</td>
<td>SOAM VIP GUI: Verify the peer node info</td>
<td>
1. Navigate to Diameter > Configuration > Peer Node.


2. Verify all the peer nodes are shown.
</td>
</tr>
</table>

Procedure 3. Recovery Scenario 3

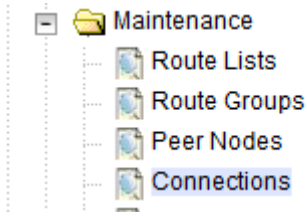
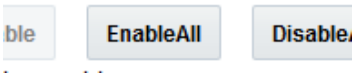
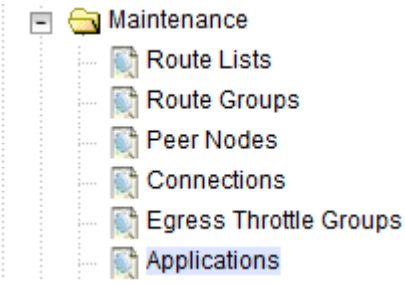
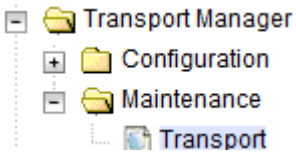
29. ☐	**SOAM VIP GUI**: Verify the connections info	1. Navigate to **Diameter > Configuration > Connections**.  2. Verify all the connections are shown.
30. ☐	For vSTP Only **SOAM VIP Server Console (Optional)**: Verify vSTP MP local node information	1. Log into the SOAM VIP server console as **admusr**.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

Procedure 3. Recovery Scenario 3

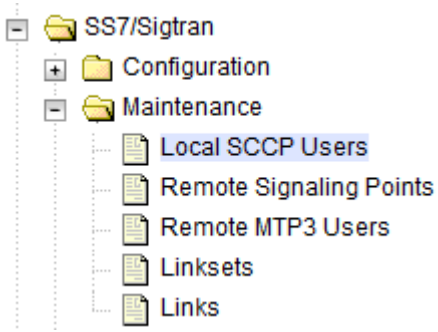
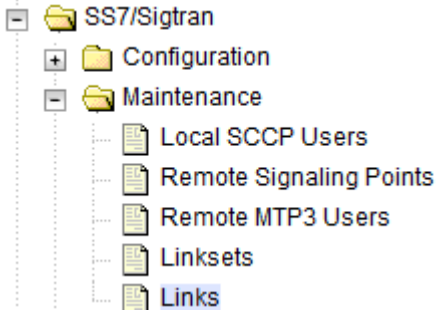
31. ☐	For vSTP Only
	SOAM VIP Server Console (Optional): Verify vSTP MP remote nodes information
		1. Log into the SOAM VIP server console as **admusr**.
		2. Execute the following command
		`[admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts`
		3. Verify the output similar to this output.
		{
		"data":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

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

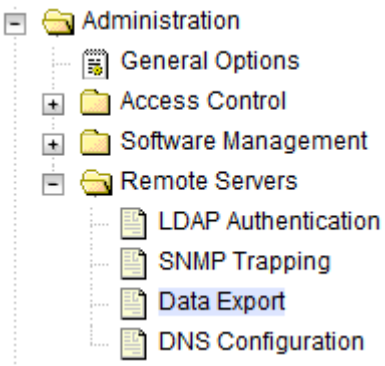
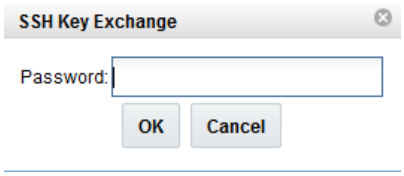
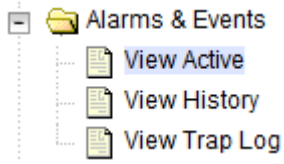
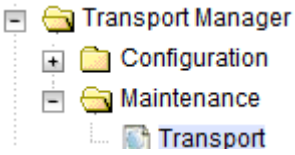
Procedure 3. Recovery Scenario 3

33. ☐	**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**.
34. ☐	**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**. 
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**.

Procedure 3. Recovery Scenario 3

36. ☐	**SOAM VIP GUI**: Re-enable MAPIWF application, if needed. This step is applicable when the MAP-IWF is activated.	1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.  2. Click the **Enable** button corresponding to MAPIWF Application Name.  3. Verify the SSN Status is **Enabled**.
37. ☐	**SOAM VIP GUI**: Re-enable links, if needed. This step is applicable when the MAP-IWF is activated.	1. Navigate to **SS7/Sigtran > Maintenance > Links**.  2. Click **Enable** for each link.  3. Verify the Operational Status for each link is **Up**.

Procedure 3. Recovery Scenario 3

38. ☐	**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**. 
39. ☐	**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).
40. ☐	**SOAM VIP GUI**: Re-enable transports, if needed	Navigate to **Transport Manager > Maintenance > Transport**.  Select each transport and click **Enable**.  Verify the Operational Status for each transport is **Up**.
41. ☐	Restore GUI usernames and passwords	If applicable, execute steps in section 5 to recover the user and group information restored.

Procedure 3. Recovery Scenario 3

42. ☐	Backup and archive all the databases from the recovered system	Execute Appendix E DSR Database Backup to back up the Configuration databases.

4.4 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 using 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 procedure 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 is intact at the active NOAM server and does not require restoration at the SO and MP servers
  - Re-apply signaling networks configuration if the failed blade is an MP

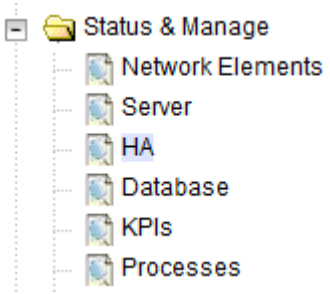
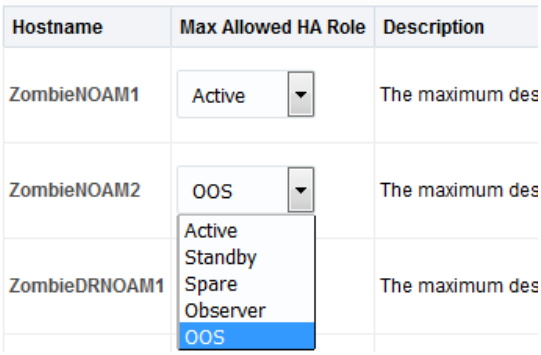
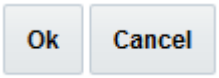
Procedure 4. Recovery Scenario 4

S T E P #	This procedure performs recovery if at least 1 NOAM server is intact and available and 1 SOAM server is intact and available. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Workaround	Refer to Appendix F to Check and Create Backup Directory.
2. ☐	Gather required materials	Gather the documents and required materials listed in section 3.1 Required Materials.

Procedure 4. Recovery Scenario 4

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

Procedure 4. Recovery Scenario 4

4. ☐	**Active NOAM**: Set failed servers to OOS	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. **Modifying HA attributes**  3. Set the Max Allowed HA Role to **OOS** for the failed servers. 4. Click **OK**. 
5. ☐	Recover the failed software	**For VMWare based deployments**: 1. For NOAMs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 2 (VMWare Only) Configure NOAM Guests Based On Resource Profile 2. For SOAMs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile 3. For failed MPs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager,

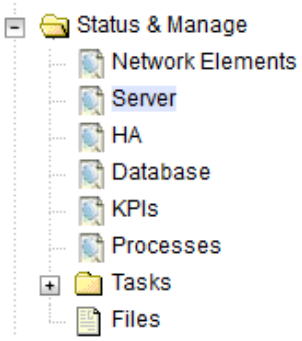
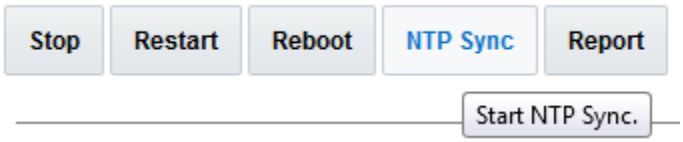
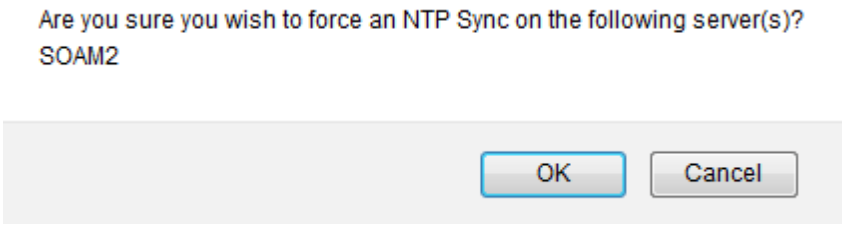
Procedure 4. Recovery Scenario 4

		skip this procedure to import OVA. b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile **For KVM/OpenStack based deployments**: 1. For NOAMs, execute the following procedures from reference [1]: a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 5 (KVM/OpenStack Only) Configure NOAM Guests Based On Resource Profile 2. For SOAMs, execute the following procedures from reference [1]: a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile 3. For failed MPs, execute the following procedures from reference [1]: a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this 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**: 1. Execute the following procedures from reference [1]: a. Procedure 7 (OVM-S/OVM-M) Import DSR OVA and Prepare for VM creation b. Procedure 8 (OVM-S/OVM-M) Configure each DSR VM While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs).
6. ☐	Repeat	If necessary, repeat step 5. for all remaining servers.

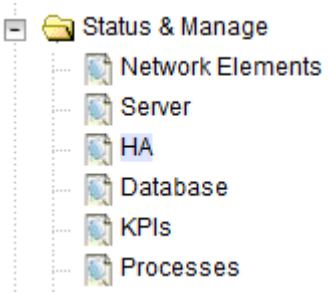
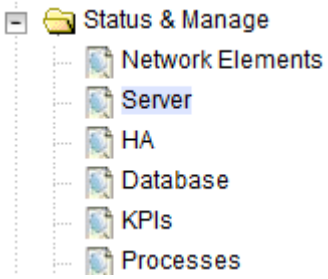
Procedure 4. Recovery Scenario 4

7. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 
8. ☐	**NOAM VIP GUI**: Recover standby NOAM	Install the second NOAM server by executing these procedures from reference [1]: • Execute Configure the Second NOAM Server, steps 3-5 and 7 • Execute Configure the NOAM Server Group, step 4 ***Note***: If topology or nodeID alarms are persistent after the database restore, refer to Appendix F to Check and Create Backup Directory.
9. ☐	Recover remaining failed SOAM server(s), if needed	1. Install the SOAM servers by executing Configure the SOAM Servers, steps 1 and 3-7 from reference [1]. ***Note***: Wait for the server to reboot. 2. Repeat for each remaining SOAM server (standby, spare).
10. ☐	**Recovered Server**: Login	Log into the recovered server using SSH terminal as **admusr** user.

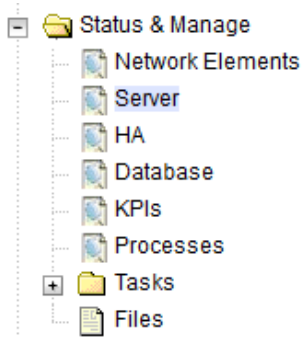
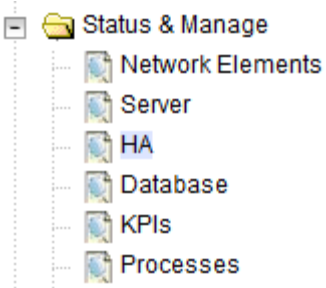
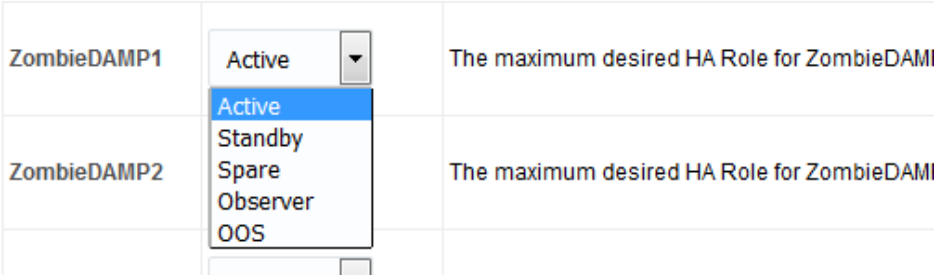
Procedure 4. Recovery Scenario 4

11. ☐	**Recovered Server**: Synchronize NTP	1. Navigate to **Status & Manage > Server**.  2. Select the recovered server and click **NTP Sync**.  3. Click **OK** to confirm. 

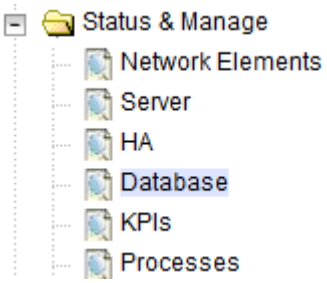
Procedure 4. Recovery Scenario 4

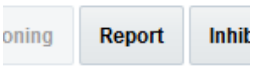
12. ☐	**NOAM VIP GUI**: Restart DSR application on recovered C-level servers	1. Navigate to **Status & Manage > HA**.  2. Click **Edit** at the bottom of the screen. 3. For each SOAM server with a Max Allowed HA Role set to **Standby**, set it to **Active**.  4. Click **OK**.
13. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**. 
14. ☐	**Active NOAM**: Perform key exchange between the active-NOAM and recovered servers (DA-MP, SBRs, IPFE, SS7-MP, and 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 Configure the MP Virtual Machines, steps 1, 11-14 (and 15 if required) of reference [1] for each server that has been recovered.

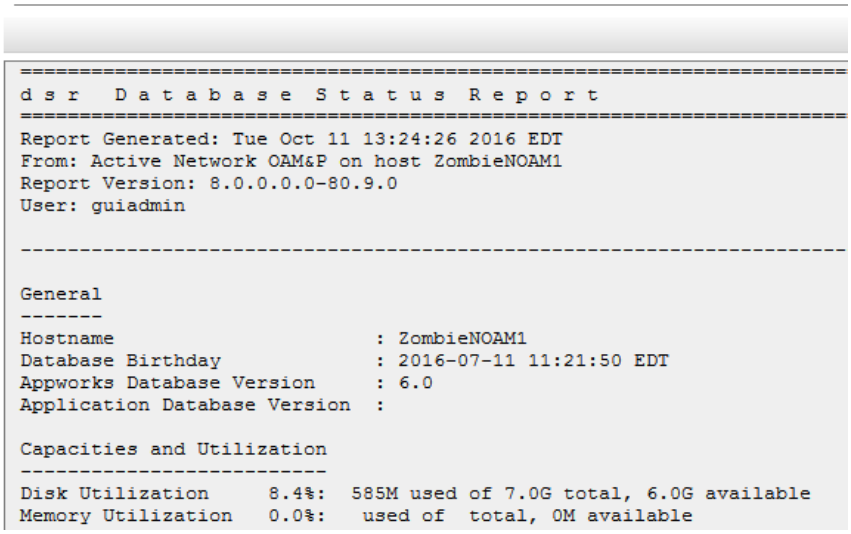
Procedure 4. Recovery Scenario 4

15. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**. 
16. ☐	**NOAM VIP GUI**: Restart DSR application on recovered C-level servers	3. Navigate to **Status & Manage > HA**.  4. Click **Edit** at the bottom of the screen. 5. For each SOAM server with a Max Allowed HA Role set to **Standby**, set it to **Active**.  6. Click **OK**.
17. ☐	**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.

Procedure 4. Recovery Scenario 4

<table>
<tr>
<td>18. ☐</td>
<td>Active NOAM: Activate optional features</td>
<td>
Note for PCA Activation:
If you have PCA installed in the system being recovered, re-activate PCA by executing PCA Activation on Entire Server on Recovered NOAM Server and PCA Activation on Active SOAM Server from [3].
Note: While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:
<code>iload#31000{S/W Fault}</code>
Note: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.
Refer to section 1.4 Optional Features to activate any features previously activated.
</td>
</tr>
<tr>
<td>19. ☐</td>
<td>NOAM VIP GUI: Fetch and store the database report for the newly restored data and save it</td>
<td>
1. Navigate to Status & Manage > Database.


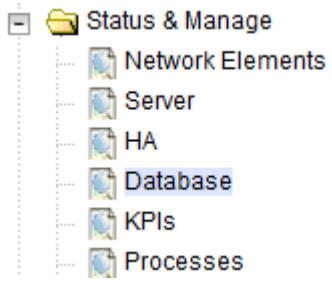
2. Select the active NOAM server and click Report.


The following screen displays:
Main Menu: Status & Manage -> Database [Report]


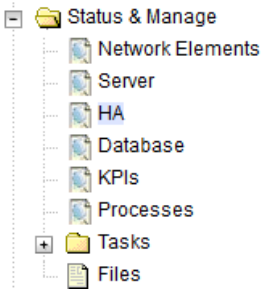
3. Click Save and save the report to your local machine.
</td>
</tr>
</table>

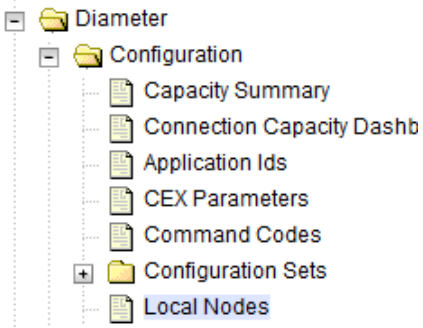
Procedure 4. Recovery Scenario 4

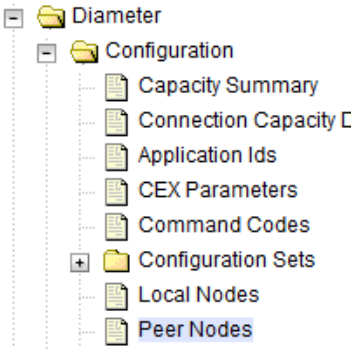
20. ☐	**Active NOAM**: Verify replication between servers	1. Log into the active NOAM using SSH terminal as **admusr**.
		2. Execute this command:
		`$ sudo irepstat -m`
		Output:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`RDU06-MP1 -- Stby`
		`  BC From RDU06-SO1 Active  0  0.50 ^0.17%cpu 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`

21. ☐	**NOAM VIP GUI**: Verify the database states	1. Navigate to **Status & Manage > 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 the status is **Normal**: **Main Menu: Status & Manage -> Database** Filter* Info* Tasks Network Element / Server / Role / OAM Max HA Role / Application Max HA Role / Status SOAM_NE / SO1 / System OAM / Standby / N/A / Normal SOAM_NE / SO2 / System OAM / Active / N/A / Normal NOAM_NE / NO2 / Network OAM&P / Standby / N/A / Normal SOAM_NE / DAMP1 / MP / Active / Active / Normal NOAM_NE / NO1 / Network OAM&P / Active / N/A / Normal

Procedure 4. Recovery Scenario 4

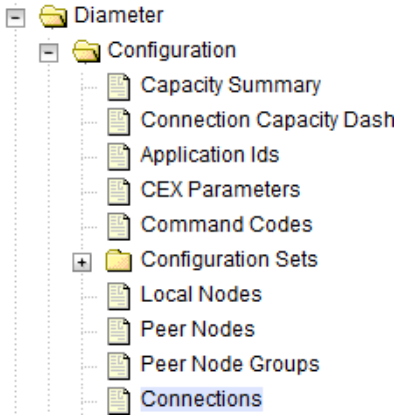
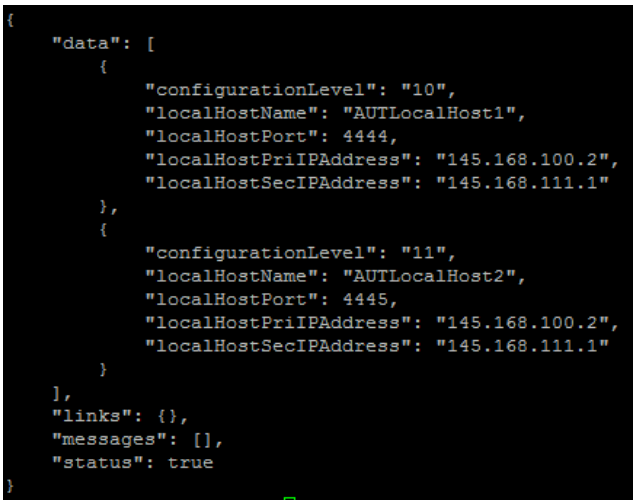
<table>
<tr>
<td>22. ☐</td>
<td>NOAM VIP GUI: Verify the HA status</td>
<td>
1. Navigate to Status and Manage > HA.


2. Select the row for all of the servers.
3. Verify the HA Role is either Active or Standby.
<table>
<tr><th>Hostname</th><th>OAM HA Role</th><th>Application HA Role</th><th>Max Allowed HA Role</th></tr>
<tr><td>ZombieNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieDRNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieDRNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieSOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieSOAM2</td><td>Standby</td><td>N/A</td><td>Standby</td></tr>
</table>
</td>
</tr>
<tr>
<td>23. ☐</td>
<td>SOAM VIP GUI: Verify the local node info</td>
<td>
1. Navigate to Diameter > Configuration > Local Node.


2. Verify all the local nodes are shown.
</td>
</tr>
<tr>
<td>24. ☐</td>
<td>SOAM VIP GUI: Verify the peer node info</td>
<td>
1. Navigate to Diameter > Configuration > Peer Node.


2. Verify all the peer nodes are shown.
</td>
</tr>
</table>

Procedure 4. Recovery Scenario 4

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

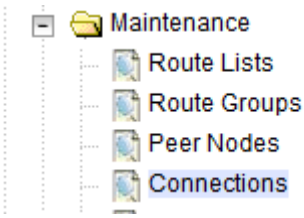
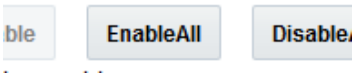
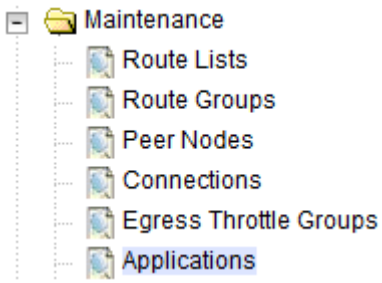
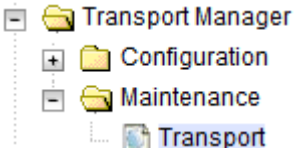
Procedure 4. Recovery Scenario 4

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

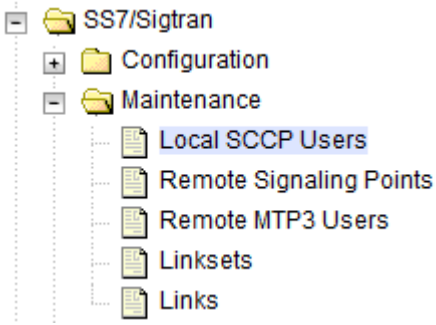
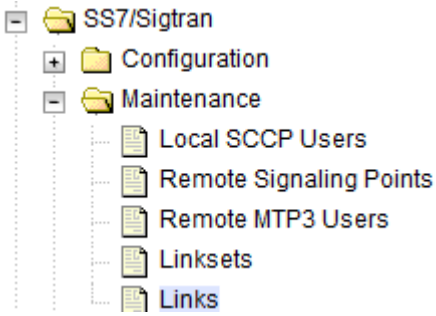
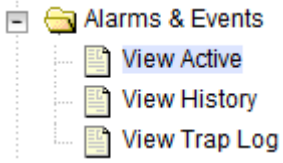
28. ☐	For vSTP Only
	SOAM VIP Server Console (Optional): Verify the vSTP MP connections information
		1. Log into the SOAM VIP server console as **admusr**.
		2. Execute the following command
		`[admusr@SOAM1 ~]$ mmiclient.py /vstp/connections`
		3. Verify the output similar to this output.
		{
		"data":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

29. ☐	**MP Servers**: Disable SCTP Auth Flag	For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [1]. Execute this procedure on all failed MP servers.

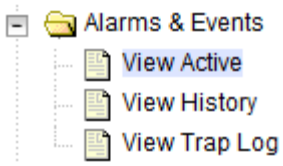
Procedure 4. Recovery Scenario 4

30. ☐	**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.
31. ☐	**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**. 
32. ☐	**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 4. Recovery Scenario 4

33. ☐	**SOAM VIP GUI**: Re-enable MAPIWF application, if needed. This step is applicable when the MAP-IWF is activated.	1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.  2. Click the **Enable** button corresponding to MAPIWF Application Name.  3. Verify the SSN Status is **Enabled**.
34. ☐	**SOAM VIP GUI**: Re-enable links, if needed. This step is applicable when the MAP-IWF is activated.	1. Navigate to **SS7/Sigtran > Maintenance > Links**.  2. Click **Enable** for each link.  3. Verify the Operational Status for each link is **Up**.
35. ☐	**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 4. Recovery Scenario 4

36. ☐	**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).

37. ☐	Restart oampAgent, if needed	***Note***: If alarm 10012: **The responder for a monitored table failed to respond to a table change** displays, 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`

38. ☐	Backup and archive all the databases from the recovered system	Execute Appendix E DSR Database Backup to back up the Configuration databases.

4.5 Recovery Scenario 5 — Both NOAM Servers Failed with DR-NOAM Available

For a partial outage with both NOAM servers failed but a DR NOAM available, the DR NOAM is switched from secondary to primary then recovers the failed NOAM servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedure 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 software
  - 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 software
  - Recover the software
  - The database in intact at the active NOAM server and does not require restoration at the SOAM and MP servers

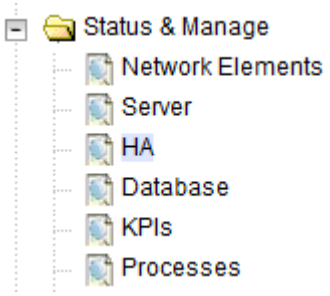
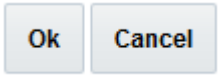
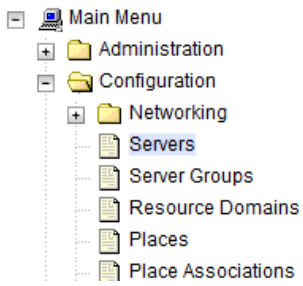
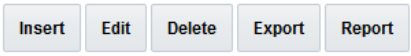
Procedure 5. Recovery Scenario 5

S T E P #	This procedure performs recovery if both NOAM servers have failed but a DR NOAM is available Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Workaround	Refer to Appendix F to Check and Create Backup Directory.
2. ☐	Gather required materials	Gather the documents and required materials listed in section 3.1 Required Materials.
3. ☐	Switch DR NOAM to primary	Refer to [2] DSR/SDS 8.2 NOAM Failover User's Guide.
4. ☐	Recover the failed software	**For VMWare based deployments**: 1. For NOAMs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 2 (VMWare Only) Configure NOAM Guests Based On Resource Profile 2. For SOAMs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile 3. For failed MPs, execute the following procedures from reference [1]: a. Procedure 1 (VMWare) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile **For KVM/OpenStack based deployments**: 1. For NOAMs, execute the following procedures from reference [1]: a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. b. Procedure 5 (KVM/OpenStack Only) Configure NOAM Guests Based On Resource Profile 2. For SOAMs, execute the following procedures from reference [1]: a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.

Procedure 5. Recovery Scenario 5

		b. Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile 3. For failed MPs, execute the following procedures from reference [1]: a. Procedure 4 (KVM/OpenStack) Import DSR OVA If OVA is already imported and present in the Infrastructure Manager, skip this 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**: 1. Execute the following procedures from reference [1]: a. Procedure 7 (OVM-S/OVM-M) Import DSR OVA and Prepare for VM creation b. Procedure 8 (OVM-S/OVM-M) Configure each DSR VM While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs).
5. ☐	Recover failed SOAMs	If all SOAM servers failed, execute Procedure 2.
6. ☐	**DR-NOAM VIP GUI**: Login	1. Establish a GUI session on the DR-NOAM server by using the VIP address of the DR-NOAM server. Open the web browser and enter a URL of: `http://<Primary_DR-NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 

Procedure 5. Recovery Scenario 5

7. ☐	**DR-NOAM VIP GUI**: Set failed NOAM servers to standby	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Set the Max Allowed HA Role to **Standby** for the failed servers. 4. Click **OK**. 
8. ☐	**DR-NOAM VIP GUI**: Export the initial configuration	1. Navigate to **Configuration > Servers**.  2. From the GUI screen, 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 the **admusr** user. 2. 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`

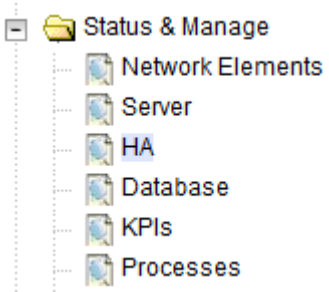
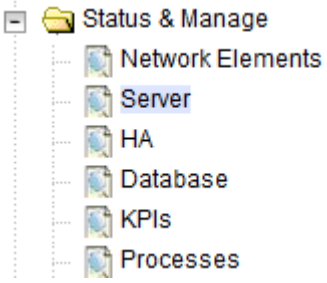
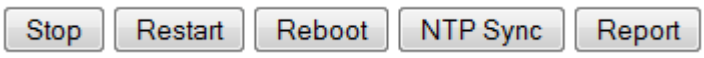
Procedure 5. Recovery Scenario 5

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).
		2. Login as the **admusr** user.
		3. 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.
		4. Verify awpushcfg was called by checking the following file.
		`$ sudo cat /var/TKLC/appw/logs/Process/install.log`
		Verify this message displays:
		`[SUCCESS] script completed successfully!`
		5. Reboot the server:
		`$ sudo init 6`
		6. Wait for the server to reboot.

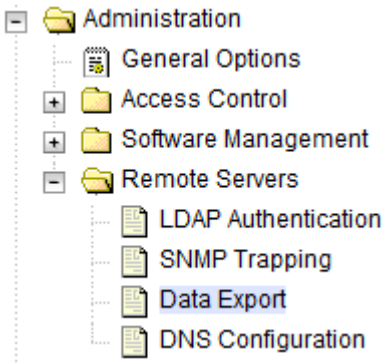
11. ☐	**Recovered NOAM Server**: Verify server health	Execute this command on the failed NOAM server and make sure no errors are returned:
		`$ sudo syscheck`
		`Running modules in class hardware...OK`
		`Running modules in class disk...OK`
		`Running modules in class net...OK`
		`Running modules in class system...OK`
		`Running modules in class proc...OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

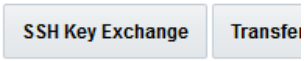
12. ☐	Repeat for additional 2nd failed NOAM	Repeat steps 8. - 11. for the 2nd failed NOAM server.
13. ☐	Perform keyexchange between active NOAM and recovered NOAM servers	1. From a terminal window connection on the active NOAM as the **admusr** user, exchange SSH keys for **admusr** between the active NOAM and the recovered NOAM servers using the keyexchange utility, using the host names of the recovered NOAMs. 2. When prompted for the password, enter the password for the **admusr** user of the recovered NOAM servers. `$ keyexchange admusr@<Recovered_NOAM Hostname>`

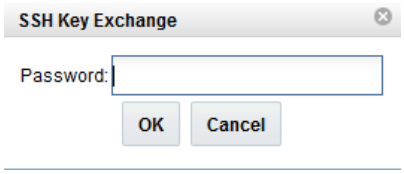
Procedure 5. Recovery Scenario 5

14. ☐	**NOAM VIP GUI**: Set HA on recovered NOAMs	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. For each NOAM server with a Max Allowed HA Role set to **Standby**, set it to **Active**.  4. Click **OK**.
15. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select each recovered NOAM server and click **Restart**. 

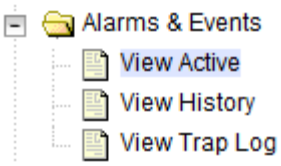
Procedure 5. Recovery Scenario 5

<table>
<tr>
<td>16. ☐</td>
<td>Recovered NOAM Servers: Activate optional features</td>
<td>Map-Diameter Interworking (MAP-IWF) and/or Policy and Charging Application (PCA) Only
Activate the features Map-Diameter Interworking (MAP-IWF) and Policy and Charging Application (PCA) as follows:
For PCA:
1. Establish SSH sessions to the all the recovered NOAM servers and login as admusr. Refer [3] DSR PCA Activation Guide and execute PCA Activation on Standby NOAM Server on all recovered NOAM servers to re-activate PCA.
2. Establish SSH session to the recovered active NOAM and login as admusr.
For MAP-IWF:
1. Establish SSH session to the recovered active NOAM and login as admusr. Refer to [4] DSR MAP-Diameter IWF Feature Activation Procedure to activate Map-Diameter Interworking (MAP-IWF).
Note: While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:
<code>iload#31000{S/W Fault}</code>
Note: If any of the MPs are failed and recovered, then these MP servers should be restarted after activation of the feature.</td>
</tr>
<tr>
<td>17. ☐</td>
<td>Switch DR NOAM back to secondary</td>
<td>Once the system have been recovered:
Refer Document [2] DSR/SDS 8.2 NOAM Failover User's Guide.</td>
</tr>
<tr>
<td>18. ☐</td>
<td>NOAM VIP GUI: Perform key exchange with export server</td>
<td>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.
 
</td>
</tr>
</table>

Procedure 5. Recovery Scenario 5

19. ☐	**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).
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, or any C-level servers.

4.6 Recovery Scenario 6 — Database Recovery — Case 1

For a partial outage with

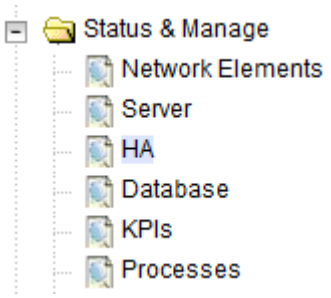
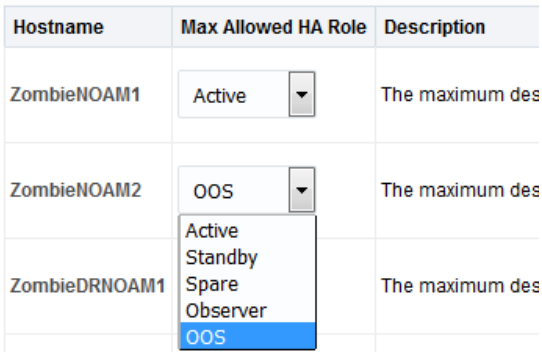
- Server having a corrupted database
- Replication channel from parent is inhibited because of upgrade activity or
- Server is in a different release then that of its active parent because of upgrade activity.
- Verify the server runtime backup files, performed at the start of the upgrade, are present 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 is replaced by the server runtime backup. Any configuration done after taking the backup is not available post recovery.

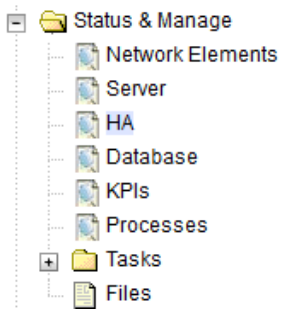
Procedure 6. Recovery Scenario 6 (Case 1)

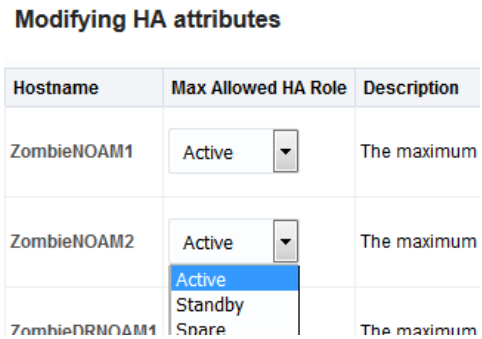
S T E P #	This procedure performs recovery if database is corrupted in the system Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Workaround	Refer to Appendix F to Check and Create Backup Directory.

Procedure 6. Recovery Scenario 6 (Case 1)

2. ☐	**NOAM VIP GUI**: Set failed servers to standby	1. Navigate to **Status & Manage > HA**.  2. Select **Edit**. **Modifying HA attributes**  3. Set the Max Allowed HA Role 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**: Change runlevel to 3	Bring the system to runlevel 3. `$ sudo init 3`
5. ☐	**Server in Question**: Recover system	Execute this command and follow the instructions appearing in the console prompt. `$ sudo /usr/TKLC/appworks/sbin/backout_restore`
6. ☐	**Server in Question**: Change runlevel to 4	Bring the system back to runlevel 4. `$ sudo init 6`

Procedure 6. Recovery Scenario 6 (Case 1)

<table>
<tr>
<td>7. ☐</td>
<td>Server in Question: Verify the server</td>
<td>Verify if the processes are up and running.
<pre>$ sudo pm.getprocs</pre>
Example Output:
<pre>A 5139 cmha   Up   12/21 13:16:25 1 cmha
A 5140 cmplatalarm   Up   12/21 13:16:25 1 cmplatalarm
A 5143 cmsnmpsa   Up   12/21 13:16:25 1 cmsnmpsa -R 1.3.6.1.4.1.3
23.5.3.28.1
A 5145 cmsoapa   Up   12/21 13:16:25 1 cmsoapa
A 9969 eclipseHelp   Up   12/21 13:16:39 1 eclipseHelp
A 5149 idbsvc   Up   12/21 13:16:25 1 idbsvc -M10 -ME204 -D40 -
DE820 -W1 -S2
A 6149 idbunlock   Up   12/21 13:16:36 1 idbunlock -f
A 5151 inetmerge   Up   12/21 13:16:25 1 inetmerge
A 5155 inetrep   Up   12/21 13:16:25 1 inetrep
A 5160 oampAgent   Up   12/21 13:16:25 1 oampAgent
A 5164 pm.watchdog   Up   12/21 13:16:25 1 pm.watchdog
A 5167 raclerk   Up   12/21 13:16:25 1 raclerk -r 6000
A 5171 re.portmap   Up   12/21 13:16:25 1 re.portmap -c100
A 5174 statclerk   Up   12/21 13:16:25 1 statclerk -s -0
A 5177 vipmgr   Up   12/21 13:16:25 1 vipmgr
A   -1 AstateInit   Done 12/21 13:16:36 1 AstateInit
A   -1 auditPTask   Done 12/21 13:16:36 1 auditPeriodicTask
A   -1 auditTasks   Done 12/21 13:16:36 1 auditDefunctTasks
A   -1 guiReqMapLoad   Done 12/21 13:16:25 1 guiReqMapLoad
A   -1 mkdbhooks   Done 12/21 13:16:25 1 mkdbhooks
[root@MP-1 admusr]#</pre>
</td>
</tr>
<tr>
<td>8. ☐</td>
<td>NOAM VIP GUI: Set failed servers to active</td>
<td>1. Navigate to Status & Manage > HA.


2. Click Edit.
3. Select the failed server and set it to Active.


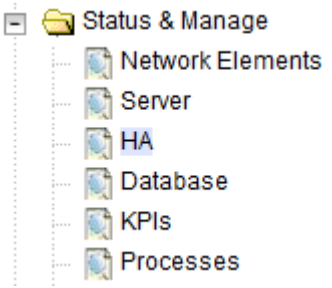
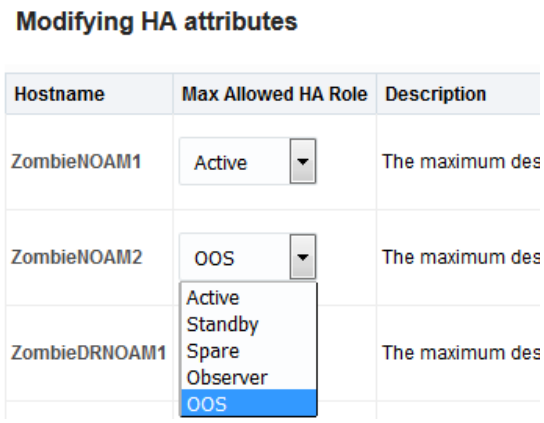
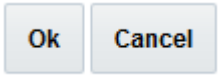
4. Click OK.</td>
</tr>
<tr>
<td>9. ☐</td>
<td>Backup and archive all the databases from the recovered system</td>
<td>Execute Appendix E DSR Database Backup to back up the Configuration databases.</td>
</tr>
</table>

4.7 Recovery Scenario 6 — Database Recovery — Case 2

For a partial outage with:

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

Procedure 7. Recovery Scenario 6 (Case 2)

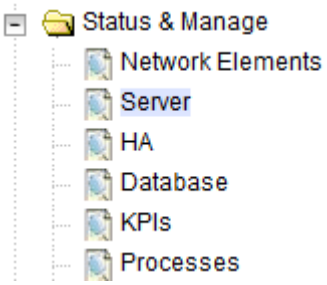
S T E P #	This procedure performs recovery if database got corrupted in the system and system is in the state to get replicated. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Workaround	Refer to Appendix F to Check and Create Backup Directory.
2. ☐	**NOAM VIP GUI**: Set failed servers to standby	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**.  3. Set the Max Allowed HA Role 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**.

Procedure 7. Recovery Scenario 6 (Case 2)

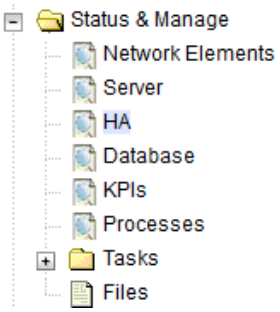
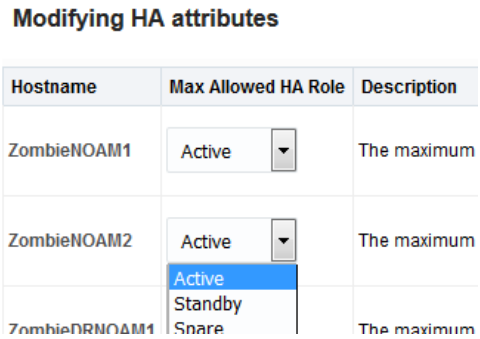
4. ☐	**Server in Question**: Take server out of service	Take the server out of service.
		`$ sudo bash -l`
		`$ prod.clobber`

5. ☐	**Server in Question**: Take server to DbUp state and start the application	Take the server to Dbup and start the DSR application.
		`$ sudo bash -l`
		`$ prod.start`

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

7. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select each recovered server and click **Restart**. 

Procedure 7. Recovery Scenario 6 (Case 2)

8. ☐	**NOAM VIP GUI**: Set failed servers to active	1. Navigate to **Status & Manage > HA**.  2. Click **Edit** at the bottom of the screen. 3. Select the failed server and set it to **Active**.  4. Click **OK**.
9. ☐	Backup and archive all the databases from the recovered system	Execute Appendix E 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.
```

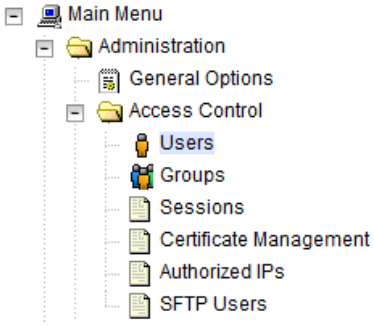
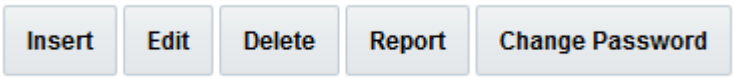
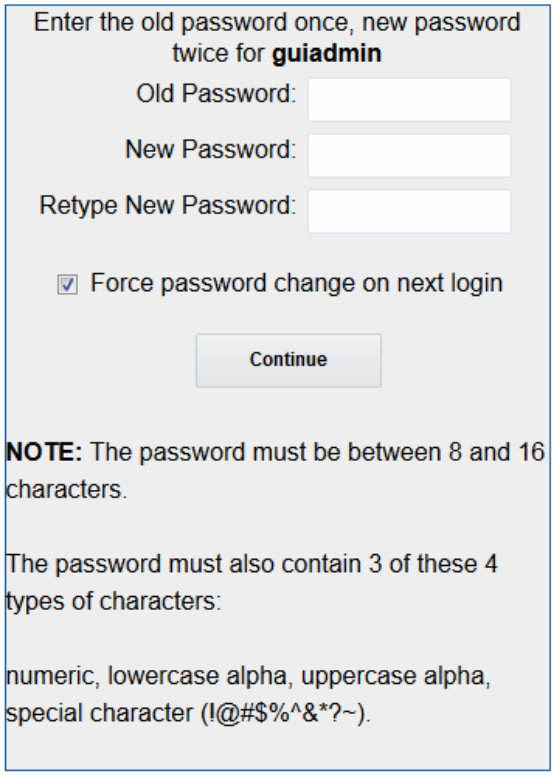
These users were removed before creation of the backup and archive file. They are reintroduced by system restoration of that file.

5.2 Keep a Restored User

Procedure 8. Keep Restored User

S T E P #		
	Perform this procedure to keep users 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, it is recommended to 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.
2. ☐	**After Restoration**: Log into the NOAM VIP	1. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 

Procedure 8. Keep Restored User

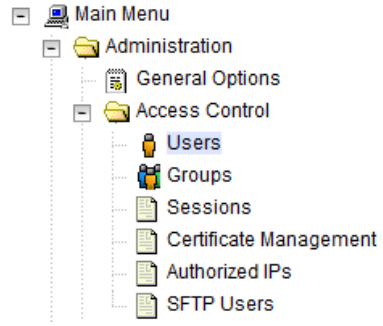
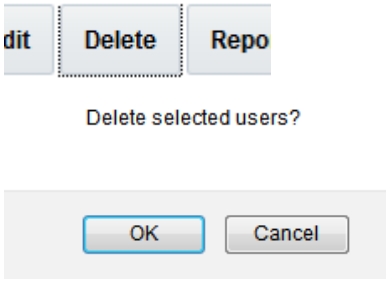
3. ☐	**After Restoration**: Reset user passwords	1. Navigate to **Administration > Access Control > Users**.  2. Select the user. 3. Click **Change Password**.  4. Type a new password.  5. Click **Continue**.

5.3 Remove a Restored User

Procedure 9. Remove the Restored User

S T E P #		
	Perform this procedure to remove users 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**After Restoration**: Log into the NOAM VIP	1. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. 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.

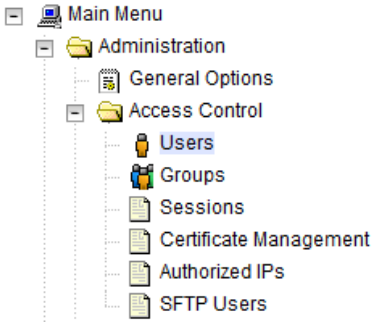
```
- User 'testuser' exists in current database but not in the selected backup
file.
```

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

S T E P #		
	Perform this procedure to remove users 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, it is recommended to 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. ☐	**Before Restoration**: Log into the NOAM VIP	1. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 

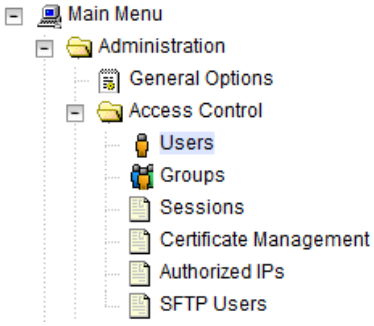
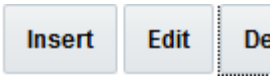
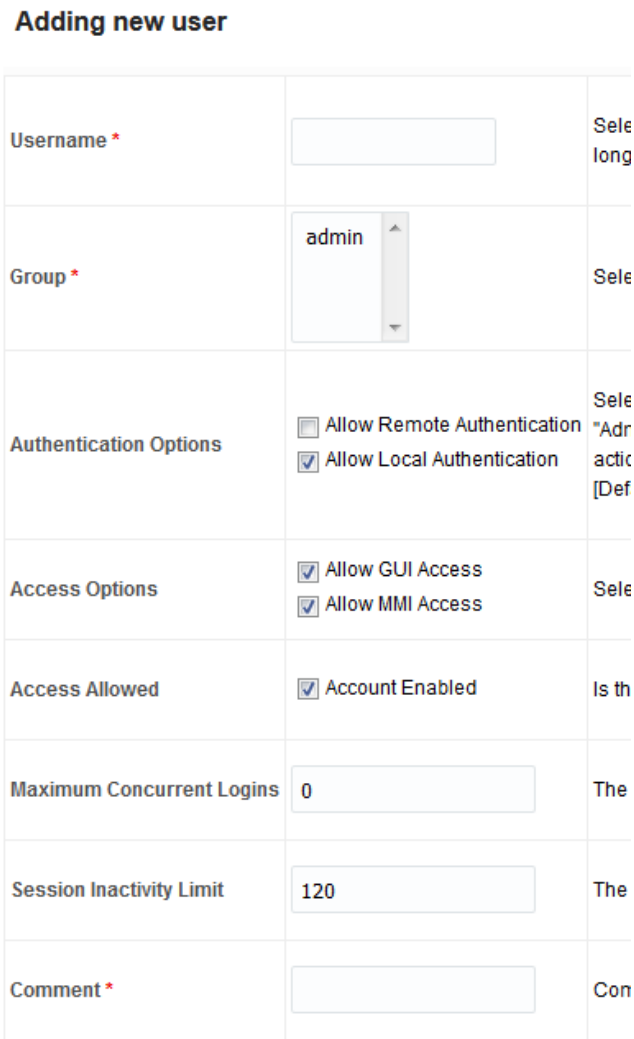
Procedure 10. Restore an Archive That Does Not Contain a Current User

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

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

5. ☐	After restoration: recreate affected user	1. Navigate to **Administration > Access Control > Users**.  2. Click **Insert**.  3. Recreate the user using the data collected from step 3.  4. Click **OK**.

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

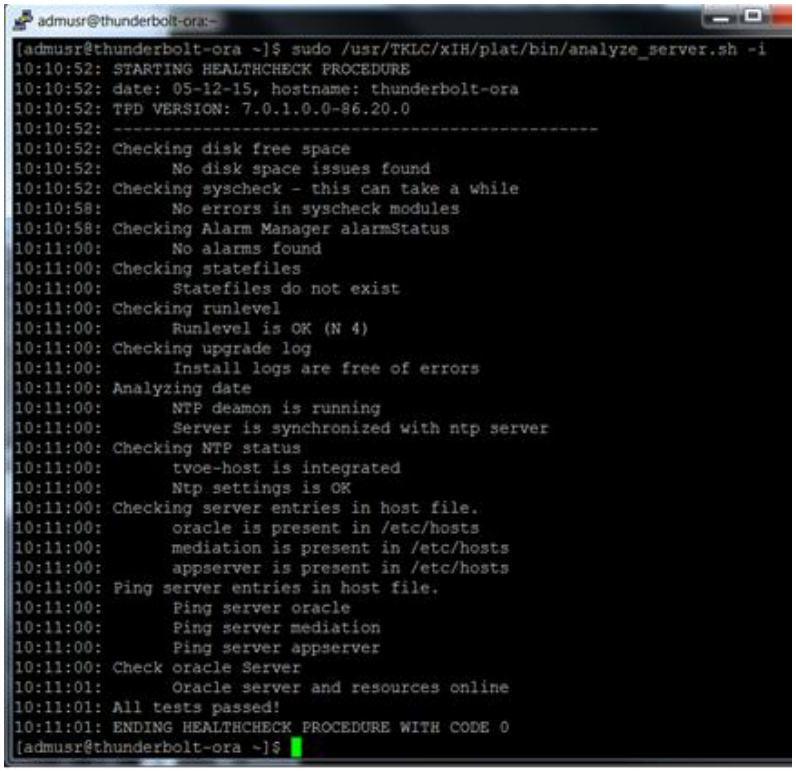
6. ☐	**After Restoration**: Repeat for additional users	Repeat step 5 to recreate additional users.
7. ☐	**After Restoration**: Reset the passwords	See Procedure 8 for resetting passwords for a user.

6. IDIH Disaster Recovery

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

Note: The fdconfig xml file for disaster recovery is exactly the same as the one for upgrade and this file should have been created during the latest upgrade or fresh installation. In case the file is not found, please refer to fresh installation section to re-create it.

Procedure 11. IDIH Disaster Recovery Preparation

STEP #	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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Oracle Gues**: Login and perform database and health check	1. Establish an SSH session to the Oracle gues and login as **admusr**. 2. Execute following command to set shared memory to unlimited: `$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i` Output: 

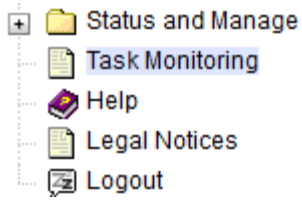
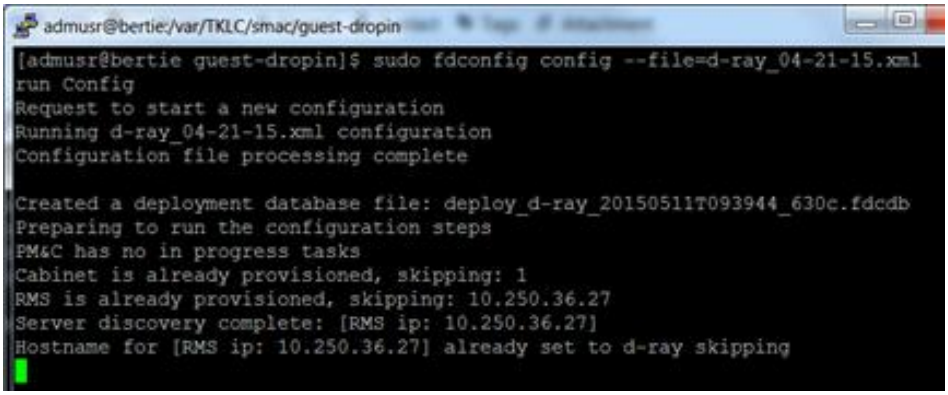
Procedure 11. IDIH Disaster Recovery Preparation

		Note: If this step fails, a re-installation is necessary using these procedures from reference [1]. **For VMWare-based deployments**: Section 5.6: (VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional) Section 5.9: Configure iDIH Virtual Machines **For KVM/OpenStack-based deployments**: Section 5.7: Create iDIH Virtual Machines (KVM/Openstack) Section 5.9: Configure iDIH Virtual Machines **For OVM-S/OVM-M-based deployments**: Section 5.8: Create iDIH Virtual Machines (OVM-S/OVM-M) Section 5.9: Configure iDIH Virtual Machines

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

STEP #	This procedure performs disaster recovery for the IDIH by re-installing the mediation and application servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Create iDIH Application and Mediation VMs	Execute the following procedure from [1] to recover the Application and Mediation VMs: **For VMWare-based deployments**: Section 5.6: (VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional) **For KVM/OpenStack-based deployments**: Section 5.7: Create iDIH Virtual Machines (KVM/Openstack) **For OVM-S/OVM-M-based deployments**: Section 5.8: Create iDIH Virtual Machines (OVM-S/OVM-M). Import three IDIH OVAs and create and configure a VM for each
2. ☐	Configure iDIH VM Networks	Execute the following procedure from [1] to configure the VM networks on the Application and Mediation VMs only: Section5.9: Configure iDIH VM Networks
3. ☐	Configure VMs	Execute the following procedure from [1]: Section 5.10, Post iDIH Installation Configuration, Procedure 38. Run Post Installation Scripts on iDIH VMs, steps 3 through 7
4. ☐	Integrate into DSR (Optional)	If integration is needed, execute the following procedure from [1]: Section 5.10, Post iDIH Installation Configuration, Pocedure 41. Integrate iDIH into DSR

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

5. ☐	**PMAC GUI**: Monitor the configuration	1. If not already done so, establish a GUI session on the PMAC server. 2. Navigate to **Status & Manage > Task Monitoring**.  3. Monitor the IDIH configuration to completion. Alternatively, you can monitor the fdconfig status through the command line after executing the fdconfig command: Example: 

Appendix A. Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost)

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

S T E P #	
	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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.
1. ☐	**Active NOAM**: Login	Log into the active NOAM server using SSH as **admusr**.

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

2. ☐	**Active NOAM**: Inhibit replication on all C-level servers	Execute the script from **/usr/TKLC/dsr/tools/InhibitReplication.sh**, if available.
		If the **/usr/TKLC/dsr/tools/** path does not have the **InhibitReplication.sh** script, then use this manual command.
		`/usr/TKLC/dsr/tools/InhibitReplication.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**.
		For example, if SOAM1 belongs to the site being recovered, then the server group is SO_SG.
		 

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

3. ☐	**Active NOAM**: Verify replication has been inhibited	After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.
		Verification of replication inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO_SG is set as **A B**.
		Execute this command:
		`$ 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 B. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost)

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

STEP #	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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.
1. ☐	**Active NOAM**: Login	Log into the active NOAM server using SSH as **admusr**.

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

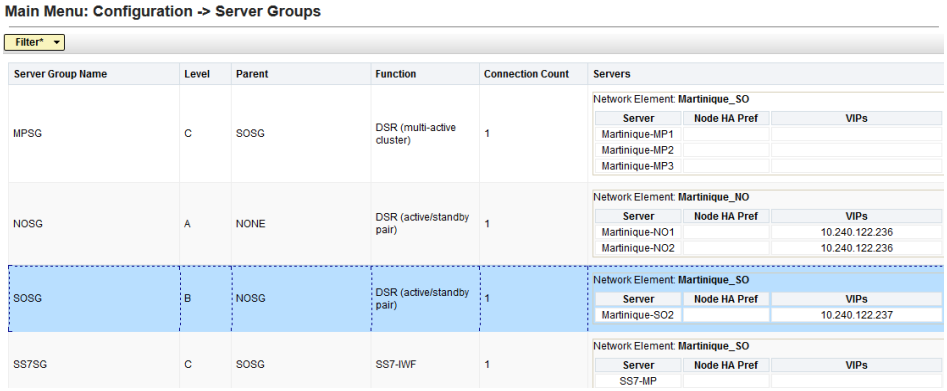
2. ☐	**Active NOAM**: Un-Inhibit replication on all C-level servers	Execute the script from **/usr/TKLC/dsr/tools/InhibitReplication.sh**, if available.
		If the **/usr/TKLC/dsr/tools/** path does not have the **InhibitReplication.sh** script, then use this manual command.
		`/usr/TKLC/dsr/tools/InhibitReplication.sh –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**.
		For example, if SOAM1 belongs to the site being recovered, then the server group is SO_SG.
		 

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

3. ☐	**Active NOAM**: Verify replication has been Inhibited	After executing above steps to un-inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.
		Verification of replication inhibition on MPs can be done by analyzing NodeInfo output. 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 C. Inhibit A and B Level Replication on C-level Servers

Procedure 15. Inhibit A and B Level Replication on C-level Servers

STEP #	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, it is recommended to 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 $(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<SOAM Site_NE name of the site>'"); do iset -finhibitRepPlans='A B' NodeInfo where "nodeName='$i'"; done` ***Note***: SOAM Site_NE name of the site can be found out by logging into the active NOAM GUI and navigating to **Configuration > Server Groups**. Please see the snapshot below for more details, for example, if ServerSO1 belongs to the site being recovered, then siteID is SO_HPC03. 

Procedure 15. Inhibit A and B Level Replication on C-level Servers

3. ☐	**Active NOAM**: Verify replication has been Inhibited	After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.
		Verification of replication inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site, for example, Site SO_HPC03 is set as **A B**.
		Execute this command:
		`$ 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 D. Un-Inhibit A and B Level Replication on C-level Servers

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

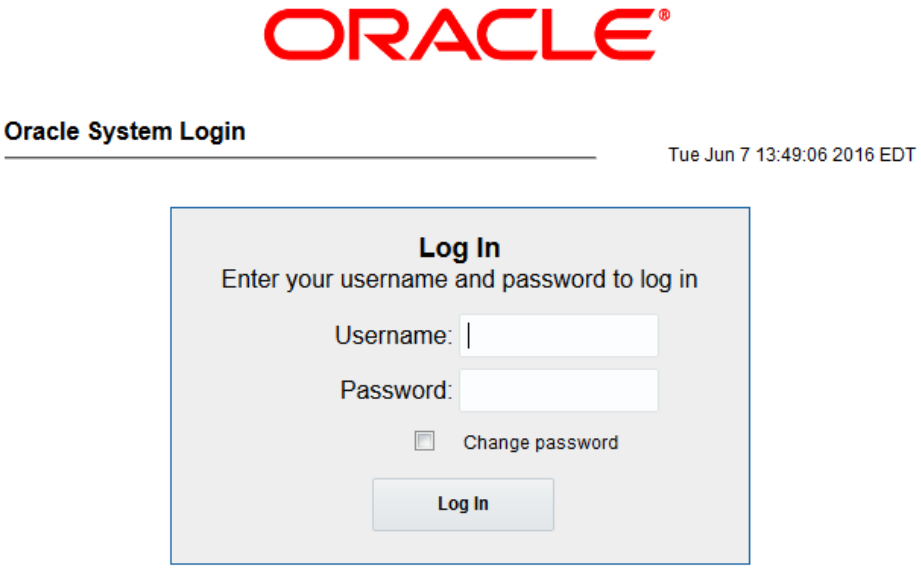
STEP #	This procedure un-inhibits A and B level replication on all C-level servers of this site Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.
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 $(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<SOAM_Site_NE_name>'"); do iset -finhibitRepPlans='' NodeInfo where "nodeName='$i'"; done` ***Note***: SOAM Site NE name of the site can be found out by logging into the active NOAM GUI and navigating to **Configuration > Server Groups**. Please see the snapshot below for more details, for example, if ServerSO1 belongs to the site being recovered, then siteID is SO_HPC03. **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

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

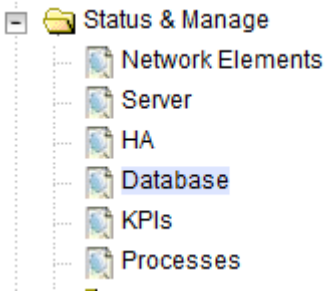
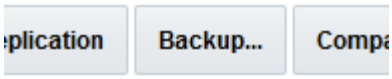
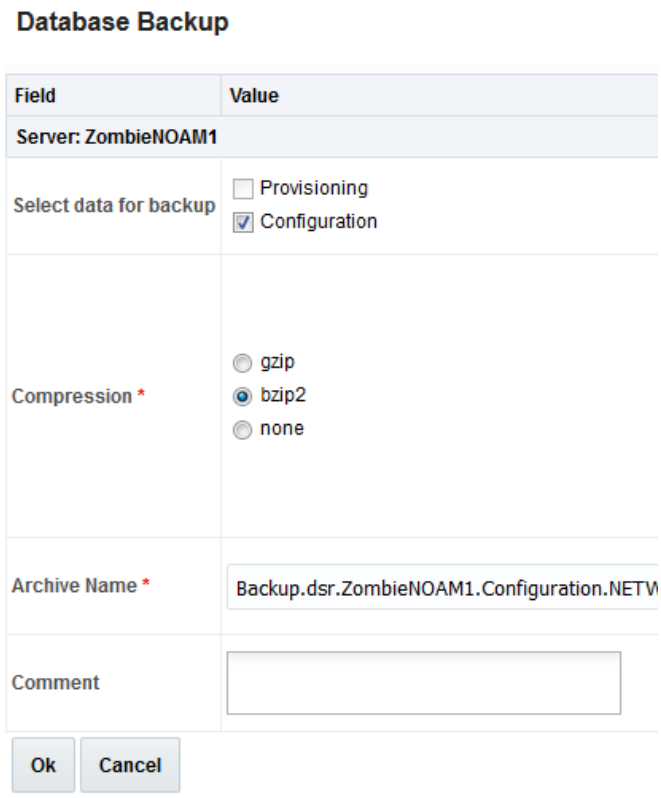
3. ☐	**Active NOAM**: Verify replication has been Inhibited	After executing above steps to un-inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.
		Verification of replication un-inhibition on MPs can be done by analyzing NodeInfo output. The InhibitRepPlans field for all the 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 E. DSR Database Backup

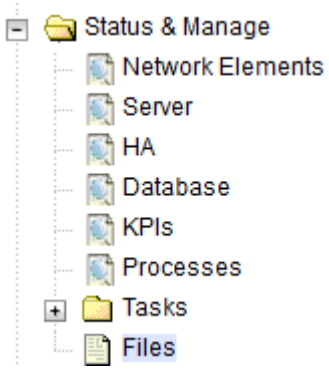
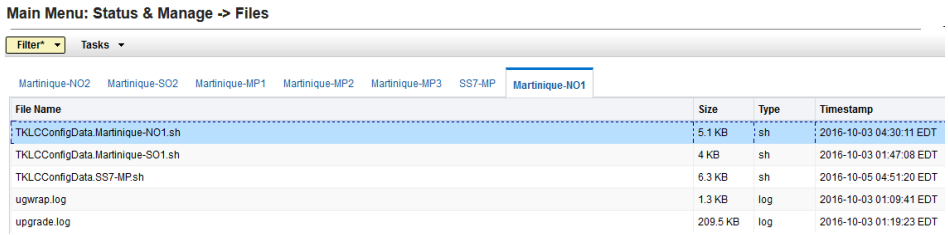
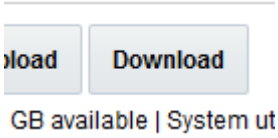
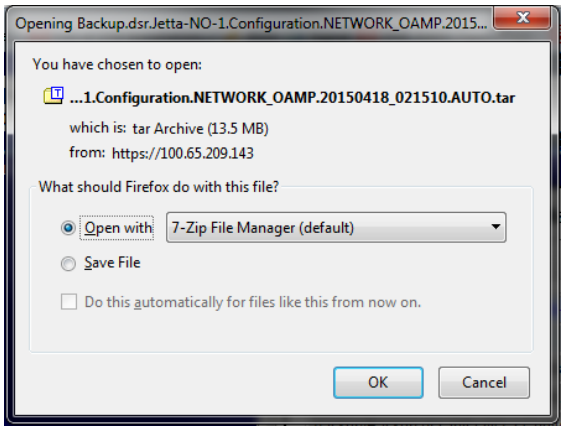
Procedure 17. DSR Database Backup

STEP #		
	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, it is recommended to 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 address of the NOAM or SOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM/SOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 

Procedure 17. DSR Database Backup

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

Procedure 17. DSR Database Backup

3. ☐	**NOAM/SOAM VIP**: Verify the backup file existence	1. Navigate to **Status & 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 F. Check and Create Backup Directory

Procedure 18. Backup Directory

S T E P #		
	This procedure checks and creates the 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, it is recommended to 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.

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`

Procedure 18. Backup Directory

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 N**etwork 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. 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.