Oracle® Communications

Diameter Signaling Router

C-Class Disaster Recovery Guide

Release 8.6.0.0.0

F56014-01

April 2022

Oracle Communications DSR C-Class Disaster Recovery User's Guide, Release 8.6.0.0.0

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

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

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

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

See more information My Oracle Support (MOS).

Table of Contents

1. Introduction

1.1 Purpose and Scope

This document describes procedures used to execute disaster recovery for DSR. This includes recovery of partial or complete loss of one or more DSR servers. The audience for this document includes GPS groups such as software engineering, product verification, documentation, customer service, software operations, and first office application. This document can be executed by Oracle customers as long as Oracle Customer Service personnel are involved and/or consulted. Executing this procedure also involves referring to and executing procedures in existing support documents.

Note: Components dependent on DSR might need to be recovered as well, for example, SDS, IDIH, and PMAC.

1.2 References

[1] TPD Initial Product Manufacture

[2] Platform Configuration Procedure Reference

[3] CPA Feature Activation Procedure

[4] DSR Mediation Feature Activation Procedure

[5] DSR FABR Feature Activation Procedure

[6] DSR RBAR Feature Activation Procedure

[7] DSR MAP-Diameter IWF Feature Activation Procedure

[8] DSR C-Class Software Installation and Configuration Procedure Part 2/2

[9] DSR GLA Feature Activation Procedure

[10] DSR C-Class Hardware and Software Installation Procedure 1/2

[11] PMAC Disaster Recovery Guide

[12] SDS C-Class Disaster Recovery Guide

[13] DSR PCA Activation Guide

[14] DSR DTLS Feature Activation Procedure

[15] DSR Security Guide

[16] DCA Framework and Application Activation and Deactivation Guide

[17] DSR/SDS 8.x NOAM Failover User's Guide

1.3 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CD	Compact Disk
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing

Acronym	Definition
FRU	Field Replaceable Unit
HP c-Class	HP blade server offering
iLO	Integrated Lights Out manager
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
MSA	Modular Smart Array
NB	NetBackup
OA	HP Onboard Administrator
OS	Operating System (for example, TPD)
RMS	Rack Mounted Server
PMAC	Platform Management & Configuration
SAN	Storage Area Network
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtual Operating Environment
VM	Virtual Machine
VSP	Virtual Serial Port
IPFE	IP Front End
PCA	Policy and Charging Application
IDIH	Integrated Diameter Intelligence Hub
SDS	Subscriber Database Server

1.4 Terminology

Table 2. Terminology

Term	Definition
Base hardware	Base hardware includes all hardware components (bare metal) and electrical wiring to allow a server to power on.
Base software	Base software includes installing the server's operating system: Oracle Platform Distribution (TPD).
Failed server	A failed server in disaster recovery context refers to a server that has suffered partial or complete software and/or hardware failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-install the software and/or hardware.
Software Centric	The business practice of delivering an Oracle software product, while relying upon the customer to procure the requisite hardware components. Oracle provides the hardware specifications, but does not provide the hardware or hardware firmware, and is not responsible for hardware installation, configuration, or maintenance.

Term	Definition
Enablement	The business practice of providing support services (hardware, software, documentation, etc.) that enable a 3rd party entity to install, configuration, and maintain Oracle products for Oracle customers.

1.5 Optional Features

Further configuration and/or installation steps are needed for optional features that may be present in this deployment. Refer to these documents for disaster recovery steps needed for their components.

Table 3. Optional Features

Feature	Document
Diameter Mediation	DSR Meta Administration Feature Activation Procedure
Full Address Based Resolution (FABR)	DSR FABR Feature Activation Procedure
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation Procedure
Policy and Charging Application (PCA)	DSR PCA Activation Guide
Gateway Location Application (GLA)	DSR GLA Feature Activation Procedure
Host Intrusion Detection System (HIDS)	DSR Security Guide (Section 3.2)
Diameter Custom Applications (DCA)	DCA Framework and Application Activation and Deactivation Guide

2. General Description

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

Table 4. Recovery Scenarios

Procedure	State of NOAM and/or SOAM server(s)
Recovery of the entire network from a total outage Recovery Scenario 1 (Complete Server Outage)	• All NOAM servers failed. • All SOAM servers failed. • MP servers may or may not be 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)	• At least 1 NOAM server is intact and available. • All SOAM servers failed. • MP servers may or may not be 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. • At least 1 SOAM server out of active, standby, spare is intact and available. • MP servers may or may not be failed.

Procedure	State of NOAM and/or SOAM server(s)
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)	• At least 1 NOAM server is intact and available. • At least 1 SOAM server out of active, standby, spare is intact and available. • 1 or more MP servers have failed.
Recovery Scenario 5 (Both NOAM Servers Failed with DR-NOAM Available)	• Both NOAM servers failed. • DR NOAM is available • SOAM servers may or may not be failed. • MP servers may or may not be failed.
Section Recovery Scenario 6 (Database Recovery) Recovery of one or more server with corrupt databases that cannot be restored using replication from the active parent node.	• Server is intact • Database gets corrupted on the server • Latest database backup of the corrupt server is present • Replication is inhibited (either manually or because of Comcol upgrade barrier)
Section Recovery Scenario 6: Case 1	• Server is intact • Database gets corrupted on the server • Replication is occurring to the server with corrupted database
Section Recovery Scenario 6: Case 2	• Server is intact • Database gets corrupted on the server • Latest Database backup of the corrupt server is NOT present • Replication is inhibited (either manually or because of comcol upgrade barrier)

Note: Aggregation switches, OA, or 6120/6125/3020 switches refer to Recover/Replace Failed 3rd Party Components (Switches, OAs).

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

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

2.1 Complete Server Outage (All Servers)

This is the worst-case scenario where all the servers in the network have suffered complete software and/or hardware failure. The servers are recovered using base recovery of hardware and software and then restoring database backups to the active NOAM and SOAM servers.

Database backups are taken from customer offsite backup storage locations (assuming these were performed and stored offsite before the outage). If no backup files are available, the only option is to

rebuild the entire network from scratch. The network data must be reconstructed from whatever sources are available, including entering all data manually.

2.2 Partial Server Outage with One NOAM Server Intact and Both SOAMs Failed

This case assumes at least one NOAM server is intact. All SOAM servers have failed and are recovered using base recovery of hardware and software. Database is restored on the SOAM server and replication recovers the database of the remaining servers.

2.3 Partial Server Outage with Both NOAM Servers Failed and One SOAM Server Intact

If both NOAM servers have suffered complete software and/or hardware failure (where DR-NOAMs are not present), but at least one SOAM server is available. Database is restored on the NOAM and replication recovers the database of the remaining servers.

2.4 Partial Server Outage with NOAM and One SOAM Server Intact

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

Note: This includes failures of any disaster recovery network NOAM servers.

2.5 Partial Service Outage with Corrupt Database

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

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

3. Procedure Overview

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

3.1 Required Materials

The following items are needed for disaster recovery:

1. A hardcopy of this document and hardcopies of all documents in the reference list
2. Hardcopy of all NAPD performed at the initial installation and network configuration of this customer's site. If the NAPD cannot be found, escalate this issue within My Oracle Support (MOS) until the NAPD documents can be located.
3. DSR recent backup files: electronic backup file (preferred) or hardcopy of all DSR configuration and provisioning data.
4. Latest Network Element report: Electronic file or hardcopy of Network Element report.
5. Oracle Tekelec Platform Distribution (TPD) Media (64 bits).
6. Platform Management and Configuration (PMAC) ISO or SW.
7. DSR CD-ROM (or ISO image file on USB Flash) of the target release.
8. TVOE Platform Media (64 bits)
9. The xml configuration files used to configure the switches, available on the PMAC server (or PMAC backup)

10. The switch backup files taken after the switch is configured, available on the PMAC server (or PMAC backup)
11. The network element XML file used for the blades initial configuration.
12. The HP firmware upgrade pack (or customer-provided firmware)
13. NetBackup Files if they exist. This may require the assistance of the customer's NetBackup administrator.
14. PMAC and TVOE backups (If available)
15. List of activated and enabled features
16. IDIH CD-ROM (or ISO image file on USB Flash) of the target release (If IDIH is being recovered)

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

Note: NOAMs are deployed using the fast deployment tool from the PMAC. In scenarios where both NOAMs are failed, this fast deployment file is used. In scenarios where only one NOAM is failed, the fast deployment file is NOT used.

SUDO

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

3.2 Disaster Recovery Strategy

Disaster recovery procedure execution is performed as part of a disaster recovery strategy with these basic steps:

1. Evaluate failure conditions in the network and determine that normal operations cannot continue without disaster recovery procedures. This means the failure conditions in the network match one of the failure scenarios described in section 2.
2. Read and review the content in this document.
3. Gather required materials in section Required Materials
4. From the failure conditions, determine the Recovery Scenario and procedure to follow (using Figure 1. Determining Recovery Scenario and Table 4. Recovery Scenarios
5. Execute appropriate recovery procedures (listed in Table 4. Recovery Scenarios).

Note: Refer to Appendix N for Database restore procedure.

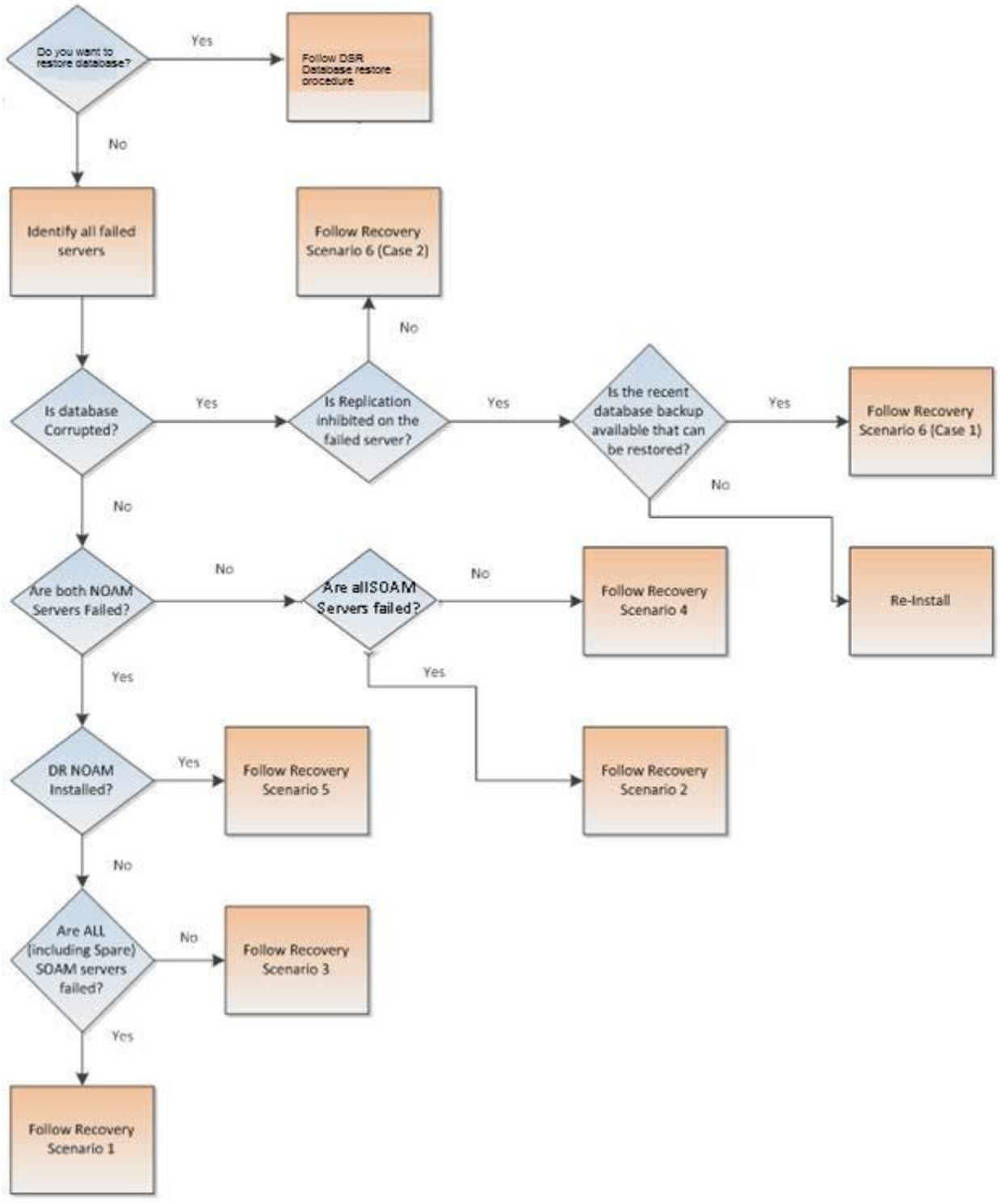


Figure 1. Determining Recovery Scenario

4. Disaster Recovery Procedure

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

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

!!WARNING!!

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

Recovering Base Hardware:

1. Hardware recovery is executed by the appropriate HW vender.
2. Base hardware replacement must be controlled by an engineer familiar with the DSR application.

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

!!WARNING!!

When there is a need to restore the database backup for NOAM and SOAM servers in any of Recovery Scenarios described in the following sections, the backup directory may not be there in the system since the system is DRed. In this case, please refer to Appendix L: Backup Directory for steps to check and create the backup directory.

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

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

4.1 Recovery Scenario 1 (Complete Server Outage)

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

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

- Recover base hardware and software for all rack mount servers and blades
  - Recover the base hardware. (By replacing the hardware and executing hardware configuration procedures) - Reference [10] for the DSR base hardware installation procedure
- Recover the **NOAM** servers by recovering executing the fast deployment xml file
  - Recover the NOAM database
  - Reconfigure the DSR application

- Recover the **SOAM** servers by recovering base hardware/software and/or VM image
  - Recover the SOAM database
  - Reconfigure the DSR Application
- Recover all **MP servers** by recovering base hardware and software
  - Reconfigure the signaling interface and routes on the MPs. The DSR software automatically reconfigures the signaling interface from the recovered database
  - Reference [8] for the applicable DSR software installation/configuration guide if any existing routes need to be altered
- Restart process and re-enable provisioning replication

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

Procedure 1. Recovery Scenario 1

This procedure performs recovery if both NOAM servers are failed and all SOAM servers are failed. This procedure also covers the C-level server failure. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Gather required materials	Gather the documents and required materials listed in Section Required Materials.
2. ☐	Replace failed equipment	HW vendor to replace the failed equipment.
3. ☐	**Recover PMAC and PMAC TVOE Host**: Configure BIOS settings and update firmware	1. Configure and verify the BIOS settings by executing procedure **Configure the RMS and Blade Server BIOS Settings** from reference [10]. 2. Verify and/or upgrade server firmware by executing procedure **Upgrade Management Server Firmware** from reference [10]. ***Note***: As indicated in [10], repeat for additional rack mount servers if equipped.

Procedure 1. Recovery Scenario 1

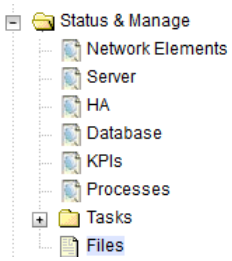
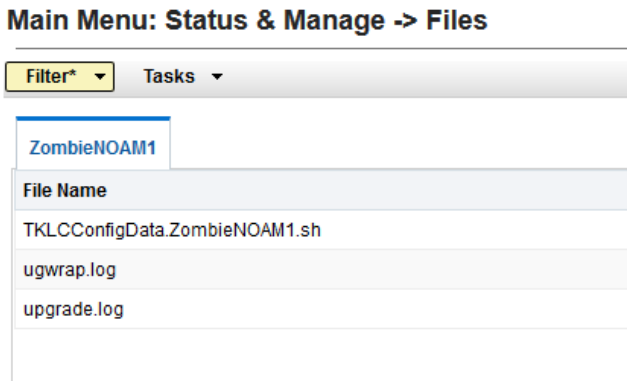
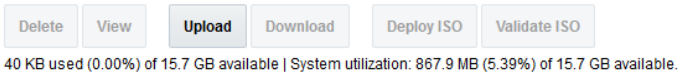
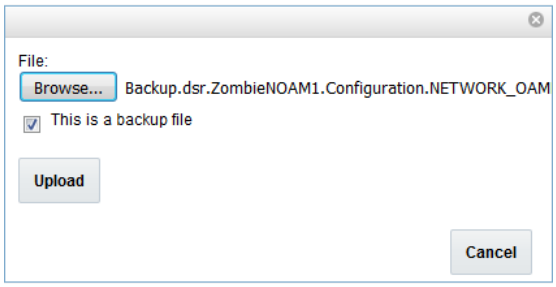
4. ☐	**PMAC, TVOE Hosts, and Switch Recovery**: Backups available	This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, **skip this step**. 1. Restore the PMAC TVOE host backup by executing Restore TVOE Configuration from Backup Media. 2. Restore the PMAC backup by executing Restore PMAC from Backup. 3. Recover failed OAs, aggregation, and enclosure switches by referring to Recover/Replace Failed 3rd Party Components (Switches, OAs). 4. Verify/Update blade server firmware by executing **Server Blades Installation Preparation** from reference [10]. 5. Install TVOE on ALL failed TVOE servers as needed by executing **Install TVOE on Blade Servers** from reference [10]. 6. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on **ALL** failed TVOE host blade servers. 7. **Proceed to Step 7**.
5. ☐	**PMAC, TVOE Hosts, and Switch Recovery**: Backups NOT available	This step assumes TVOE and PMAC backups are **NOT** available. If the TVOE and PMAC have already been restored, **skip this step**. 1. Execute section **Configure and IPM Management Server** from reference [10]. 2. Execute **Install PMAC** from reference [10]. 3. Execute **Configure Aggregation Switches** from reference [10] to recover Cisco 4948 aggregation switches, if needed. 4. Execute **Configure PMAC Application** from reference [10]. 5. Execute **HP C-7000 Enclosure Configuration** from reference [10] to recover and configure any failed OAs, if needed. 6. Execute **Enclosure and Blades Setup** from reference [10]. 7. Execute **Configure Enclosure Switches** from reference [10] to recover enclosure switches, if needed. 8. Verify/Update Blade server firmware by executing **Server Blades Installation Preparation** from reference [10]. 9. Install and configure TVOE on failed rack mount servers by executing **Installing TVOE on Rack Mount Server(s)** from reference [10]. 10. Install and configure TVOE on failed TVOE blade servers by executing **Install TVOE on Blade Servers** from reference [10].

Procedure 1. Recovery Scenario 1

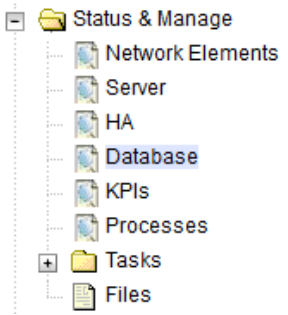
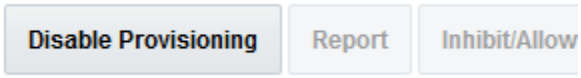
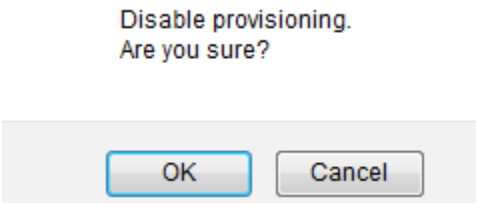
6. ☐	Execute Fast Deployment File for NOAMs	The backup fdconfig file used during the initial DSR installation is available on the PMAC, if a database backup was restored on the PMAC.
		If a backup fast deployment xml is NOT available, execute **Configure NOAM Servers** from reference [8].
		If a backup fast deployment xml is already present on the PMAC, execute this procedure:
		1. Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade has been performed since initial installation).
		2. Execute these commands:
		`$ cd /usr/TKLC/smac/etc`
		`$ screen`
		`$ sudo fdconfig config --file=<Created_FD_File>.xml`

7. ☐	Execute DSR installation procedure for the first NOAM	1. Configure the first NOAM server by executing **Configure the First NOAM NE and Server** section from reference [8]. 2. Configure the NOAM server group by executing the **Configure the NOAM Server Group** section from reference [8]. ***Note***: Use the backup copy of network configuration data and site surveys (Step 2).
8. ☐	**NOAM GUI**: Login	Log into the NOAM GUI as the **guiadmin** user: 

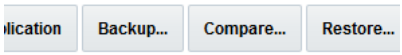
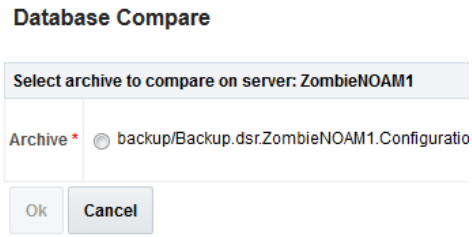
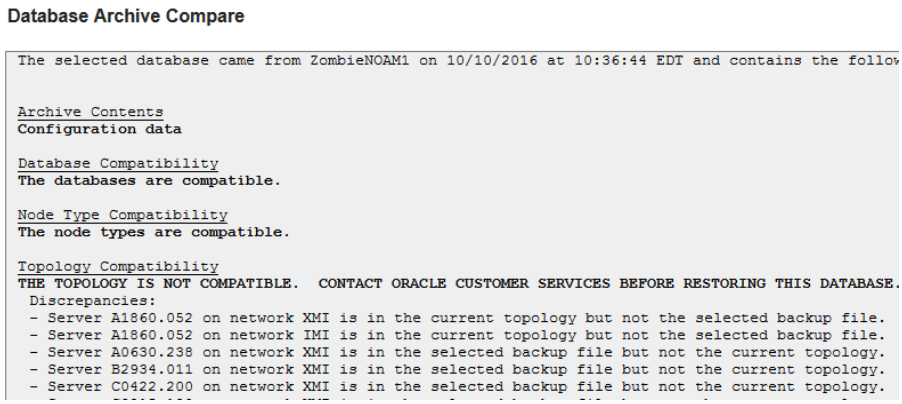
Procedure 1. Recovery Scenario 1

9. ☐	**NOAM GUI**: Upload the backed up database file	1. Navigate to **Status and Manage > Files**.  2. Select the active NOAM server.  3. Click **Upload** and select the **NO Provisioning and Configuration** file backed up after initial installation and provisioning.  4. Click **Browse** and locate the backup file. 5. 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.

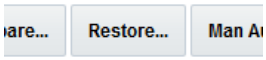
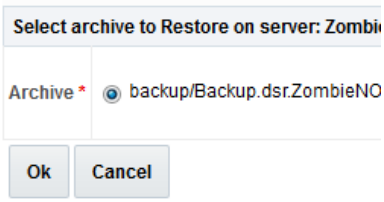
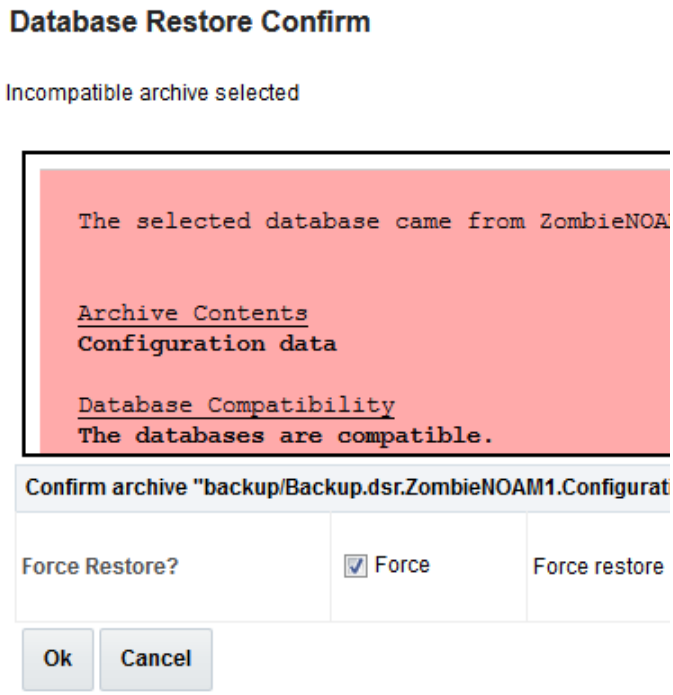
Procedure 1. Recovery Scenario 1

10. ☐	**NOAM GUI**: Disable provisioning	1. Navigate to **Status and Manage > Database**.  2. Click **Disable Provisioning**.  3. A confirmation window displays. Click **OK** to disable Provisioning. 

Procedure 1. Recovery Scenario 1

11. ☐	**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 9. 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** and continue to **next step** in this procedure.

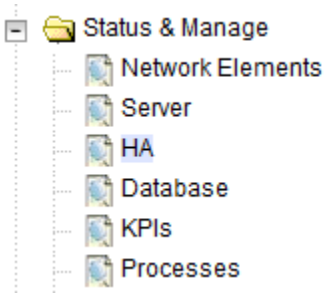
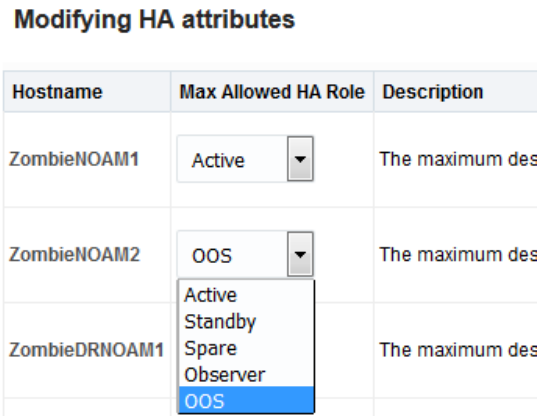
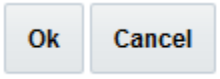
Procedure 1. Recovery Scenario 1

12. ☐	**Active NOAM**: Restore the database	1. From **Status and Manage > Database**. 2. Select the **Active NOAM** server and click **Restore**.  3. Select the proper backup provisioning and configuration file.  4. Click **OK**. The following confirmation screen displays. 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.

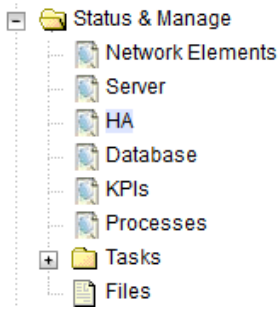
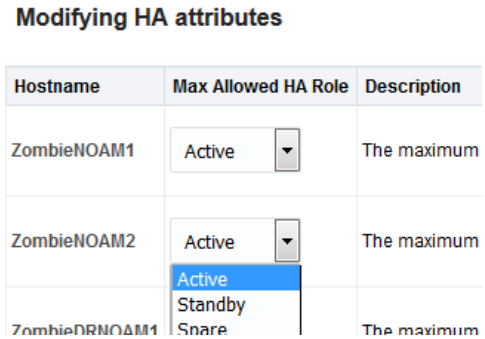
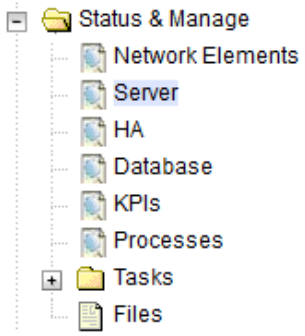
Procedure 1. Recovery Scenario 1

13. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 
14. ☐	**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.

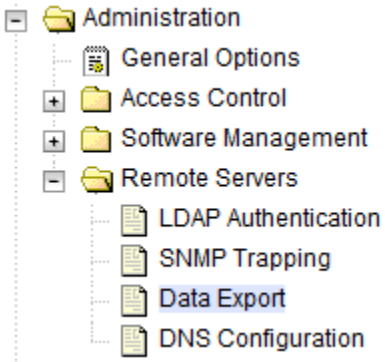
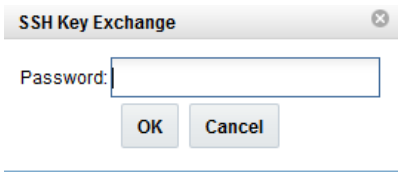
Procedure 1. Recovery Scenario 1

15. ☐	**Active NOAM**: Set failed servers to standby	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Set the Max Allowed HA Role drop down box to **OOS** for the failed servers.  4. Click **OK**. 
16. ☐	**Active NOAM**: Login	Log into the recovered active NOAM using SSH terminal as **admusr** user.
17. ☐	**NOAM VIP GUI**: Recover standby NOAM	1. Install the second NOAM server by executing procedure **Configure the Second NOAM Server**, steps 3-5 and 7, from reference [8]. ***Note***: Execute step 6 if NetBackup is used. 2. If NetBackup is used, then execute **Install NetBackup Client** from reference [8].

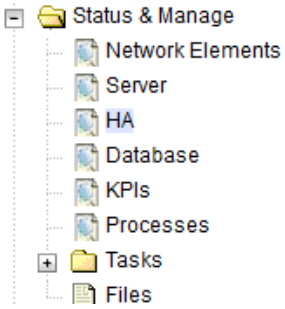
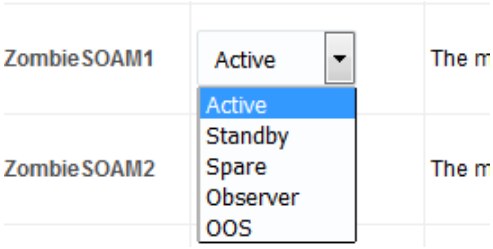
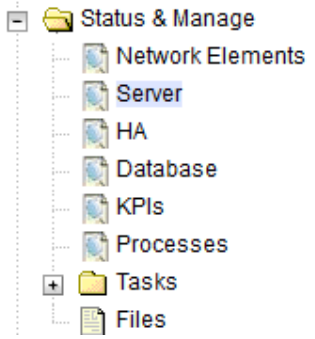
Procedure 1. Recovery Scenario 1

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

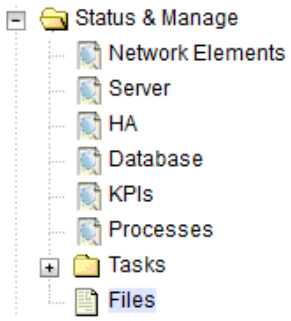
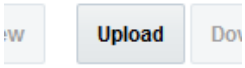
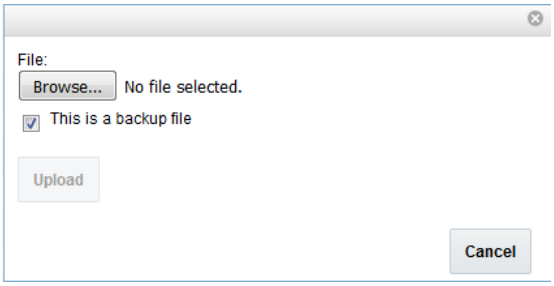
Procedure 1. Recovery Scenario 1

20. ☐	**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**. 
21. ☐	**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 E 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.
22. ☐	Configure SOAM TVOE server blades	If the TVOE restore has already been executed (step 5), skip this step. If a TVOE backup of the SOAM server blades is not available, execute **Configure SOAM TVOE Server Blades** from reference [8].
23. ☐	Create and IPM SOAM VMs	1. Execute **Create SOAM Guest VMs** for the failed SOAM VMs and MP blades from reference [8]. 2. Execute **IPM Blades and VMs** for the failed SOAM VMs and MP blades from reference [8]. 3. Execute **Install the Application** for the failed SOAM VMs and MP blades from reference [8].

Procedure 1. Recovery Scenario 1

24. ☐	Recover active SOAM server	1. Execute **Configure the SOAM Servers**, steps 1-3 and 5-8, from reference [8]. ***Note***: If you are using NetBackup, also execute step 10. 2. If you are using NetBackup, execute **Install NetBackup Client** from reference [8].
25. ☐	**NOAM VIP GUI**: Set HA on SOAM server	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Select the SOAM server and set it to **Active**.  4. Click **OK**.
26. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered SOAM server and click **Restart**. 

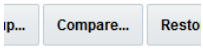
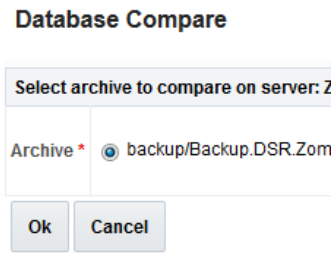
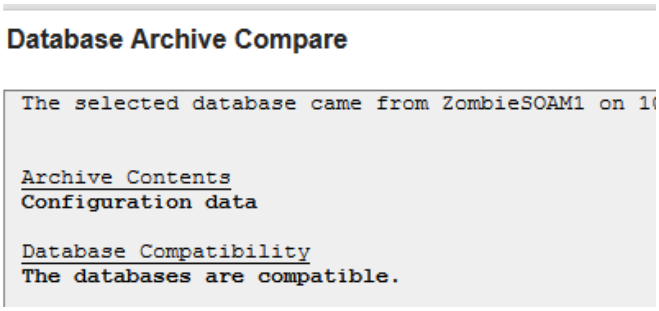
Procedure 1. Recovery Scenario 1

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

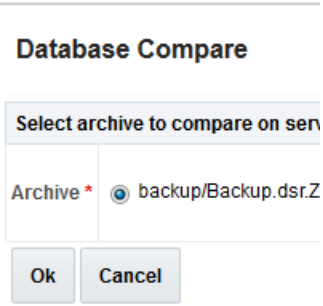
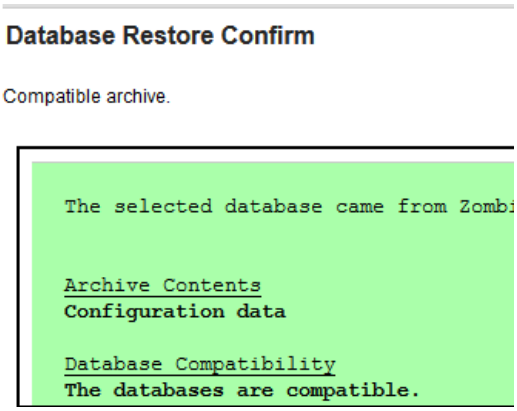
Procedure 1. Recovery Scenario 1

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

Procedure 1. Recovery Scenario 1

29. ☐	**Recovered SOAM GUI:** Verify the archive contents and database compatibility	1. Navigate to **Status and Manage > Database**. 2. Select the **Active SOAM** server and click **Compare**.  3. Click the button for the restored database file uploaded as a part of Step 27. 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** and continue to **next step** in this procedure.

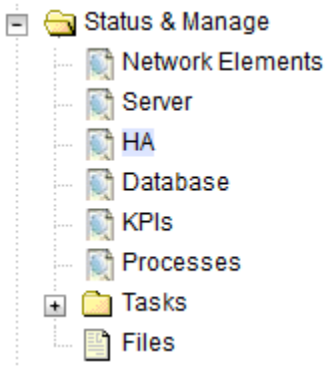
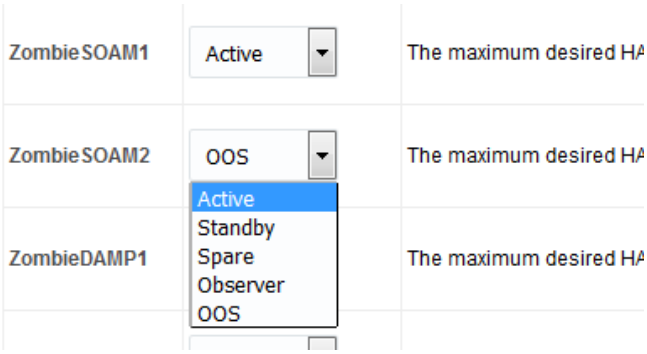
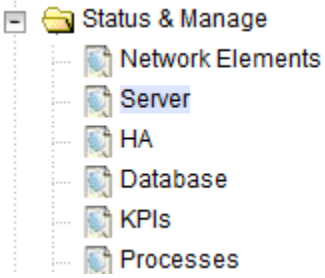
Procedure 1. Recovery Scenario 1

30. ☐	**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 get 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. The provisioning is disabled after this step.
31. ☐	**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.

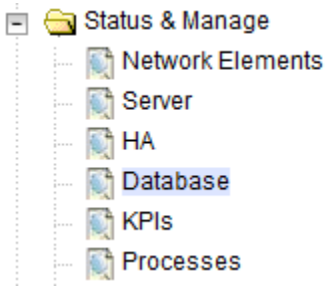
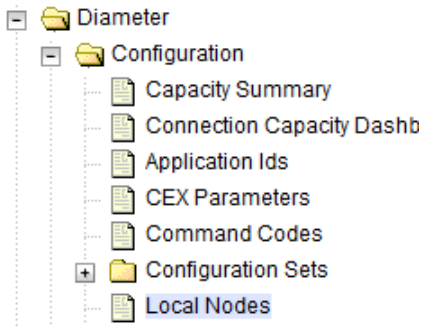
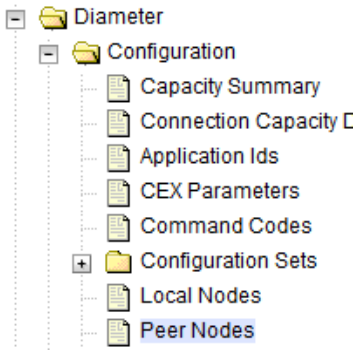
Procedure 1. Recovery Scenario 1

32. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 
33. ☐	**NOAM VIP GUI**: Recover the remaining SOAM servers	Recover the **remaining** SOAM servers (**standby, spare**) by repeating these steps for each SOAM server: 1. Execute **Configure the SOAM Servers**, steps 1-3 and 5-8, from reference [8]. ***Note***: If you are using NetBackup, also execute step 10. 2. If you are using NetBackup, execute **Install NetBackup Client** from reference [8].

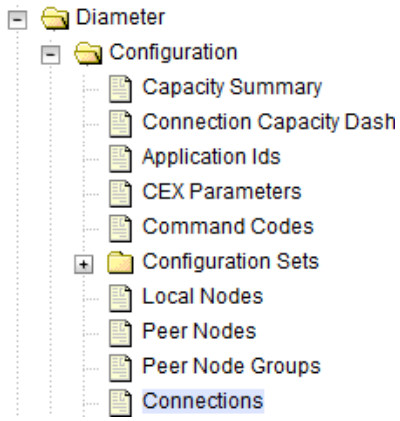
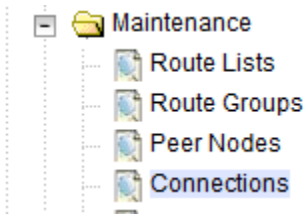
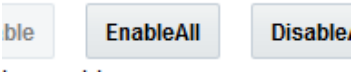
Procedure 1. Recovery Scenario 1

34. ☐	**NOAM VIP GUI**: Set HA on remaining SOAMs	1. Navigate to **Status and 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**.
35. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered standby SOAM server and click **Restart**. 

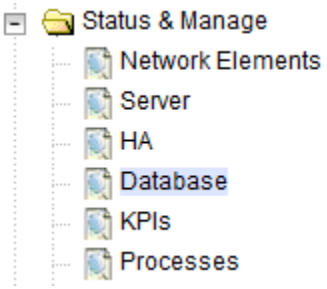
Procedure 1. Recovery Scenario 1

36. ☐	**NOAM VIP GUI**: Start replication on the recovered standby SOAM	Un-Inhibit (Start) Replication to the recovered **Standby SOAM**. 1. Navigate to **Status and Manage > Database**.  2. Click **Allow Replication** on the recovered standby SOAM server. 3. Verify the replication on all servers is allowed. This can be done by checking **Repl status** column of respective server
37. ☐	**SOAM VIP GUI**: Verify the local node info	1. Navigate to **Diameter > Configuration > Local Node**.  2. Verify all the local nodes are shown.
38. ☐	**SOAM VIP GUI**: Verify the peer node info	1. Navigate to **Diameter > Configuration > Peer Node**.  2. Verify all the peer nodes are shown.

Procedure 1. Recovery Scenario 1

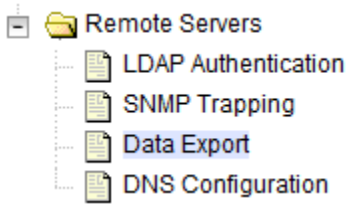
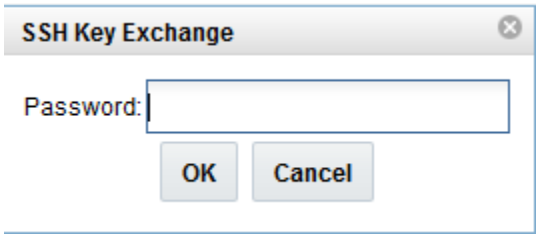
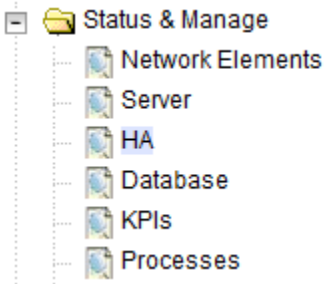
39. ☐	**SOAM VIP GUI**: Verify the connections info	1. Navigate to **Diameter > Configuration > Connections**.  2. Verify all the connections are shown.
40. ☐	**SOAM VIP GUI**: Enable connections, if needed	1. Navigate to **Diameter > Maintenance > Connections**.  2. Select each connection and click **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
41. ☐	**Active NOAM**: Activate optional features	Establish an SSH session to the active NOAM, login as **admusr.** **Note for PCA Activation:** If you have PCA installed in the system being recovered, re-activate PCA by executing **PCA Activation on Entire Server on Recovered NOAM Server** from [13]. ***Note***: If not all SOAM sites are recovered at this point, then you should repeat activation for each *new* SOAM site that comes online. ***Note***: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature. Refer to 1.5 Optional Features to activate any features previously activated.

Procedure 1. Recovery Scenario 1

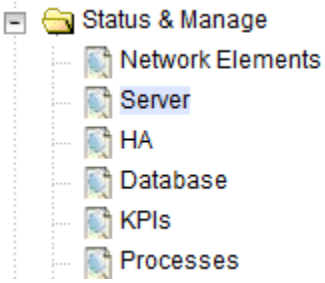
42. ☐	**NOAM VIP GUI**: Start replication on working C-level servers	Un-Inhibit (Start) Replication to the **working** C-level Servers which belongs to the same site as of the failed SOAM servers. **If the spare SOAM is also present in the site and lost**, execute Appendix F Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost). **If the spare SOAM is NOT deployed in the site**, execute Appendix D Un-Inhibit A and B Level Replication on C-level Servers. 1. Navigate to **Status and Manage > Database**.  2. If the **Repl Status** is set to **Inhibited**, click **Allow Replication** using this order; otherwise, if none of the servers are inhibited, skip this step and continue with the next step: • Active NOAM Server • Standby NOAM Server • Active SOAM Server • Standby SOAM Server • Spare SOAM Server **(if applicable)** • Active DR NOAM Server • Standby DR NOAM Server • MP/IPFE servers (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

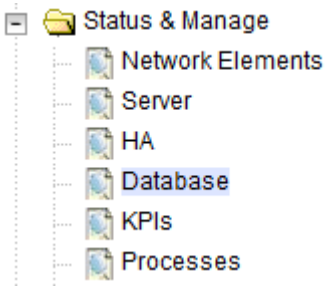
Procedure 1. Recovery Scenario 1

43. ☐	**SOAM VIP GUI**: Perform key exchange with export server	1. Navigate to **Administration > Remote Servers > Data Export**.  2. Click **SSH Key Exchange**. 3. Type the **Password** and click **OK**. 
44. ☐	**NOAM VIP GUI**: Recover the C-level server (DA-MP, SBRs, IPFE)	1. Execute **Configure MP Blade Servers**, steps 1, 7, 11-14, and 17, from reference [8]. ***Note***: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. 2. Repeat this step for any remaining failed MP servers.
45. ☐	**NOAM VIP GUI**: Set HA on all C-level servers	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. For each recovered C-level whose Max Allowed HA Role is set to **Standby**, set it to **Active**.  4. Click **OK**.

Procedure 1. Recovery Scenario 1

46. ☐	**NOAM VIP GUI**: Restart DSR application on recovered C-level servers	1. Navigate to **Status and Manage > Server**.  2. Select the recovered C-level servers and click **Restart**. 

Procedure 1. Recovery Scenario 1

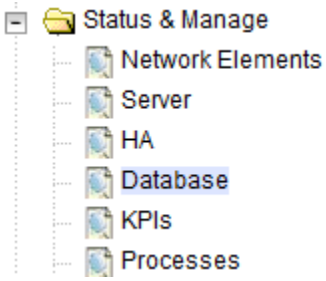
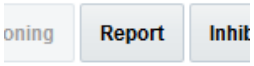
<table>
<tr>
<td>47. ☐</td>
<td>NOAM VIP GUI: Start replication on all C-level servers</td>
<td>Un-inhibit (start) replication to the ALL C-level servers.
1. Navigate to Status and Manage > Database.
 

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)
• Active DR NOAM Server
• Standby DR NOAM Server
• MP/IPFE servers (if MPs are configured as active/standby, start with the Active MP; otherwise, the order of the MPs does not matter)
• SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare)
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>
<tr>
<td>48. ☐</td>
<td>Active NOAM: Perform key exchange between the active-NOAM and recovered servers</td>
<td>1. Establish an SSH session to the active NOAM, 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.</td>
</tr>
</table>

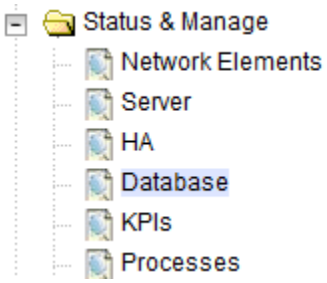
Procedure 1. Recovery Scenario 1

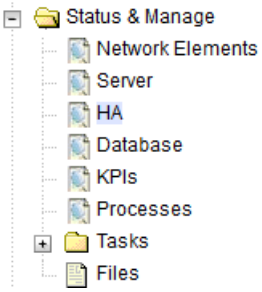
49. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status and Manage > Database**.
		 
		2. Select the active NOAM server and click **Report**.
		 
		The following screen displays:
		Main Menu: Status & Manage -> Database [Report]
		`==========`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

50. ☐	**Active NOAM**: Verify replication between servers	1. Log into the active NOAM using SSH terminal as **admusr**.
		2. Execute this command:
		`$ sudo irepstat –m`
		Output:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`Oahu-DAMP-1 – Act/Act`
		`  BC From Oahu-SOAM-2  Active   0   0.50 ^0.15%cpu 25B/s  A=me`
		`  CC To   Oahu-DAMP-2  Active   0   0.10  0.14%cpu 25B/s  A=me`
		`Oahu-DAMP-2 – Act/Stb`
		`  BC From Oahu-SOAM-2  Active   0   0.50 ^0.11%cpu 31B/s  A=C3642.212`
		`  CC From Oahu-DAMP-1  Active   0   0.10 ^0.14 1.16%cpu 31B/s A=C3642.212`
		`Oahu-IPFE-1 -- Active`
		`  BC From Oahu-SOAM-2  Active   0   0.50 ^0.03%cpu 24B/s  A=C3642.212`
		`Oahu-IPFE-2 -- Active`
		`  BC From Oahu-SOAM-2  Active   0   0.50 ^0.03%cpu 28B/s  A=C3642.212`
		`Oahu-NOAM-1 -- Stby`
		`  AA From Oahu-NOAM-2  Active   0   0.25 ^0.03%cpu 23B/s`
		`Oahu-NOAM-2 -- Active`
		`  AA To   Oahu-NOAM-1  Active   0   0.25 1%R 0.04%cpu 61B/s`
		`  AB To   Oahu-SOAM-2  Active   0   0.50 1%R 0.05%cpu 75B/s`
		`Oahu-SOAM-1 -- Stby`
		`  BB From Oahu-SOAM-2  Active   0   0.50 ^0.03%cpu 27B/s`
		`Oahu-SOAM-2 -- Active`
		`  AB From Oahu-NOAM-2  Active   0   0.50 ^0.03%cpu 24B/s`
		`  BB To   Oahu-SOAM-1  Active   0   0.50 1%R 0.04%cpu 32B/s`
		`  BC To   Oahu-IPFE-1  Active   0   0.50 1%R 0.04%cpu 21B/s`
		`irepstat ( 40 lines) (h)elp (m)erged`

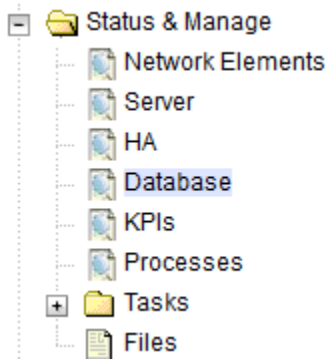
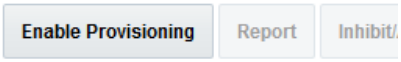
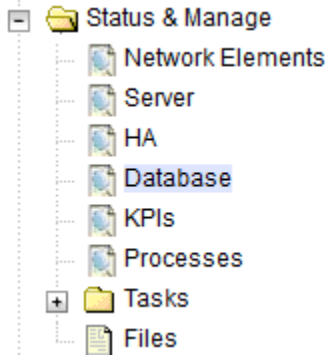
Procedure 1. Recovery Scenario 1

<table>
<tr>
<td>51. ☐</td>
<td>NOAM VIP GUI: Verify the database states</td>
<td>
1. Navigate to Status and Manage > Database.


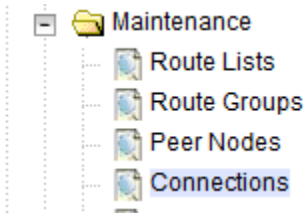
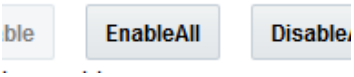
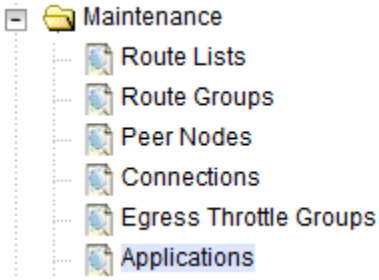
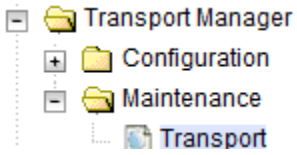
2. Verify the OAM Max HA Role is either Active or Standby for NOAM and SOAM; Application Max HA Role for MPs is Active; and the status is Normal:
<table>
<tr><th>Network Element</th><th>Server</th><th>Role</th><th>OAM Max HA Role</th></tr>
<tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM1</td><td>Network OAM&P</td><td>Active</td></tr>
<tr><td>ZombieNOAM</td><td>ZombieNOAM2</td><td>Network OAM&P</td><td>Standby</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSOAM2</td><td>System OAM</td><td>N/A</td></tr>
<tr><td>ZombieNOAM</td><td>ZombieNOAM1</td><td>Network OAM&P</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSOAM1</td><td>System OAM</td><td>Active</td></tr>
<tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM2</td><td>Network OAM&P</td><td>Standby</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieDAMP2</td><td>MP</td><td>Standby</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSS7MP2</td><td>MP</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSS7MP1</td><td>MP</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieIPFE1</td><td>MP</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieIPFE2</td><td>MP</td><td>Active</td></tr>
</table>
</td>
</tr>
<tr>
<td>52. ☐</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>
</table>

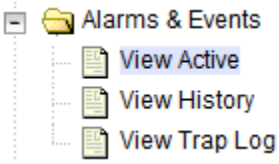
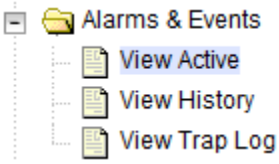
Procedure 1. Recovery Scenario 1

53. ☐	**NOAM GUI**: Enable provisioning	1. Navigate to **Status and Manage > Database**.  2. Click **Enable Provisioning**.  3. A confirmation window displays. Click **OK** to enable Provisioning.
54. ☐	**SOAM GUI**: Enable site provisioning	1. Navigate to **Status and Manage > Database**.  2. Click **Enable Site Provisioning**.  3. A confirmation window displays. Click **OK** to enable Provisioning.
55. ☐	**MP Servers**: Disable SCTP Auth Flag	For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [14]. Execute this procedure on all failed MP servers.

Procedure 1. Recovery Scenario 1

56. ☐	**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
57. ☐	**SOAM VIP GUI**: Enable optional features	1. Navigate to **Diameter > Maintenance > Applications**.  2. Select the optional feature application configured in step 41. 3. Click **Enable**. 
58. ☐	**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 1. Recovery Scenario 1

59. ☐	**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).
60. ☐	**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).
61. ☐	Restore GUI usernames and passwords	If applicable, execute Resolving User Credential Issues after Database Restore to recover the user and group information restored.
62. ☐	Backup and archive all the databases from the recovered system	Execute DSR Database Backup to back up the Configuration databases.
63. ☐	Recover IDIH	If IDIH were affected, refer to IDIH Disaster Recovery to perform disaster recovery on IDIH.
64. ☐	SNMP workaround	Refer to SNMP Configuration to configure SNMP as a workaround in these cases: 1. If SNMP is not configured in DSR. 2. If SNMP is already configured and **SNMPv3** is selected as enabled version.

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 of base hardware and software and then executing a database restore to the active SOAM server using a database backup file obtained from the SOAM servers. All other servers are recovered using recovery procedures of base hardware and software. Database replication from the active NOAM server recovers 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 procedure detailed steps are in Procedure 2. The major activities are summarized as follows:

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

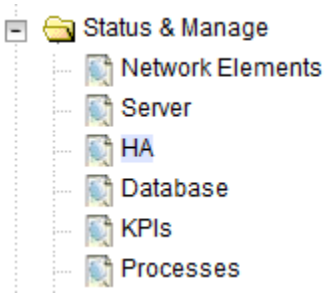
Procedure 2. Recovery Scenario 2

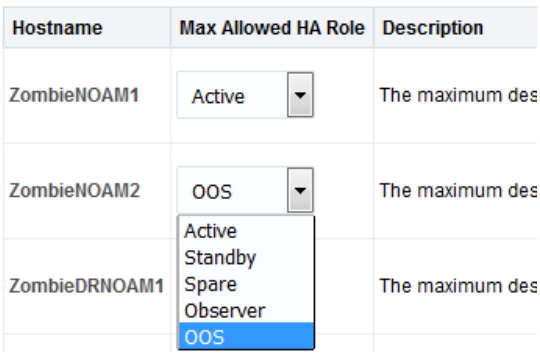
This procedure performs recovery if at least 1 NOAM server is available, but all SOAM servers in a site have failed. This includes any SOAM server that is in another location. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Workarounds	Refer to SNMP Configuration to configure SNMP as a workaround in these cases: 1. If SNMP is not configured in DSR. 2. If SNMP is already configured and **SNMPv3** is selected as enabled version.
2. ☐	Gather required materials	Gather the documents and required materials listed in Required Materials.

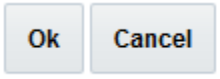
Procedure 2. Recovery Scenario 2

3. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP 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

<table>
<tr>
<td>4. ☐</td>
<td>Active NOAM: Set failed servers to OOS</td>
<td>
1. Navigate to Status and Manage > HA.


2. Click Edit.
Modifying HA attributes


3. Set the Max Allowed HA Role drop down box to OOS for the failed servers.
4. Click OK.


</td>
</tr>
<tr>
<td>5. ☐</td>
<td>Replace failed equipment</td>
<td>HW vendor to replace the failed equipment.</td>
</tr>
<tr>
<td>6. ☐</td>
<td>RMS NOAM Failure: Configure BIOS settings and update firmware</td>
<td>
If the failed server is NOT a rack mount server, skip to step 10.
1. Configure and verify the BIOS settings by executing procedure Configure the RMS and Blade Server BIOS Settings from reference [10].
2. Verify and/or upgrade server firmware by executing procedure Upgrade Management Server Firmware from reference [10].
Note: Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.
</td>
</tr>
</table>

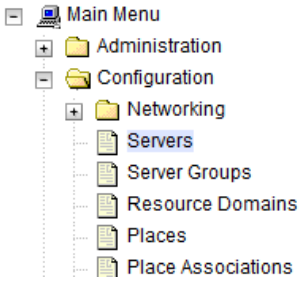
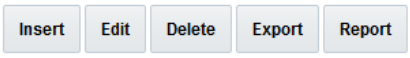
Procedure 2. Recovery Scenario 2

7. ☐	**RMS NOAM Failure**: Backups available	If the failed server is **NOT** a rack mount server, **skip to step 10.** This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, **skip this step**. 1. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media. 2. If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing Restore PMAC from Backup
8. ☐	**RMS NOAM Failure**: Backups NOT available	If the failed server is **NOT** a rack mount server, **skip to step 10.** This step assumes that TVOE and PMAC backups **NOT** are available, if the TVOE and PMAC have already been restored, **skip this step.** If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. **Configure and IPM Management Server** from reference [10]. 2. **Install PMAC** from reference [10]. 3. **Configure PMAC Application** from reference [10]. If the PMAC is **NOT** located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. **Installing TVOE on Rack Mount Server(s)** from reference [10].
9. ☐	Recover failed aggregation/ enclosure switches, and OAs	Recover failed OAs, aggregation and enclosure switches, if needed. Backups Available: 1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) section to recover failed OAs, aggregation, and enclosure switches Backups **NOT** Available: 1. Execute **HP C-7000 Enclosure Configuration** from reference [10] to recover and configure any failed OAs, if needed. 2. Execute **Configure Enclosure Switches** from reference [10] to recover enclosure switches, if needed.
10. ☐	**HP-Class Blade Failure**: Configure blade server iLO, update firmware/BIOS settings	If the failed server is **NOT** an HP C-Class Blade, **skip to step 14.** 1. Execute **Configure Blade Server iLO Password for Administrator Account** from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing **Server Blades Installation Preparation** from reference [10]
11. ☐	**HP-Class Blade Failure**: Backups available	If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 14.** This step assumes TVOE backups are available. If backups are **NOT** available, **skip this step**. 1. Install and configure TVOE on failed TVOE blade servers by executing **Install TVOE on Blade Servers** from reference [10]. 2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on **ALL** failed TVOE Host blade servers.

Procedure 2. Recovery Scenario 2

12. ☐	HP-Class Blade Failure: Backups NOT available	If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 14.** This step assumes TVOE backups are **NOT** available: 1. Install and configure TVOE on failed TVOE blade servers by executing **Install TVOE on Blade Servers** from reference [10]. 2. Configure the NOAM and/or SOAM failed TVOE server blades by executing **Configure SOAM TVOE Server Blades** from reference [8]. ***Note***: Although the title of the procedure is related to SOAMs only, execute this procedure for any failed NOAMs located on TVOE server blades.
13. ☐	Create VMs	Execute Create NOAM/SOAM Virtual Machines to create the NOAM and SOAM VMs on failed TVOE servers.
14. ☐	IPM and install DSR application on failed guest/servers	1. Execute **IPM Blades and VMs** for the failed SOAM VMs and MP blades from reference [8]. 2. Execute **Install the Application Software** for the failed SOAM VMs and MP blades from reference [8].
15. ☐	Install NetBackup client (Optional)	If NetBackup is used, execute **Install NetBackup Client** from reference [8].
16. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 

Procedure 2. Recovery Scenario 2

17. ☐	**NOAM VIP GUI**: Export the initial configuration	If the failed server is NOT a NOAM server, skip to **step 24.** 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. 
18. ☐	**NOAM VIP GUI**: Copy configuration file to failed NOAM server	1. Obtain a terminal session to the 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_control_IP_address>:/var/tmp/TKLCConfigData.sh`

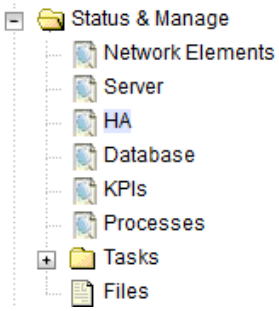
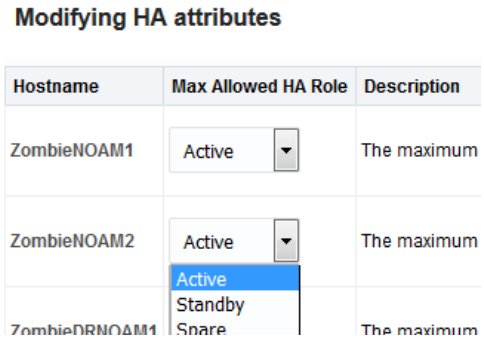
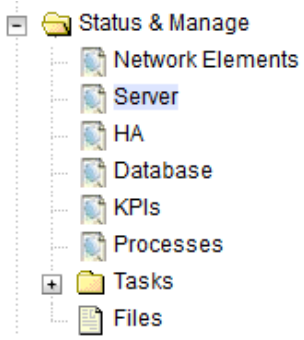
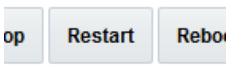
19. ☐	**Failed NOAM Server**: Verify the configuration was called and reboot the server	1. Establish an SSH session to the failed NOAM server, login as the **admusr** user.
		The automatic configuration daemon looks for the file named **TKLCConfigData.sh** in the **/var/tmp** directory, implements the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

Procedure 2. Recovery Scenario 2

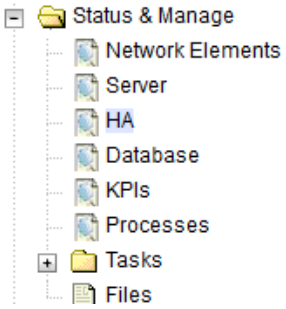
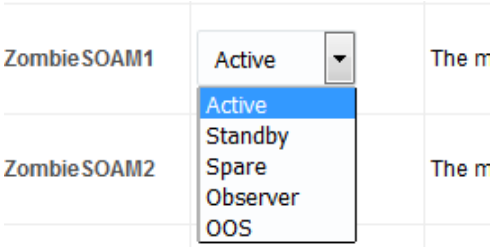
20. ☐	**Failed NOAM Server**: Configure networking for dedicated NetBackup interface (Optional)	***Note***: Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.
		Obtain a terminal window to the failed NOAM server, logging in as the **admusr.**
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP_Adress> --netmask=<NO2_NetBackup_NetMask>`
		`$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NO1_NetBackup_Network_ID> --netmask=<NO2_NetBackup_NetMask> --gateway=<NO2_NetBackup_Gateway_IP_Address>`

21. ☐	**Failed NOAM Server**: Verify server health	Execute this command on the 2nd 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`

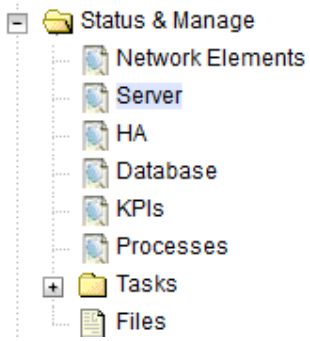
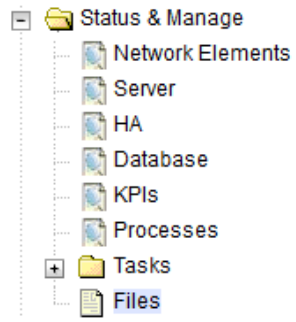
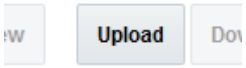
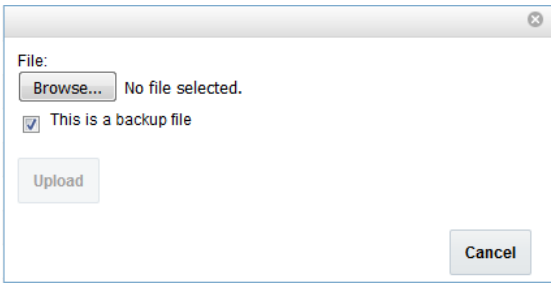
Procedure 2. Recovery Scenario 2

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

Procedure 2. Recovery Scenario 2

24. ☐	**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 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 Inhibit A and B Level Replication on C-level Servers to inhibit replication to working C-level servers before continuing.
25. ☐	Recover active SOAM server	1. Execute **Configure the SOAM Servers**, steps 1-3 and 5-8, from reference [8]. ***Note***: If you are using NetBackup, also execute step 10. 2. If you are using NetBackup, execute **Install NetBackup Client** from reference [8].
26. ☐	**NOAM VIP GUI**: Set HA on SOAM server	1. Navigate to **Status and Manage > HA**.  2. Click **Edit** at the bottom of the screen. 3. Select the SOAM server and set it to **Active**.  4. Click **OK**.

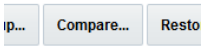
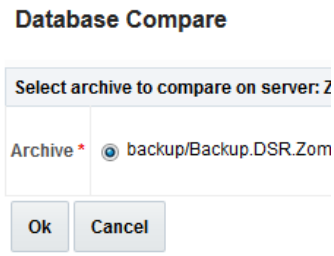
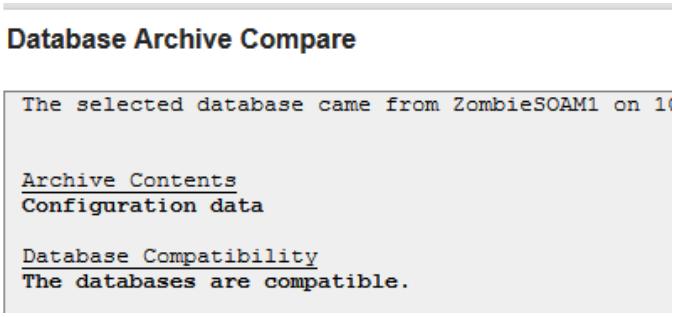
Procedure 2. Recovery Scenario 2

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

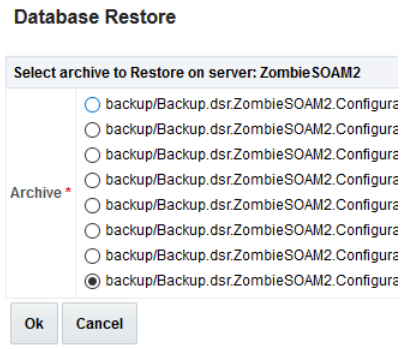
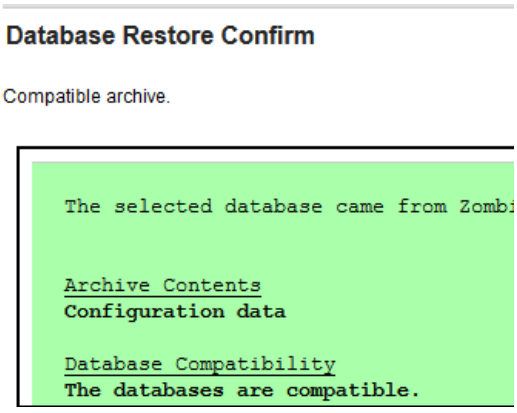
Procedure 2. Recovery Scenario 2

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

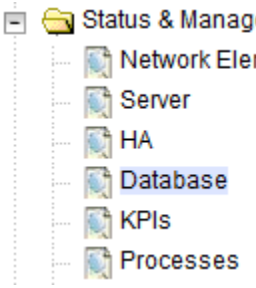
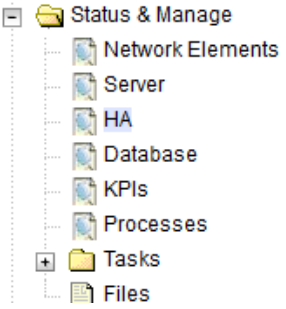
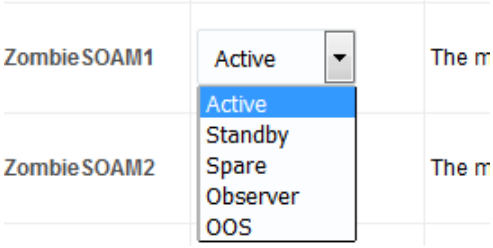
Procedure 2. Recovery Scenario 2

30. ☐	**Recovered SOAM GUI:** Verify the archive contents and database compatibility	1. Navigate to **Status and Manage > Database**. 2. Select the **Active SOAM** server and click **Compare**.  3. Click the button for the restored database file uploaded as a part of step 28 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**, then cancel and continue to **next step** in this procedure.

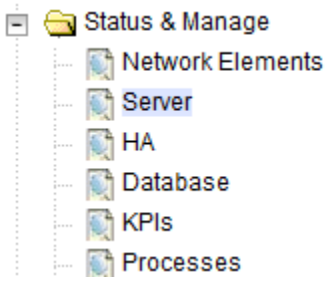
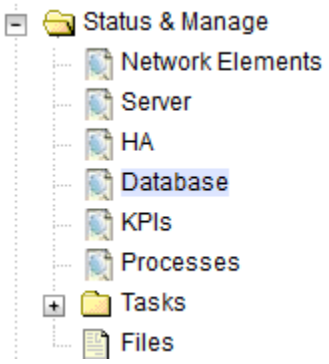
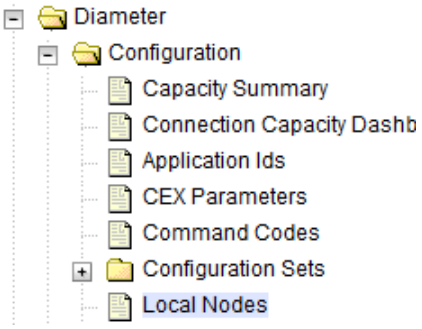
Procedure 2. Recovery Scenario 2

31. ☐	**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 get 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. The provisioning is disabled after this step.
32. ☐	**Recovered SOAM GUI**: Monitor and Confirm database restoral	Wait for **5-10 minutes** for the system to stabilize with the new topology: Monitor the Info tab for **Success**. This 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.

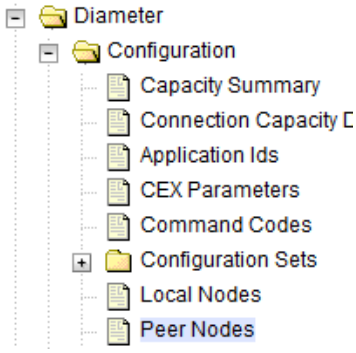
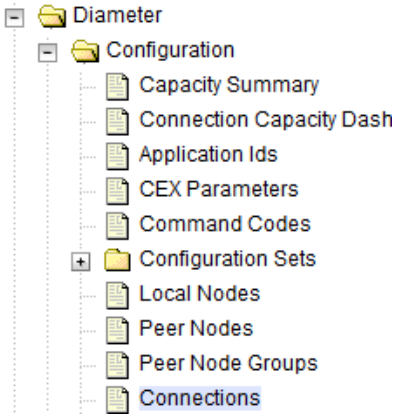
Procedure 2. Recovery Scenario 2

33. ☐	**NOAM VIP GUI**: Recover the remaining SOAM servers	Recover the **remaining** SOAM servers (**standby, spare**) by repeating these steps for each SOAM server: 1. Execute **Configure the SOAM Servers**, steps 1-3 and 5-8, from reference [8]. ***Note***: If you are using NetBackup, also execute step 10. 2. If you are using NetBackup, execute **Install NetBackup Client** from reference [8].
34. ☐	**NOAM VIP GUI**: Start replication on the recovered SOAMs	Un-Inhibit (Start) Replication to the recovered SOAM servers 1. Navigate to **Status and Manage > Database**.  2. Click **Allow Replication** on the recovered SOAM servers. 3. Verify the replication on all SOAMs servers is allowed. This can be done by checking **Repl status** column of respective server
35. ☐	**NOAM VIP GUI**: Set HA on recovered standby SOAM server	1. Navigate to **Status and Manage > HA**.  2. Click **Edit** at the bottom of the screen 3. Select the recovered standby SOAM server and set it to **Active**.  4. Click **OK**.

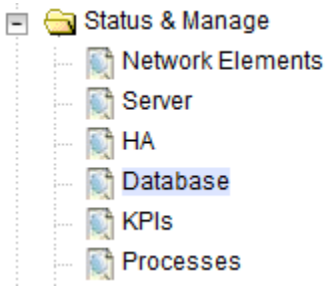
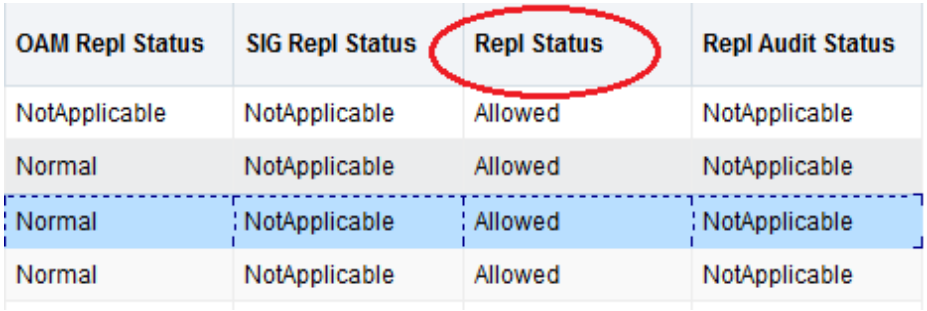
Procedure 2. Recovery Scenario 2

36. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered standby SOAM server and click **Restart**. 
37. ☐	**SOAM GUI**: Enable provisioning	1. Navigate to **Status and Manage > Database**.  2. Click **Enable Site Provisioning**.  3. A confirmation window displays. Click **OK** to enable provisioning.
38. ☐	**SOAM VIP GUI**: Verify the local node info	1. Navigate to **Diameter > Configuration > Local Node**.  2. Verify all the local nodes are shown.

Procedure 2. Recovery Scenario 2

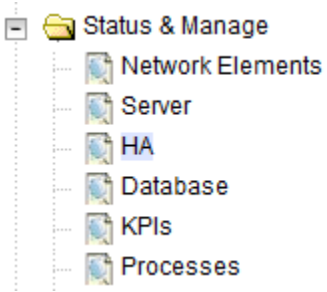
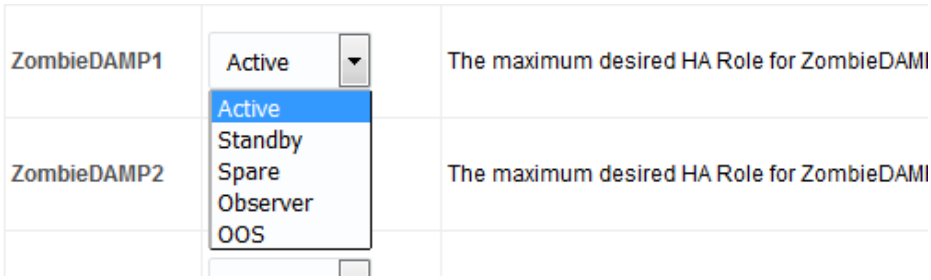
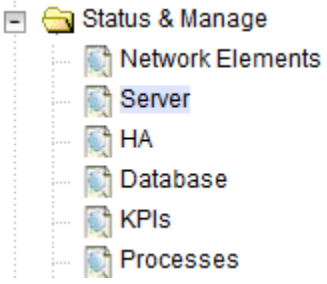
39. ☐	**SOAM VIP GUI**: Verify the peer node info	1. Navigate to **Diameter > Configuration > Peer Node**.  2. Verify all the peer nodes are shown.
40. ☐	**SOAM VIP GUI**: Verify the connections info	1. Navigate to **Diameter > Configuration > Connections**.  2. Verify all the connections are shown.

Procedure 2. Recovery Scenario 2

41. ☐	**NOAM VIP GUI**: Start replication on working C-level servers **Note**: Wait until audit becomes active on SOAM or NOAM. Click **Allow Replication** for each DP server until all DP servers associated with this SOAM Network Element have been inhibited.	Un-Inhibit (Start) Replication to the **working** C-level servers which belong to the same site as of the failed SOAM servers. **If the spare SOAM is also present in the site and lost**, execute Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost). **If the spare SOAM is NOT deployed in the site**, execute Un-Inhibit A and B Level Replication on C-level Servers. 1. Navigate to **Status and Manage > Database**.  2. If the **Repl Status** is set to **Inhibited**, click **Allow Replication** using this order; otherwise, if none of the servers are inhibited, skip this step and continue with the n**e**xt step: • Active NOAM Server • Standby NOAM Server • Active SOAM Server • Standby SOAM Server • Spare SOAM Server **(if applicable)** • Active DR NOAM Server • Standby DR NOAM Server • MP/IPFE servers (if MPs are configured as active/standby, start with the Active MP; otherwise, the order of the MPs does not matter) • SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare) 3. Verify the replication on all the working servers is allowed. This can be done by checking the **Repl Status** as shown here. 

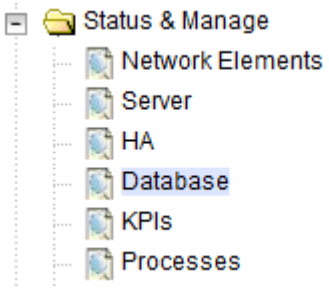
OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
NotApplicable	NotApplicable	Allowed	NotApplicable
Normal	NotApplicable	Allowed	NotApplicable
Normal	NotApplicable	Allowed	NotApplicable
Normal	NotApplicable	Allowed	NotApplicable

Procedure 2. Recovery Scenario 2

42. ☐	**NOAM VIP GUI**: Recover the C-level server (DA-MP, SBRs, IPFE)	Execute **Configure MP Blade Servers**, steps 1, 7, 11-14, and 17, from reference [8]. ***Note***: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. Repeat this step for any remaining failed MP servers.
43. ☐	**NOAM VIP GUI**: Restart DSR application on recovered C-level servers	1. Navigate to **Status and Manage > HA**.  2. Click **Edit** at the bottom of the screen. 3. For each recovered C-level with a Max Allowed HA Role set to **Standby**, set it to **Active**.  4. Click **OK**.
44. ☐	**NOAM VIP GUI**: Restart DSR application on recovered C-level servers	1. Navigate to **Status and Manage > Server**.  2. Select the recovered C-level servers and click **Restart**. 

Procedure 2. Recovery Scenario 2

<table>
<tr>
<td>45. ☐</td>
<td>NOAM VIP GUI: Start replication on ALL C-level servers

Note: Wait until audit becomes active on SOAM or NOAM.
Click Allow Replication for each DP server until all DP servers associated with this SOAM Network Element have been inhibited.</td>
<td>Un-Inhibit (Start) Replication to the ALL C-level servers.
1. Navigate to Status and Manage > Database.
 

2. If the Repl Status is set to Inhibited, click Allow Replication using this order:
• Active NOAMP Server
• Standby NOAMP Server
• Active SOAM Server
• Standby SOAM Server
• Spare SOAM Server (if applicable)
• Active DR NOAM Server
• Standby DR NOAM Server
• MP/IPFE Servers (if MPs are configured as active/standby, start with the Active MP; otherwise, the order of the MPs does not matter).
3. Verify the replication on all servers is allowed. This can be done by checking the Repl Status 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>
<tr>
<td>46. ☐</td>
<td>Active NOAM: Perform keyexchange between the active-NOAM and recovered servers</td>
<td>1. Establish an SSH session to the active NOAM, login as admusr.
2. Execute this command to perform a keyexchange from the active NOAM to each recovered server:

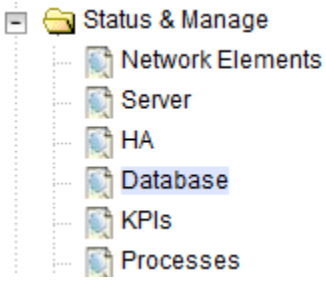
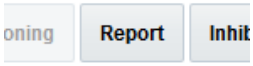
```
$ keyexchange admusr@<Recovered Server Hostname>
```

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

Procedure 2. Recovery Scenario 2

47. ☐	**Active NOAM**: Activate optional features	Establish an SSH session to the active NOAM, login as **admusr**. **Note for PCA Feature Activation:** If you have PCA installed in the system being recovered, re-activate the PCA by executing **PCA Activation on Standby NOAM server** on the recovered standby NOAM server, and **PCA Activation on Active SOAM server** on the recovered active SOAM server from [13]. Refer to Optional Features to activate any features that were previously activated. ***Note***: While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: `iload#31000{S/W Fault}` ***Note***: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.

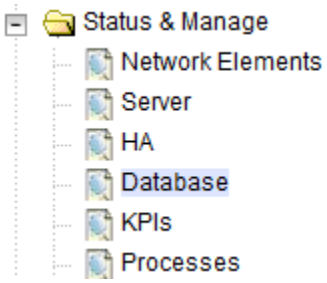
Procedure 2. Recovery Scenario 2

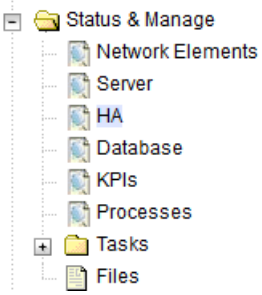
48. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status and Manage > Database**.
		 
		2. Select the active NOAM server and click **Report**.
		 
		The following screen displays:
		Main Menu: Status & Manage -> Database [Report]
		`dsr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

49. ☐	**Active NOAM**: Verify replication between servers	1. Log into the active NOAM using SSH terminal as **admusr**.
		2. Execute this command:
		`$ sudo irepstat –m`
		Output:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`Oahu-DAMP-1 - Act/Act`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.15%cpu 25B/s  A=me`
		`  CC To  Oahu-DAMP-2  Active  0  0.10  0.14%cpu 25B/s  A=me`
		`Oahu-DAMP-2 - Act/Stb`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.11%cpu 31B/s  A=C3642.212`
		`  CC From Oahu-DAMP-1  Active  0  0.10 ^0.14 1.16%cpu 31B/s A=C3642.212`
		`Oahu-IPFE-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 24B/s  A=C3642.212`
		`Oahu-IPFE-2 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 28B/s  A=C3642.212`
		`Oahu-NOAM-1 -- Stby`
		`  AA From Oahu-NOAM-2  Active  0  0.25 ^0.03%cpu 23B/s`
		`Oahu-NOAM-2 -- Active`
		`  AA To  Oahu-NOAM-1  Active  0  0.25 1%R 0.04%cpu 61B/s`
		`  AB To  Oahu-SOAM-2  Active  0  0.50 1%R 0.05%cpu 75B/s`
		`Oahu-SOAM-1 -- Stby`
		`  BB From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 27B/s`
		`Oahu-SOAM-2 -- Active`
		`  AB From Oahu-NOAM-2  Active  0  0.50 ^0.03%cpu 24B/s`
		`  BB To  Oahu-SOAM-1  Active  0  0.50 1%R 0.04%cpu 32B/s`
		`  BC To  Oahu-IPFE-1  Active  0  0.50 1%R 0.04%cpu 21B/s`
		`irepstat ( 40 lines) (h)elp (m)erged`

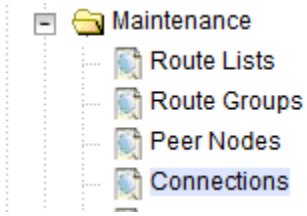
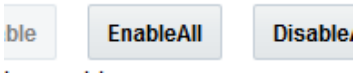
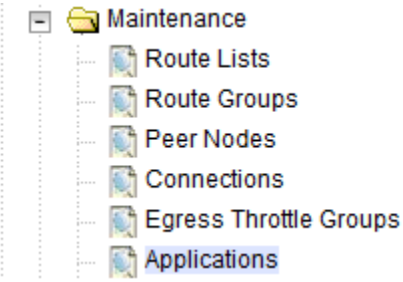
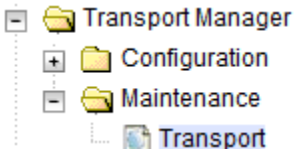
Procedure 2. Recovery Scenario 2

<table>
<tr>
<td>50. ☐</td>
<td>NOAM VIP GUI: Verify the database states</td>
<td>
1. Navigate to Status and Manager > Database.


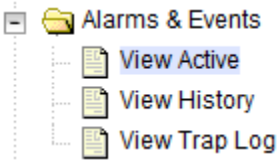
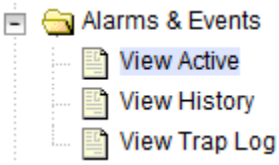
2. Verify the OAM Max HA Role is either Active or Standby for NOAM and SOAM; Application Max HA Role for MPs is Active; and status is Normal:
<table>
<tr><th>Network Element</th><th>Server</th><th>Role</th><th>OAM Max HA Role</th></tr>
<tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM1</td><td>Network OAM&P</td><td>Active</td></tr>
<tr><td>ZombieNOAM</td><td>ZombieNOAM2</td><td>Network OAM&P</td><td>Standby</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSOAM2</td><td>System OAM</td><td>N/A</td></tr>
<tr><td>ZombieNOAM</td><td>ZombieNOAM1</td><td>Network OAM&P</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSOAM1</td><td>System OAM</td><td>Active</td></tr>
<tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM2</td><td>Network OAM&P</td><td>Standby</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieDAMP2</td><td>MP</td><td>Standby</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSS7MP2</td><td>MP</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSS7MP1</td><td>MP</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieIPFE1</td><td>MP</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieIPFE2</td><td>MP</td><td>Active</td></tr>
</table>
</td>
</tr>
<tr>
<td>51. ☐</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>
</table>

Procedure 2. Recovery Scenario 2

52. ☐	**MP Servers**: Disable SCTP auth flag	For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [14]. Execute this procedure on all failed MP servers.
53. ☐	**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 disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution.
54. ☐	**SOAM VIP GUI**: Enable optional features	1. Navigate to **Diameter > Maintenance > Applications**.  2. Select the optional feature application configured in **step 47**. 3. Click **Enable**. 
55. ☐	**SOAM VIP GUI**: Re-enable transports, if needed	1. Navigate to **Transport Manager > Maintenance > Transport**.  2. Select each transport and click **Enable**.  3. Verify the Operational Status for each transport is **Up**.

Procedure 2. Recovery Scenario 2

56. ☐	**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).
57. ☐	**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.
58. ☐	Backup and archive all the databases from the recovered system	Execute DSR Database Backup to back up the Configuration databases.
59. ☐	Recover IDIH	If IDIH were affected, refer to IDIH Disaster Recovery to perform disaster recovery on IDIH.

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 of base hardware and software and then executing a database restore to the active NOAM server using a NOAM database backup file obtained from external backup sources such as customer servers or NetBackup. All other servers are recovered using recovery procedures of base hardware and software. Database replication from the active NOAM/active SOAM server recovers 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 procedure detailed steps are in Procedure 3. The major activities are summarized as follows:

- Recover **Active NOAM** server by recovering base hardware, software and the database
  - Recover the base hardware
  - Recover the software
  - Recover the database
- Recover **NOAM servers** by recovering base hardware and software
  - Recover the base hardware

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

Procedure 3. Recovery Scenario 3

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. ☐	Gather required materials	Gather the documents and required materials listed in the Required Materials section.
2. ☐	Replace failed equipment	HW vendor to replace the failed equipment.
3. ☐	**RMS NOAM Failure**: Configure BIOS settings and update firmware	If the failed server is **NOT** a rack mount server, **skip to step 8**. 1. Configure and verify the BIOS settings by executing procedure **Configure the RMS and Blade Server BIOS Settings** from reference [10]. 2. Verify and/or upgrade server firmware by executing procedure **Upgrade Management Server Firmware** from reference [10]. ***Note***: Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.
4. ☐	**RMS NOAM Failure**: Backups Available	If the failed server is **NOT** a rack mount server, **skip to step 8**. This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, **skip this step**. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media. If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing Restore PMAC from Backup**.**
5. ☐	**RMS NOAM Failure**: Backups NOT available	If the failed server is **NOT** a rack mount server, **skip to step 8.** This step assumes that TVOE and PMAC backups **NOT** are available, if the TVOE and PMAC have already been restored, **skip this step.** If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. **Configure and IPM Management Server** from reference [10]. 2. **Install PMAC** from reference [10]. 3. **Configure PMAC** from reference [10]. If the PMAC is **NOT** located on the same TVOE host as the failed NOAM, Execute the following sections/procedures: 1. **Installing TVOE on Rack Mount Server(s)** from reference [10].

Procedure 3. Recovery Scenario 3

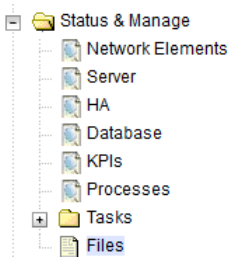
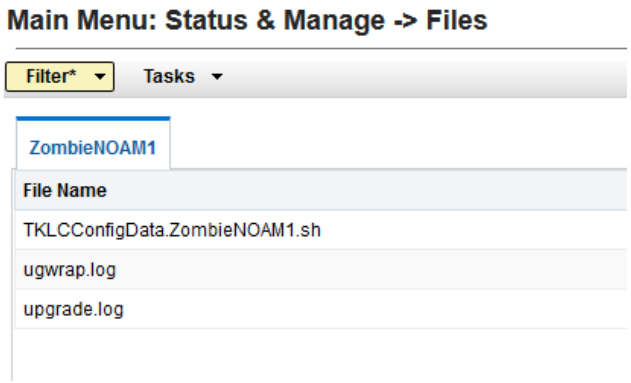
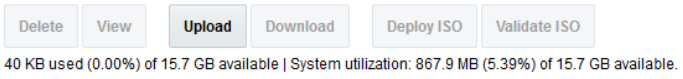
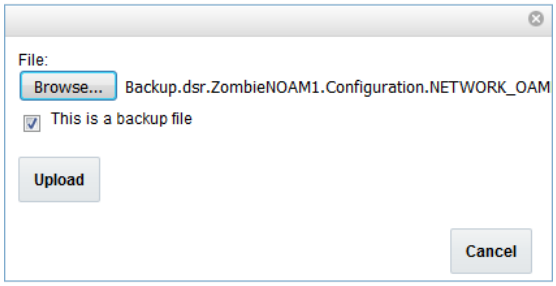
6. ☐	Recover failed aggregation/ enclosure switches, and OAs	Recover failed OAs, aggregation and enclosure switches, if needed. Backups Available: 1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches. Backups **NOT** Available, execute: 1. **HP C-7000 Enclosure Configuration** from reference [10] to recover and configure any failed OAs, if needed. 2. **Configure Enclosure Switches** from reference [10] to recover enclosure switches, if needed.
7. ☐	**HP-Class Blade Failure**: Configure blade server iLO, update firmware/BIOS settings	If the failed server is **NOT** an HP C-Class Blade, **skip to step 11**. 1. Execute **Configure Blade Server iLO Password for Administrator Account** from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing **Server Blades Installation Preparation** from reference [10].
8. ☐	**HP-Class Blade Failure**: Backups available	If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 11**. This step assumes TVOE backups are available. If backups are **NOT** available, **skip this step**. 1. Install and configure TVOE on failed TVOE blade servers by executing **Install TVOE on Blade Servers** from reference [10]. 2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on **ALL** failed TVOE Host blade servers.
9. ☐	**HP-Class Blade Failure**: Backups NOT available	If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 11**. This step assumes TVOE backups are **NOT** are available. Install and configure TVOE on failed TVOE blade servers by executing section **Install TVOE on Blade Servers** from reference [10].

10. ☐	Execute fast deployment file for NOAMs	The backup fdconfig file used during the initial DSR installation is available on the PMAC, if a database backup was restored on the PMAC.
		If a backup fast deployment xml is NOT available, execute **Configure NOAM Servers** from reference [8].
		If a backup fast deployment xml is already present on the PMAC, execute the following procedure:
		1. Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade has been performed since initial installation).
		2. Execute these commands:
		`$ cd /usr/TKLC/smac/etc`
		`$ screen`
		`$ sudo fdconfig config --file=<Created_FD_File>.xml`

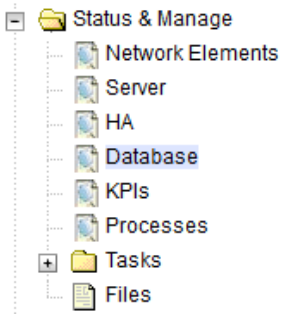
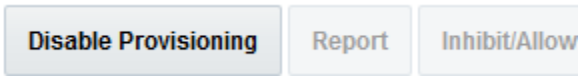
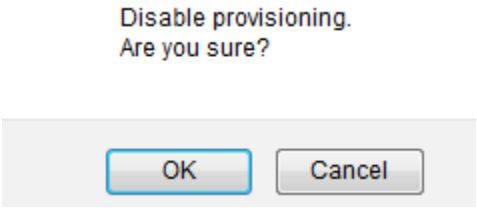
Procedure 3. Recovery Scenario 3

11. ☐	Obtain latest database backup and network configuration data	Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. From required materials list in the Required Materials section; use the site survey documents and Network Element report (if available) to determine network configuration data.
12. ☐	Execute DSR installation procedure for the first NOAM	1. Configure the first NOAM server by executing procedure **Configure the First NOAM NE and Server** from reference [8]. 2. Configure the NOAM server group by executing procedure **Configure the NOAM Server Group** from reference [8]. ***Note***: Use the backup copy of network configuration data and site surveys (step 2).
13. ☐	**NOAM GUI**: Login	Log into the NOAM GUI as the **guiadmin** user: 

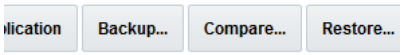
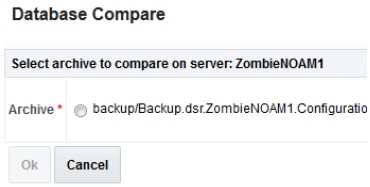
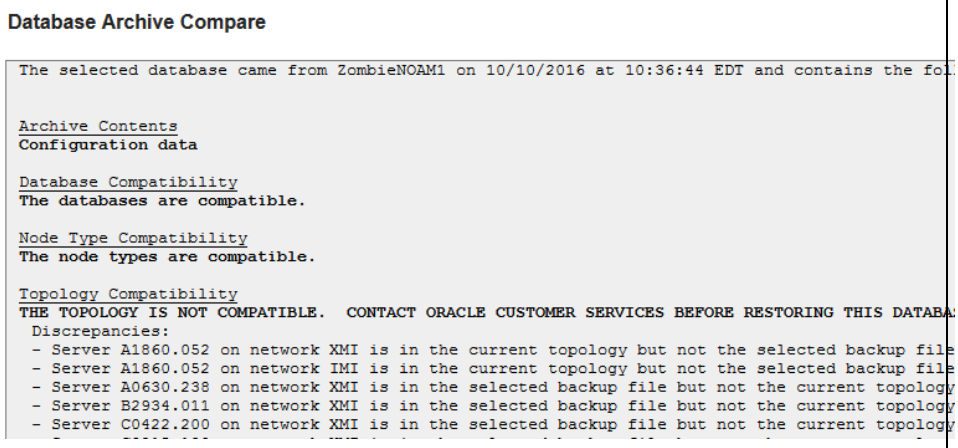
Procedure 3. Recovery Scenario 3

14. ☐	**NOAM GUI**: Upload the backed up database file	1. Navigate to **Status and Manage > Files**.  2. Select the active NOAM server.  3. Click **Upload** and select the file **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.

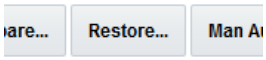
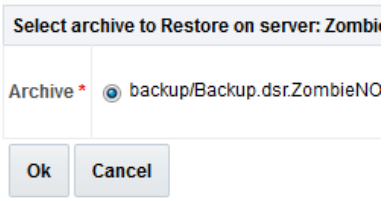
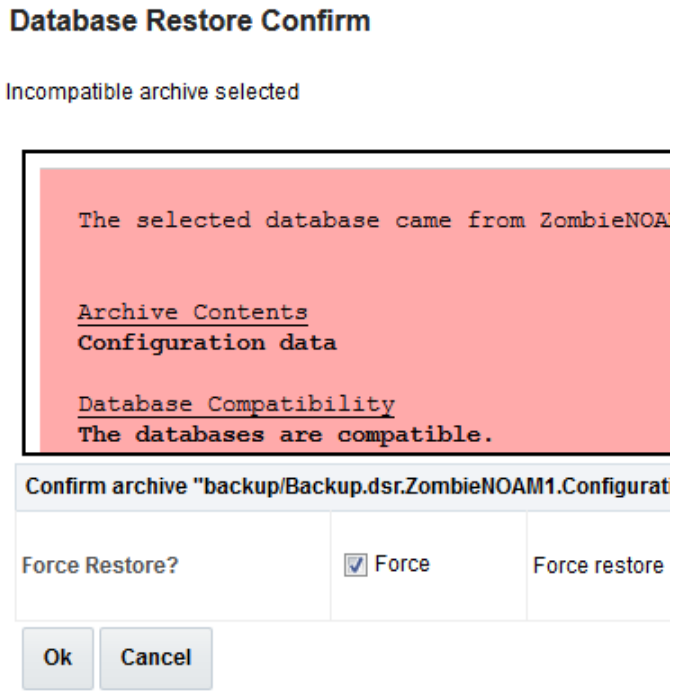
Procedure 3. Recovery Scenario 3

15. ☐	**NOAM GUI**: Disable provisioning	1. Navigate to **Status and Manage > Database**.  2. Click **Disable Provisioning**.  3. A confirmation window displays. Click **OK** to disable provisioning. 

Procedure 3. Recovery Scenario 3

16. ☐	**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 15 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) displays. 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 existing backed up data base to database with just one NOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. ***Note***: We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility. 4. If the verification is successful, click **Back**.

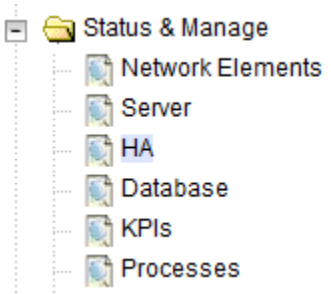
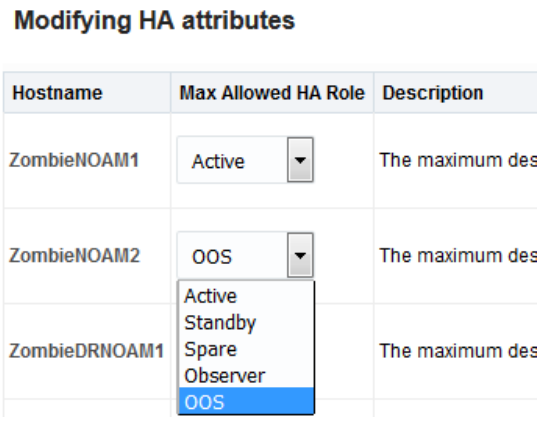
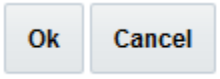
Procedure 3. Recovery Scenario 3

17. ☐	**Active NOAM**: Restore the database	1. Navigate to **Status and Manage > Database**. 2. Select the **Active NOAM** server and click **Restore**.  3. Select the proper back up 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.

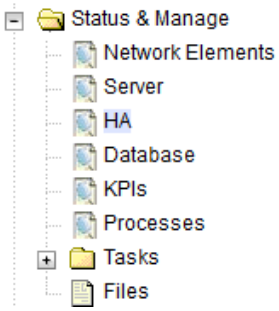
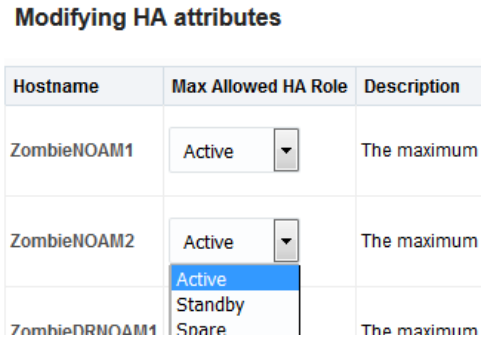
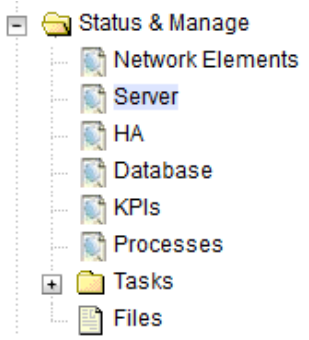
Procedure 3. Recovery Scenario 3

18. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 
19. ☐	**NOAM VIP GUI**: Monitor and confirm database restoral	Wait for **5-10 minutes** for the System to stabilize with the new topology: Monitor the Info tab for **Success**. This indicates the restore is complete and the system is stabilized. Ignore the following 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.

Procedure 3. Recovery Scenario 3

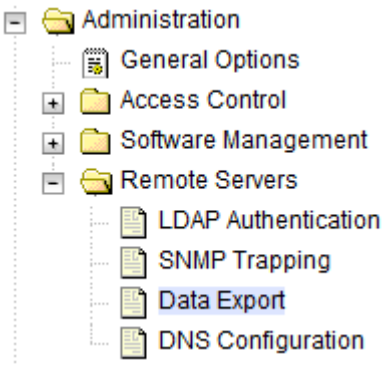
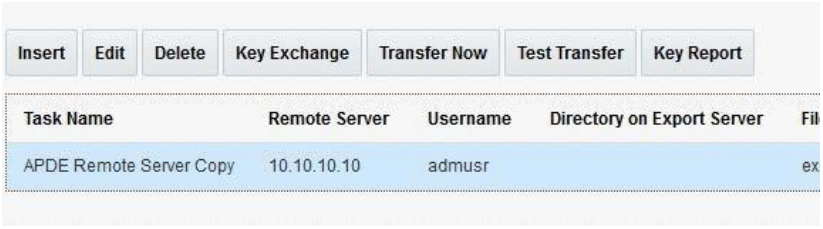
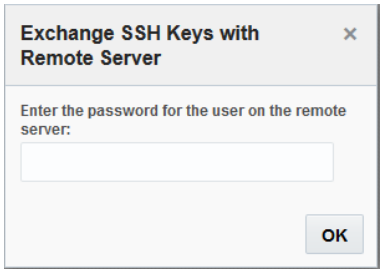
20. ☐	**Active NOAM**: Set failed servers to OOS	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**.  3. Set the Max Allowed HA Role drop down box to **OOS** for the failed servers. 4. Click **OK**. 
21. ☐	**Active NOAM**: Login	Log into the recovered active NOAM using SSH terminal as **admusr** user.
22. ☐	**NOAM VIP GUI**: Recover standby NOAM	Install the second NOAM server by executing procedure **Configure the Second NOAM Server,** steps 3-5, 7 from reference [8]. ***Note***: Execute step 6 if NetBackup is used.

Procedure 3. Recovery Scenario 3

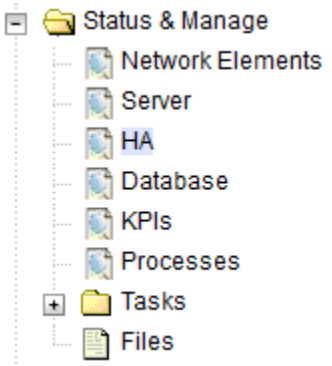
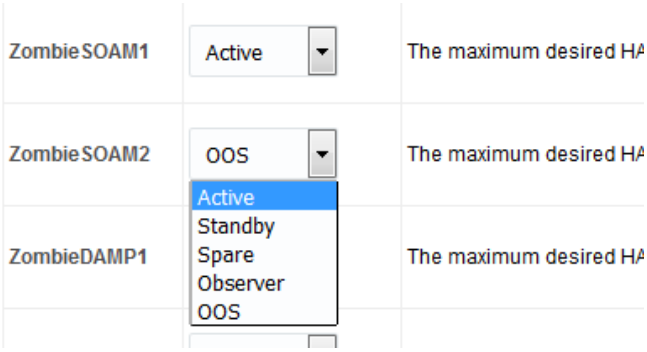
23. ☐	**NOAM VIP GUI**: Set HA on standby NOAM	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Select the standby NOAM server and set it to **Active**.  4. Click **OK**.
24. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered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

Procedure 3. Recovery Scenario 3

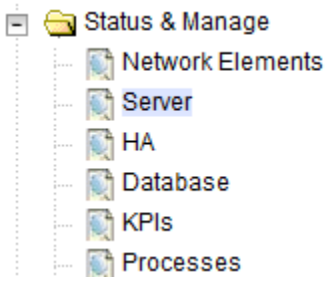
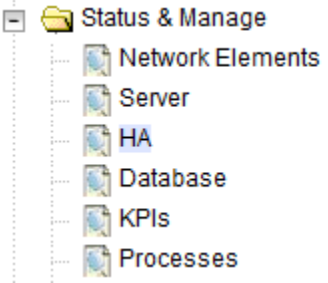
25. ☐	**Active NOAM**: Correct the recognized authority table	1. Establish an SSH session to the active NOAM, login as **admusr**.
		2. Execute this command:
		`$ sudo top.setPrimary`
		`- Using my cluster: A1789`
		`- New Primary Timestamp: 11/09/15 20:21:43.418`
		`- Updating A1789.022: <DSR_NOAM_B_hostname>`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

26. ☐	Install NetBackup client (Optional)	If NetBackup is used, execute **Install NetBackup Client** from reference [8].
27. ☐	**NOAM VIP GUI**: Perform Keyexchange with export server	1. Navigate to **Administration > Remote Servers > Data Export**.  2. Click the **Task Name** and click **Key Exchange**.  3. Type the **Password** and click **OK**.  4. Repeat for each task.

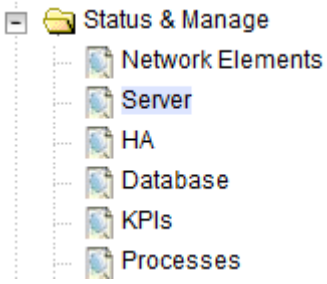
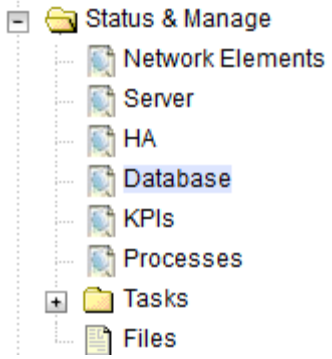
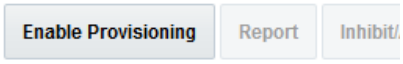
Procedure 3. Recovery Scenario 3

28. ☐	**NOAM VIP GUI**: Recover failed SOAM servers	Recover failed SOAM servers (**standby, spare**) by repeating these steps for each SOAM server: 1. Execute **Configure the SOAM Servers**, steps 1-3 and 5-8, from reference [8]. ***Note***: If you are using NetBackup, also execute step 10. 2. If you are using NetBackup, execute **Install NetBackup Client** from reference [8].
29. ☐	**NOAM VIP GUI**: Set HA on standby SOAM	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**.  3. Select the standby SOAM server and set it to **Active**. 4. Click **OK**.

Procedure 3. Recovery Scenario 3

30. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered standby SOAM server and click **Restart**. 
31. ☐	**NOAM VIP GUI**: Recover the C-level server (DA-MP, SBRs, IPFE)	Execute **Configure MP Blade Servers**, Steps 1, 7, 11-14, and 17, from reference [8]. ***Note***: Also, execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. Repeat this step for any remaining failed MP servers.
32. ☐	**NOAM VIP GUI**: Set HA on all C-level servers	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. For each server whose Max Allowed HA Role is set to OOS, set it to **Active**.  4. Click **OK**.

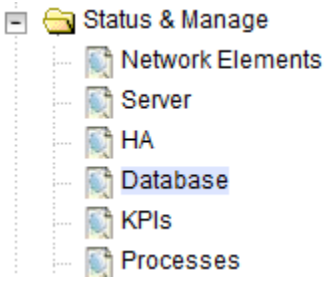
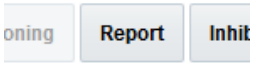
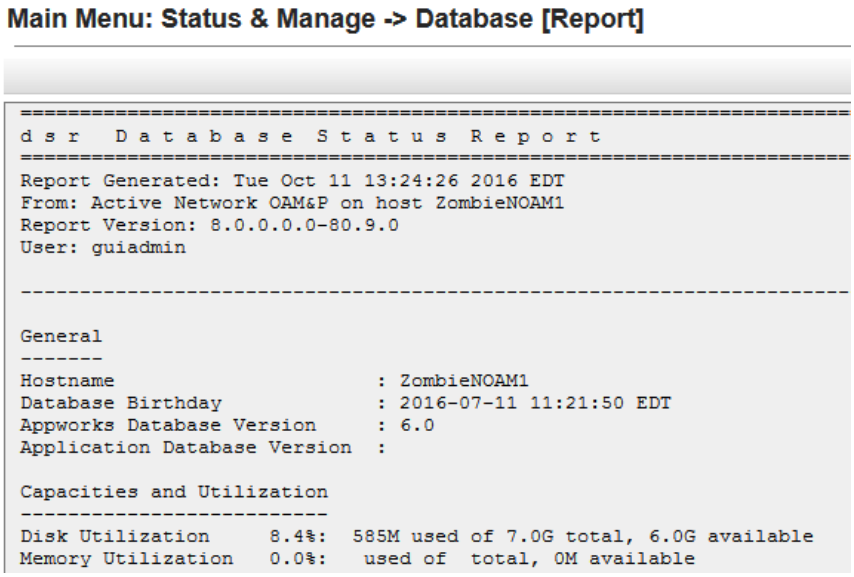
Procedure 3. Recovery Scenario 3

33. ☐	**NOAM VIP GUI**: Restart DSR application on recovered C-level servers	1. Navigate to **Status and Manage > Server**.  2. Select the recovered C-level servers and click **Restart**. 
34. ☐	**NOAM VIP GUI**: Enable provisioning	1. Navigate to **Status and Manage > Database**.  2. Click **Enable Provisioning**.  3. A confirmation window displays. Click **OK** to enable Provisioning.
35. ☐	**Active NOAM:** Perform keyexchange between the active-NOAM and recovered servers	1. Establish an SSH session to the active NOAM, 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.

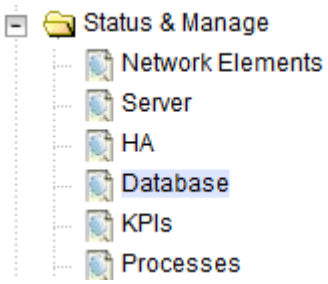
Procedure 3. Recovery Scenario 3

36. ☐	**Active NOAM**: Activate optional features	Establish an SSH session to the active NOAM, login as **admusr.** **Note For PCA Activation:** If you have PCA installed in the system being recovered, re-activate PCA by executing **PCA Activation on Active NOAM server** on recovered active NOAM server and **PCA Activation on Standby SOAM server** on recovered standby SOAM from [13]. Refer to Optional Features to activate any features that were previously activated. ***Note***: While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: `iload#31000{S/W Fault}` ***Note***: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.

Procedure 3. Recovery Scenario 3

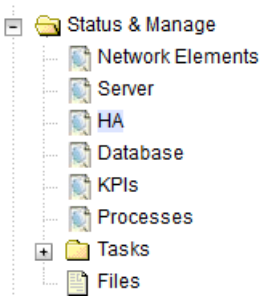
37. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status and Manage > Database**.  2. Select the active NOAM server and click **Report**.  The following screen is displayed:  3. Click **Save** and save the report to your local machine.

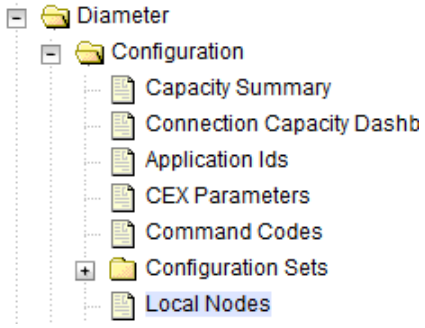
Procedure 3. Recovery Scenario 3

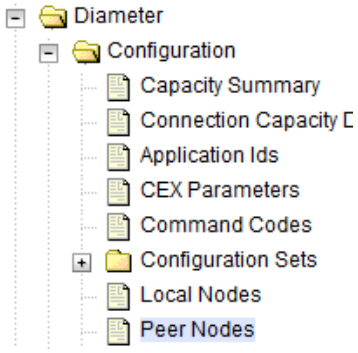
<table>
<tr>
<td>38. ☐</td>
<td>Active NOAM: Verify replication between servers</td>
<td>
1. Log into the active NOAM using SSH terminal as admusr.
2. Execute this command:
<pre>$ sudo irepstat –m</pre>
Output:
<pre>-- Policy 0 ActStb [DbReplication] ----------------------
RDU06-MP1 -- Stby
BC From RDU06-SO1 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>39. ☐</td>
<td>NOAM VIP GUI: Verify the database states</td>
<td>
1. Navigate to Status and Manager > Database.


2. Verify the OAM Max HA Role is either Active or Standby for NOAM and SOAM; Application Max HA Role for MPs is Active; and status is Normal:
<table>
<tr><th>Network Element</th><th>Server</th><th>Role</th><th>OAM Max HA Role</th></tr>
<tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM1</td><td>Network OAM&P</td><td>Active</td></tr>
<tr><td>ZombieNOAM</td><td>ZombieNOAM2</td><td>Network OAM&P</td><td>Standby</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSOAM2</td><td>System OAM</td><td>N/A</td></tr>
<tr><td>ZombieNOAM</td><td>ZombieNOAM1</td><td>Network OAM&P</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSOAM1</td><td>System OAM</td><td>Active</td></tr>
<tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM2</td><td>Network OAM&P</td><td>Standby</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieDAMP2</td><td>MP</td><td>Standby</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSS7MP2</td><td>MP</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSS7MP1</td><td>MP</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieIPFE1</td><td>MP</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieIPFE2</td><td>MP</td><td>Active</td></tr>
</table>
</td>
</tr>
</table>

Procedure 3. Recovery Scenario 3

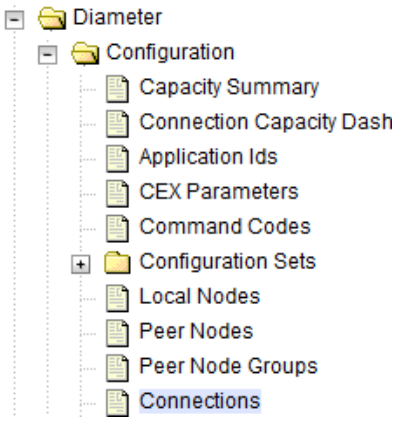
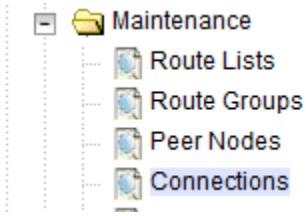
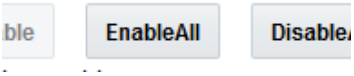
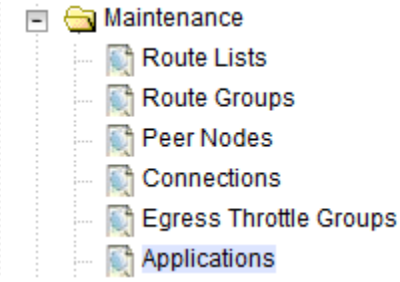
<table>
<tr>
<td>40. ☐</td>
<td>NOAM VIP GUI: Verify the HA status</td>
<td>
1. Navigate to Status and Manage > HA.


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>41. ☐</td>
<td>SOAM VIP GUI: Verify the local node info</td>
<td>
1. Navigate to Diameter > Configuration > Local Node.


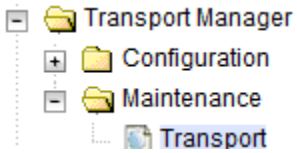
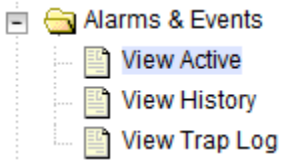
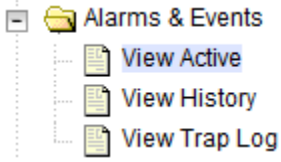
2. Verify all the local nodes are shown.
</td>
</tr>
<tr>
<td>42. ☐</td>
<td>SOAM VIP GUI: Verify the peer node info</td>
<td>
1. Navigate to Diameter > Configuration > Peer Node.


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

Procedure 3. Recovery Scenario 3

43. ☐	**SOAM VIP GUI**: Verify the connections info	1. Navigate to **Diameter > Configuration > Connections**.  2. Verify all the connections are shown.
44. ☐	**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
45. ☐	**SOAM VIP GUI**: Enable optional features	1. Navigate to **Diameter > Maintenance > Applications**.  2. Select the optional feature application configured in step 36. . 3. Click **Enable**. 

Procedure 3. Recovery Scenario 3

46. ☐	**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**.
47. ☐	**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).
48. ☐	**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).
49. ☐	Restore GUI usernames and passwords	If applicable, execute Resolving User Credential Issues after Database Restore to recover the user and group information restored.
50. ☐	Backup and archive all the databases from the recovered system	Execute DSR Database Backup to back up the Configuration databases.
51. ☐	Recover IDIH	If IDIH were affected, refer to IDIH Disaster Recovery to perform disaster recovery on IDIH.

Procedure 3. Recovery Scenario 3

52. ☐	SNMP workaround	Refer SNMP Configuration to configure SNMP as a workaround in the following cases: 1. If SNMP is not configured in DSR. 2. If SNMP is already configured and **SNMPv3** is selected as enabled version.

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 hardware and 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 base hardware and software.
  - Recover the base hardware
  - Recover the software
- The database is intact at the active NOAM server and does not require restoration at the standby NOAM server.
  - Recover any failed SO and MP servers by recovering base hardware and software.
  - Recover the base hardware
  - Recover the software
- The database 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

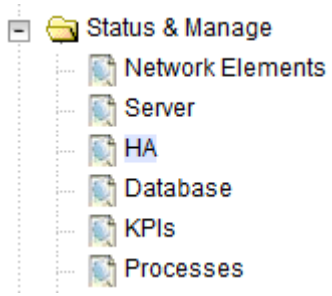
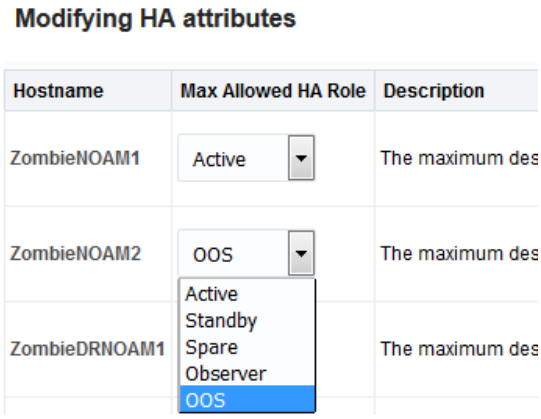
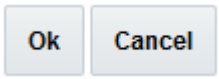
Procedure 4. Recovery Scenario 4

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. ☐	Workarounds	Refer to SNMP Configuration to configure SNMP as a workaround in the following cases: 1. If SNMP is not configured in DSR 2. If SNMP is already configured and **SNMPv3** is selected as enabled version
2. ☐	Gather required materials	Gather the documents and required materials listed in Required Materials section.

Procedure 4. Recovery Scenario 4

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

Procedure 4. Recovery Scenario 4

4. ☐	**Active NOAM**: Set failed servers to OOS	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**.  3. Set the Max Allowed HA Role to **OOS** for the failed servers. 4. Select **OK**. 
5. ☐	**RMS NOAM Failure**: Configure BIOS settings and update firmware	If the failed server is **NOT** a rack mount server, **skip to step 9.** 1. Configure and verify the BIOS settings by executing procedure **Configure the RMS and Blade Server BIOS Settings** from reference [10]. 2. Verify and/or upgrade server firmware by executing procedure **Upgrade Management Server Firmware** from reference[10]. ***Note***: Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.
6. ☐	**RMS NOAM Failure**: Backups available	If the failed server is **NOT** a rack mount server, **skip to step 9.** This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, **skip this step**. 1. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media. 2. If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing Restore PMAC from Backup.

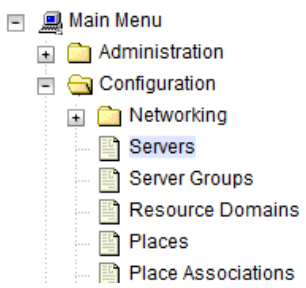
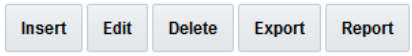
Procedure 4. Recovery Scenario 4

7. ☐	**RMS NOAM Failure**: Backups NOT available	This step assumes that TVOE and PMAC backups are **NOT** available, if the TVOE and PMAC have already been restored, **skip this step**. If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. **Configure and IPM Management Server** from reference [10]. 2. **Install PMAC** from reference [10]. 3. **Configure PMAC** from reference [10]. If the PMAC is NOT located on the same TVOE host as the failed NOAM, execute the following sections/procedures. 1. **Installing TVOE on Rack Mount Server(s)** from reference [10].
8. ☐	Recover failed aggregation/ enclosure switches, and OAs	Recover failed OAs, aggregation and enclosure switches, if needed. Backups Available: 1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches Backups **NOT** available, execute: 1. **HP C-7000 Enclosure Configuration** from reference [10] to recover and configure any failed OAs, if needed. 2. **Configure Enclosure Switches** from reference [10] to recover enclosure switches, if needed.
9. ☐	**HP-Class Blade Failure**: Configure blade server iLO, update firmware/BIOS settings	If the failed server is **NOT** an HP C-Class Blade, **skip to step 12.** 1. **Configure Blade Server iLO Password for Administrator Account** from reference [10]. 2. Verify/Update blade server firmware and BIOS settings by executing **Server Blades Installation Preparation** from reference [10]
10. ☐	**HP-Class Blade Failure**: Backups available	If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 13.** This step assumes that TVOE backups are available, if backups are **NOT** available, **skip this step**. 1. Install and configure TVOE on failed TVOE blade servers by executing **Install TVOE on Blade Servers** from reference [10]. 2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on **ALL** failed TVOE Host blade servers.
11. ☐	**HP-Class Blade Failure**: Backups NOT available	If the failed server is **NOT** an OAM HP C-Class Blade, **skip to step 13.** This step assumes that TVOE backups are **NOT** available 1. Install and configure TVOE on failed TVOE blade servers by executing **Install TVOE on Blade Servers** from reference [10]. 2. Configure the NOAM and/or SOAM failed TVOE server blades by executing **Configure SOAM TVOE Server Blades** from reference [8]. ***Note***: Although the title of the procedure is related to SOAMs only, execute this procedure for any failed NOAMs located on TVOE server blades.

Procedure 4. Recovery Scenario 4

12. ☐	Create VMs	Execute Create NOAM/SOAM Virtual Machines to create the NOAM and SOAM VMs on failed TVOE servers.
13. ☐	IPM and install DSR application on failed guest/servers	1. Execute **IPM Blades and VMs** for the failed SOAM VMs and MP blades from reference [8]. 2. Execute **Install the Application Software** for the failed NOAM and SOAM VMs and MP blades from reference [8].
14. ☐	Install NetBackup client (Optional)	If NetBackup is used, execute **Install NetBackup Client** from reference [8].
15. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 

Procedure 4. Recovery Scenario 4

16. ☐	Exchange SSH keys between PMAC and failed NOAM server	1. Use the PMAC GUI to determine the Control Network IP address of the failed NOAM server VM. From the PMAC GUI, navigate to **Software > Software Inventory**. 2. Note the IP address for the failed NOAM server VM. 3. Log into the PMAC terminal as the **admusr**. 4. From a terminal window connection on the PMAC as the **admusr** user, exchange SSH keys for **admusr** between the PMAC and the failed NOAM server VM control network IP address. When prompted for the password, enter the password for the **admusr** user of the NOAM server. `$ keyexchange admusr@<NO2_Control_IP Address>` ***Note***: If Key exchange fails, edit /home/admusr/.ssh/known_hosts and remove blank lines, and retry the keyexchange commands.
17. ☐	**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. 
18. ☐	**NOAM VIP**: Copy configuration file to failed NOAM server	1. Obtain a terminal session to the NOAM VIP, login as the **admusr**. 2. Use the **awpushcfg** utility to copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the active NOAM to the failed NOAM server, using the Control network IP address for the failed NOAM VM. The configuration file has a filename like **TKLCConfigData.<hostname>.sh**. `$ sudo awpushcfg` 3. The awpushcfg utility is interactive, so the user is prompted for the following: • IP address of the local PMAC server: Use the local control network address from the PMAC. • Username: Use **admusr** • Control network IP address for the target server: In this case, enter the control IP for the failed NOAM VM). • Hostname of the target server: Enter the server name from **Step 17**.

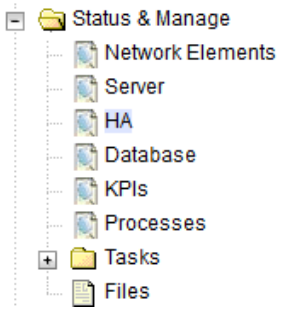
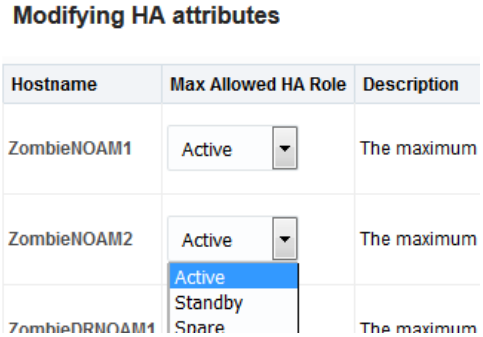
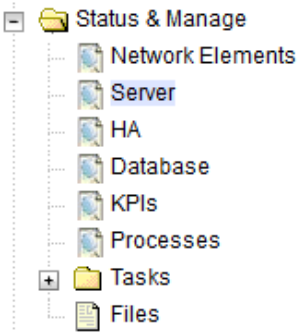
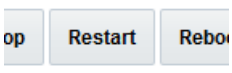
Procedure 4. Recovery Scenario 4

19. ☐	**Failed NOAM Server**: Verify awpushcfg was called and reboot the server	1. Establish an SSH session to the failed NOAM server, login as the **admusr** user.
		2. The automatic configuration daemon looks for the file named **TKLCConfigData.sh** in the **/var/tmp** directory, implements the configuration in the file, and asks the user to reboot the server.
		3. Verify awpushcfg was called by checking the following file
		`$ sudo cat /var/TKLC/appw/logs/Process/install.log`
		Verify this message displays:
		`[SUCCESS] script completed successfully!`
		4. Now reboot the server:
		`$ sudo init 6`
		5. Wait for the server to reboot

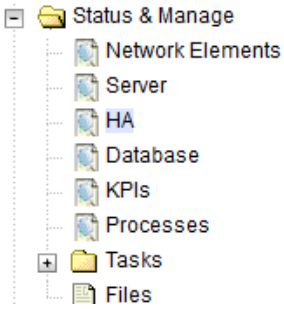
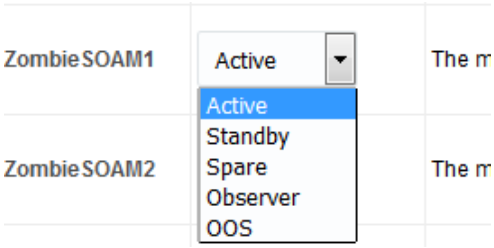
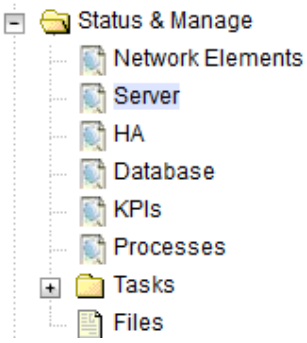
20. ☐	**Failed NOAM Server**: Configure networking for dedicated NetBackup interface (Optional)	***Note***: Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.
		Obtain a terminal window to the failed NOAM server, logging in as the **admusr**.
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP_Adress> --netmask=<NO2_NetBackup_NetMask>`
		`$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NO1_NetBackup_Network_ID> --netmask=<NO2_NetBackup_NetMask> --gateway=<NO2_NetBackup_Gateway_IP_Address>`

21. ☐	**Failed NOAM Server**: Verify server health	Execute this command on the 2nd 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`

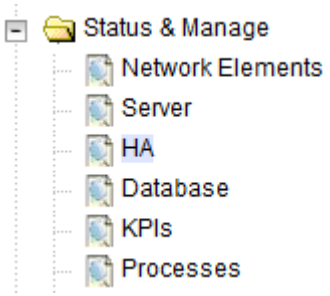
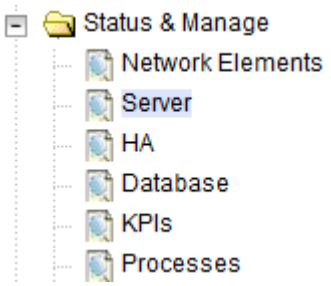
Procedure 4. Recovery Scenario 4

22. ☐	**NOAM VIP GUI**: Set HA on standby NOAM	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Select the standby NOAM server and set it to **Active**.  4. Click **OK**.
23. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**. 
24. ☐	**NOAM VIP GUI**: Recover failed SOAM servers	Recover failed SOAM servers (standby, spare) by repeating these steps for each SOAM server: 1. Execute **Configure the SOAM Servers**, steps 1-3 and 5-8, from reference [8]. ***Note***: If you are using NetBackup, also execute step 10. 2. If you are using NetBackup, execute **Install NetBackup Client** from reference [8].

Procedure 4. Recovery Scenario 4

25. ☐	**NOAM VIP GUI**: Set HA on standby SOAM	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. Select the SOAM server and set it to **Active**.  4. Click **OK**.
26. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered SOAM server and click **Restart**. 
27. ☐	**NOAM VIP GUI**: Recover the C-level server (DA-MP, SBRs, IPFE)	1. Execute **Configure MP Blade Servers**, steps 1, 7, 11-14, and 17, from reference [8]. ***Note***: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. 2. Repeat this step for any remaining failed MP servers.

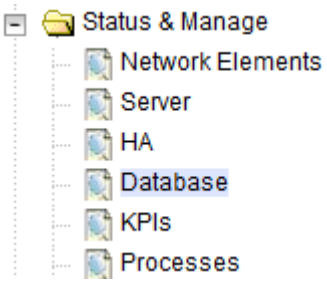
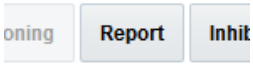
Procedure 4. Recovery Scenario 4

28. ☐	**NOAM VIP GUI**: Set HA on all C-level servers	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. For each server whose Max Allowed HA Role is set to OOS, set it to **Active**.  4. Click **OK**.
29. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select the recovered C-level servers and click **Restart**. 
30. ☐	**Active NOAM**: Login	Log into the recovered active NOAM using SSH terminal as **admusr** user.
31. ☐	**Active NOAM**: Perform key exchange between the active-NOAM and recovered servers	1. Establish an SSH session to the active NOAM, login as **admusr**. 2. Perform a keyexchange from the active NOAM to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>`

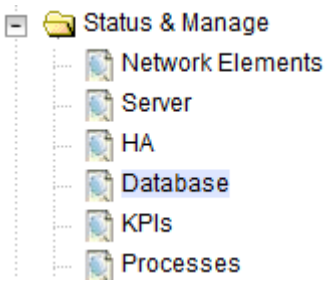
Procedure 4. Recovery Scenario 4

32. ☐	**Active NOAM**: Activate optional features	Establish an SSH session to the active NOAM, login as **admusr**. **Note For PCA Activation:** If you have PCA installed in the system being recovered, re-activate PCA by executing **PCA Activation on Standby NOAM Server** on the recovered standby NOAM server and **PCA Activation on Standby SOAM server** on the recovered standby SOAM server from [13]. Refer to Optional Features to activate any features that were previously activated. ***Note***: While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: `iload#31000{S/W Fault}` ***Note***: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.
33. ☐	**MP Servers**: Disable SCTP auth flag (DSR Only)	DSR Only, SDS **Skip This Step**. For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS from reference [14]. Execute this procedure on all failed MP servers.

Procedure 4. Recovery Scenario 4

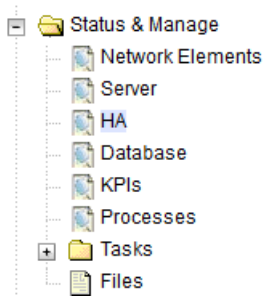
34. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status and Manage > Database**.
		 
		2. Select the active NOAM server and click **Report**.
		 
		The following screen is displayed:
		Main Menu: Status & Manage -> Database [Report]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

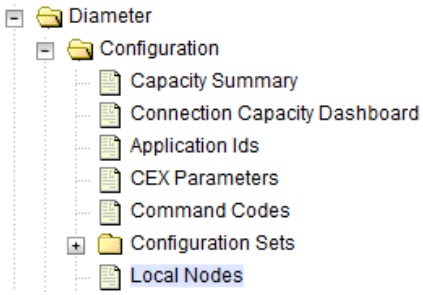
Procedure 4. Recovery Scenario 4

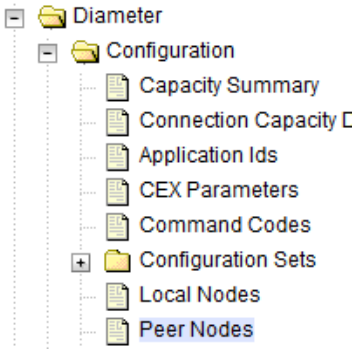
<table>
<tr>
<td>35. ☐</td>
<td>Active NOAM: Verify replication between servers</td>
<td>
1. Log into the active NOAM using SSH terminal as admusr.
2. Execute this command:
<pre>$ sudo irepstat -m</pre>
Output like below is generated:
<pre>-- Policy 0 ActStb [DbReplication] ---------------------
RDU06-MP1 -- 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>36. ☐</td>
<td>NOAM VIP GUI: Verify the database states</td>
<td>
1. Navigate to Status and Manager > Database.


2. Verify the OAM Max HA Role is either Active or Standby for NOAM and SOAM and Application Max HA Role for MPs is Active, and that the status is Normal.
<table>
<tr><th>Network Element</th><th>Server</th><th>Role</th><th>OAM Max HA Role</th></tr>
<tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM1</td><td>Network OAM&P</td><td>Active</td></tr>
<tr><td>ZombieNOAM</td><td>ZombieNOAM2</td><td>Network OAM&P</td><td>Standby</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSOAM2</td><td>System OAM</td><td>N/A</td></tr>
<tr><td>ZombieNOAM</td><td>ZombieNOAM1</td><td>Network OAM&P</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSOAM1</td><td>System OAM</td><td>Active</td></tr>
<tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM2</td><td>Network OAM&P</td><td>Standby</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieDAMP2</td><td>MP</td><td>Standby</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSS7MP2</td><td>MP</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSS7MP1</td><td>MP</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieIPFE1</td><td>MP</td><td>Active</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieIPFE2</td><td>MP</td><td>Active</td></tr>
</table>
</td>
</tr>
</table>

Procedure 4. Recovery Scenario 4

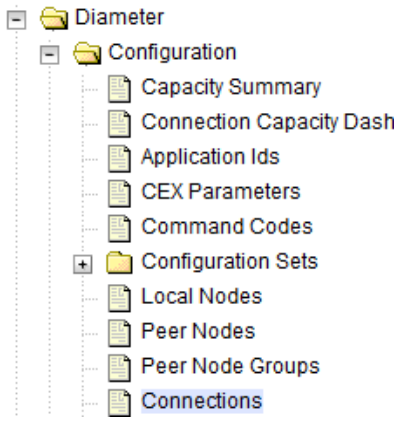
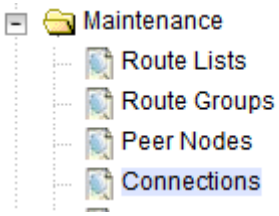
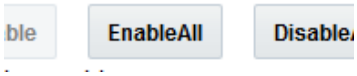
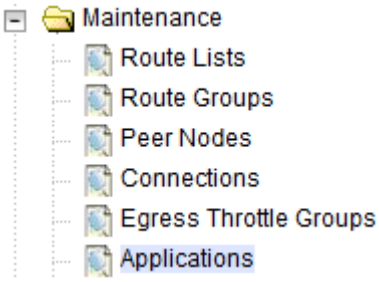
<table>
<tr>
<td>37. ☐</td>
<td>NOAM VIP GUI: Verify the HA status</td>
<td>
1. Navigate to Status and Manager > HA.


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>38. ☐</td>
<td>SOAM VIP GUI: Verify the local node info</td>
<td>
1. Navigate to Diameter > Configuration > Local Nodes.


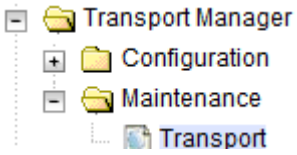
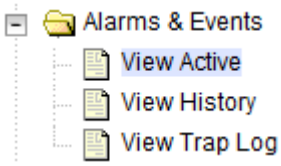
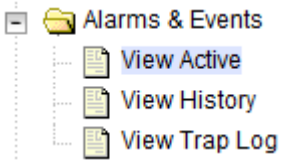
2. Verify all the connections are shown.
</td>
</tr>
<tr>
<td>39. ☐</td>
<td>SOAM VIP GUI: Verify the peer node info</td>
<td>
1. Navigate to Diameter > Configuration > Peer Node.


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

Procedure 4. Recovery Scenario 4

40. ☐	**SOAM VIP GUI**: Verify the connections info	1. Navigate to **Diameter > Configuration > Connections**.  2. Verify all the connections are shown.
41. ☐	**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.
42. ☐	**SOAM VIP GUI**: Enable optional features	1. Navigate to **Diameter > Maintenance > Applications**.  2. Select the optional feature application configured in step 32. 3. Click **Enable**. 

Procedure 4. Recovery Scenario 4

43. ☐	**SOAM VIP GUI**: Re-enable transports, if needed (Applicable ONLY for DSR 6.0+)	1. Navigate to **Transport Manager > Maintenance > Transport**.  2. Select each transport and click **Enable**.  3. Verify the Operational Status for each transport is **Up**.
44. ☐	**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).
45. ☐	**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).

46. ☐	Restart oampAgent, if needed	***Note***: If alarm 10012: The responder for a monitored table failed to respond to a table change is raised, the oampAgent needs to be restarted.
		1. Establish an SSH session to each server that has the alarm., login as **admusr**.
		2. Execute these commands:
		`$ sudo pm.set off oampAgent`
		`$ sudo pm.set on oampAgent`

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

Procedure 4. Recovery Scenario 4

48. ☐	Recover IDIH	If IDIH were affected, refer to IDIH Disaster Recovery to perform disaster recovery on IDIH.

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 base hardware and software
  - Recover the base hardware
  - Recover the software
  - The database is intact at the newly active NOAM server and does not require restoration
- If applicable, recover any failed SOAM and MP servers by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
  - The database in intact at the active NOAM server and does not require restoration at the SOAM and MP servers

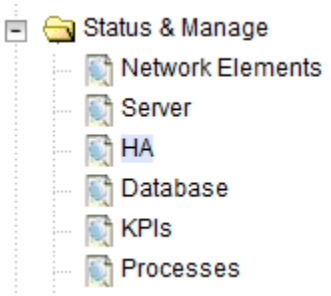
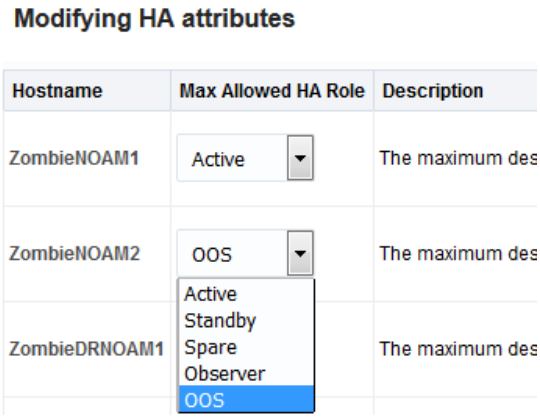
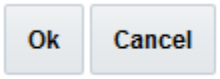
Procedure 5. Recovery Scenario 5

This procedure performs recovery if both NOAM servers have failed but a DR NOAM is available Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Workarounds	Refer to SNMP Configuration to configure SNMP as a workaround in the following cases: 1. If SNMP is not configured in DSR. 2. If SNMP is already configured and **SNMPv3** is selected as enabled version. **Note**: The Active Network server allows SNMP administration. The Global SNMP configuration cannot be modified if DR site is made Primary. It can be updated once original site becomes Primary again.
2. ☐	Gather required materials	Gather the documents and required materials listed in Required Materials section.
3. ☐	Switch DR NOAM to primary	Refer to DSR/SDS 8.x NOAM Failover User's Guide [17].
4. ☐	Recover failed SOAMs	If **ALL** SOAM servers have failed, execute Procedure 2.

Procedure 5. Recovery Scenario 5

5. ☐	**DR-NOAM VIP GUI**: Login	1. Establish a GUI session on the DR-NOAM server by using the VIP IP address of the DR-NOAM server. 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

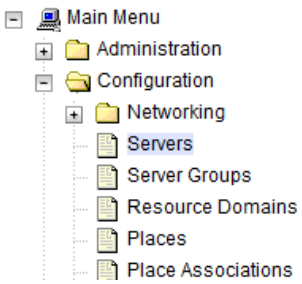
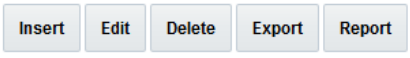
6. ☐	**DR-NOAM VIP GUI**: Set failed NOAM servers to standby	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**.  3. Set the Max Allowed HA Role drop down box to **OOS** for the failed servers. 4. Click **OK**. 
7. ☐	**RMS NOAM Failure**: Configure BIOS settings and update firmware	If the failed server is **NOT** a rack mount server, **skip to step 11**. 1. Configure and verify the BIOS settings by executing procedure **Configure the RMS and Blade Server BIOS Settings** from reference [10]. 2. Verify and/or upgrade server firmware by executing procedure **Upgrade Management Server Firmware** from reference[10]. ***Note***: Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.
8. ☐	**RMS NOAM Failure**: Backups available	If the failed server is **NOT** a rack mount server, **skip to step 11**. This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, **skip this step**. 1. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media. 2. If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing Restore PMAC from Backup.

Procedure 5. Recovery Scenario 5

9. ☐	Recover failed aggregation/ enclosure switches, and OAs	Recover failed OAs, aggregation, and enclosure switches, if needed. Backups available: 1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches. Backups **NOT** available, execute: 1. **HP C-7000 Enclosure Configuration** from reference [10] to recover and configure any failed OAs, if needed. 2. **Configure Enclosure Switches** from reference [10] to recover enclosure switches, if needed.
10. ☐	**RMS NOAM Failure**: Backups NOT available	If the failed server is **NOT** a rack mount server, **skip to step 11**. This step assumes that TVOE and PMAC backups are **NOT** available, if the TVOE and PMAC have already been restored, **skip this step**. If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. **Configure and IPM Management Server** from reference [10]. 2. **Install PMAC** from reference [10]. 3. **Configure PMAC** from reference [10]. If the PMAC is NOT located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. **Installing TVOE on Rack Mount Server(s)** from reference [10].
11. ☐	**HP-Class Blade Failure**: Configure blade server iLO, update firmware/BIOS settings	If the failed server is **NOT** an HP C-Class Blade, **skip to step 14**. 1. Execute **Configure Blade Server iLO Password for Administrator Account** from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing **Server Blades Installation Preparation** from reference [10]
12. ☐	**HP-Class Blade Failure**: Backups available	If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 14**. This step assumes that TVOE backups are available. If backups are **NOT** available, **skip this step**. 1. Install and configure TVOE on failed TVOE blade servers by executing **Install TVOE on Blade Servers** from reference [10]. 2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on **ALL** failed TVOE Host blade servers.
13. ☐	**HP-Class Blade Failure**: Backups NOT available	If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 14**. This step assumes TVOE backups are **NOT** are available. Install and configure TVOE on failed TVOE blade servers by executing **Install TVOE on Blade Servers** from reference [10].

Procedure 5. Recovery Scenario 5

14. ☐	Execute fast deployment file for NOAMs	The backup fdconfig file used during the initial DSR installation is available on the PMAC, if a database backup was restored on the PMAC.
		If a backup fast deployment xml is NOT available, execute **Configure NOAM Servers** from reference [8].
		If a backup fast deployment xml is already present on the PMAC, execute the following procedure:
		1. Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade has been performed since initial installation).
		2. Execute these commands:
		`$ cd /usr/TKLC/smac/etc`
		`$ screen`
		`$ sudo fdconfig config --file=<Created_FD_File>.xml`

15. ☐	**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. 
16. ☐	**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

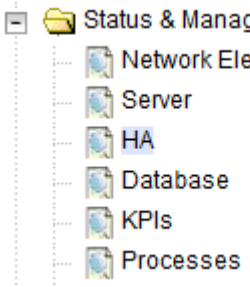
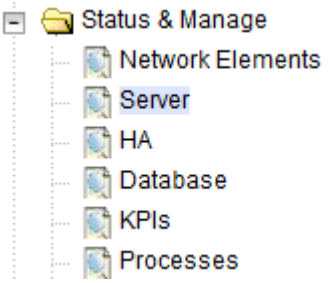
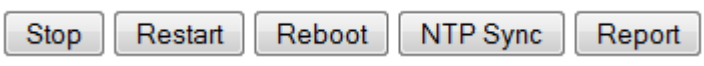
17. ☐	**Recovered NOAM Server**: Verify configuration was called and reboot the server	1. Establish an SSH session to the Recovered NOAM server (Recovered_NOAM_xmi_IP_address)
		2. Login as the **admusr** user.
		3. The automatic configuration daemon looks for the file named **TKLCConfigData.sh** in 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. Now reboot the server:
		`$ sudo init 6`
		6. Wait for the server to reboot

18. ☐	**Recovered NOAM Server**: Configure networking for dedicated netbackup interface (Optional)	***Note***: Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP_Adress> --netmask=<NO2_NetBackup_NetMask>`
		`$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NO1_NetBackup_Network_ID> --netmask=<NO2_NetBackup_NetMask> --gateway=<NO2_NetBackup_Gateway_IP_Address>`

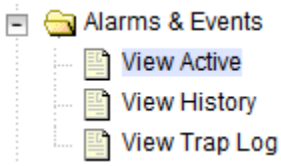
19. ☐	**Recovered NOAM Server**: Verify server health	Execute this command on the failed NOAM server and make sure no errors are returned:
		`$ sudo syscheck`
		`Running modules in class hardware...OK`
		`Running modules in class disk...OK`
		`Running modules in class net...OK`
		`Running modules in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

20. ☐	Repeat for additional 2nd failed NOAM	Repeat steps 15-19 for the 2nd failed NOAM server.

Procedure 5. Recovery Scenario 5

21. ☐	Perform keyexchange between active NOAM and recovered NOAMs	Perform a keyexchange between the newly active NOAM and the 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>`
22. ☐	**NOAM VIP GUI**: Set HA on recovered NOAMs	1. Navigate to **Status and Manage > HA**.  2. Click **Edit**. 3. For each NOAM server whose Max Allowed HA Role is set to **Standby**, set it to **Active**.  4. Click **OK**.
23. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status and Manage > Server**.  2. Select each recovered NOAM server and click **Restart**. 

Procedure 5. Recovery Scenario 5

24. ☐	**Recovered NOAM Servers**: Activate optional features	Policy and Charging Application (PCA) Activate the feature 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 [13] 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, login as **admusr**. ***Note***: If any of the MPs are failed and recovered, then these MP servers should be restarted after activation of the feature.
25. ☐	Switch DR NOAM back to secondary	Once the system have been recovered, refer to DSR/SDS 8.x NOAM Failover User's Guide [17].
26. ☐	**Recovered Servers**: Verify alarms	1. Navigate to **Alarms & Events > View Active**.  2. Verify the recovered servers are not contributing to any active alarms (Replication, Topology misconfiguration, database impairments, NTP, etc.)
27. ☐	**NOAM VIP GUI**: Recover standby/spare SOAM and C-level servers	If necessary, refer to Procedure 3 to recover any standby or Spare SOAMs as well as any C-level servers.
28. ☐	Recover IDIH	If IDIH were affected, refer to IDIH Disaster Recovery section to perform disaster recovery on IDIH.

4.6 Recovery Scenario 6 (Database Recovery)

4.6.1 Recovery Scenario 6: Case 1

For a partial outage with

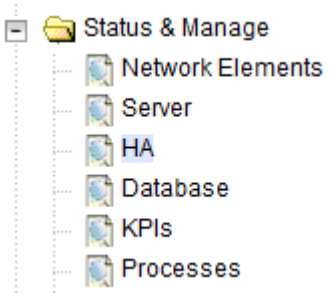
- Server having a corrupted database
- Replication channel from parent is inhibited because of upgrade activity; or
- Server is in a different release then that of its active parent because of upgrade activity
- Verify the server runtime backup files, performed at the start of the upgrade, are present 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

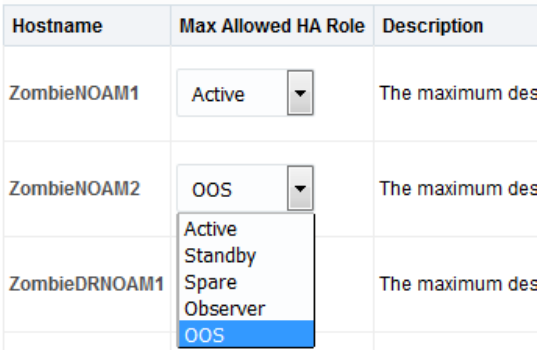
Note: During recovery, the corrupted database is replaced by the server runtime backup. Any configuration done after taking the backup is not available post recovery.

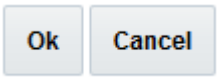
Procedure 6. Recovery Scenario 6 (Case 1)

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

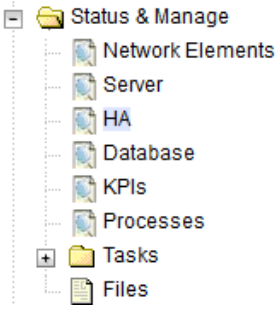
Procedure 6. Recovery Scenario 6 (Case 1)

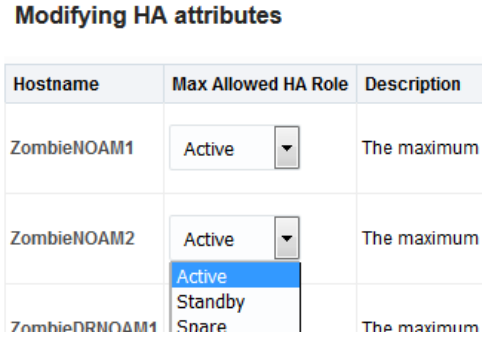
<table>
<tr><td>2. ☐</td><td>NOAM VIP GUI: Set failed servers to standby</td><td>1. Navigate to Status and Manage > HA.
 

2. Select Edit.
Modifying HA attributes
 

3. Set the Max Allowed HA Role drop down box to OOS for the failed servers.
4. Click OK.
 
</td></tr>
<tr><td>3. ☐</td><td>Server in Question: Login</td><td>Establish an SSH session to the server in question. Login as admusr.</td></tr>
<tr><td>4. ☐</td><td>Server in Question: Change runlevel to 3</td><td>Bring the system to runlevel 3.
<code>$ sudo init 3</code></td></tr>
<tr><td>5. ☐</td><td>Server in Question: Recover system</td><td>Execute this command and follow the instructions appearing in the console prompt.
<code>$ sudo /usr/TKLC/appworks/sbin/backout_restore</code></td></tr>
<tr><td>6. ☐</td><td>Server in Question: Change runlevel to 4</td><td>Bring the system back to runlevel 4.
<code>$ sudo init 6</code></td></tr>
</table>

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.
$ sudo pm.getprocs
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 and 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 DSR Database Backup to back up the Configuration databases.</td>
</tr>
</table>

4.6.2 Recovery Scenario 6: Case 2

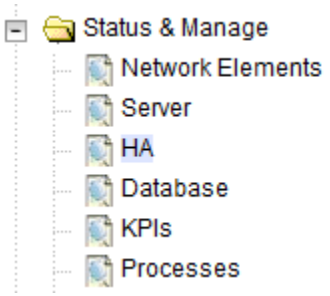
For a partial outage with:

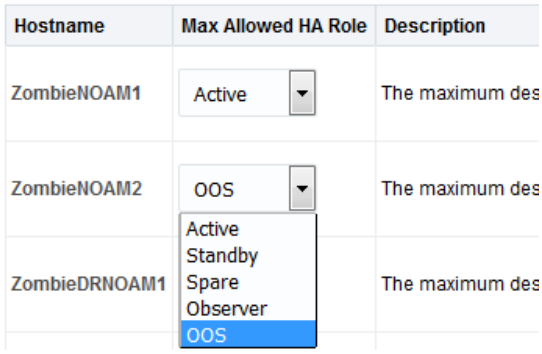
- Server having a corrupted database
- Replication channel is not inhibited; or
- Server has the same release as that of its active parent

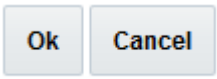
Procedure 7. Recovery Scenario 6 (Case 2)

This procedure performs recovery if database got corrupted in the system and system is in the state to get replicated. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 

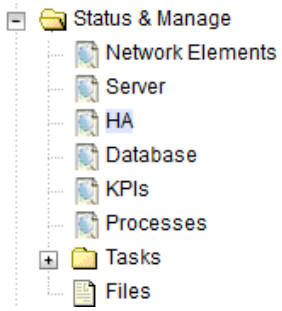
Procedure 7. Recovery Scenario 6 (Case 2)

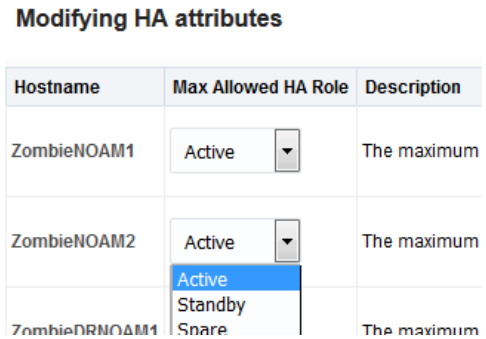
<table>
<tr><td>2. ☐</td><td>NOAM VIP GUI: Set failed servers to standby</td><td>1. Navigate to Status and Manage > HA.
 

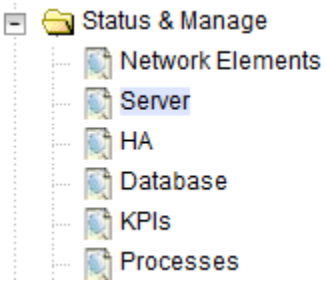
2. Click Edit.
Modifying HA attributes
 

3. Set the Max Allowed HA Role drop down box to OOS for the failed servers.
4. Click OK.
 
</td></tr>
<tr><td>3. ☐</td><td>Server in Question: Login</td><td>Establish an SSH session to the server in question. Login as admusr.</td></tr>
<tr><td>4.</td><td>Server in Question: Stop httpd service</td><td>Stop the httpd service.
<code>$ sudo bash -l</code>
<code>$ service httpd stop</code></td></tr>
<tr><td>5. ☐</td><td>Server in Question: Take server out of service</td><td>Take the server out of service.
<code>$ prod.clobber</code></td></tr>
<tr><td>6. ☐</td><td>Server in Question: Take server to DbUp state and start the application</td><td>Take the server to Dbup and start the DSR application.
<code>$ prod.start</code></td></tr>
</table>

Procedure 7. Recovery Scenario 6 (Case 2)

<table>
<tr>
<td>7.</td>
<td>Server in Question: Start httpd service</td>
<td>1. Start the httpd service.
<code>$ service httpd start</code>
2. Exit out of root.
<code>$ exit</code></td>
</tr>
<tr>
<td>8.
☐</td>
<td>NOAM VIP GUI: Set failed servers to active</td>
<td>1. Navigate to Status and Manage > HA.
 

2. Click Edit at the bottom of the screen.
3. Select the failed server and set it to Active.
 

4. Click OK.</td>
</tr>
<tr>
<td>9.
☐</td>
<td>NOAM VIP GUI: Restart DSR application</td>
<td>1. Navigate to Status and Manage > Server.
 

2. Select each recovered server and click Restart.
 
</td>
</tr>
</table>

Procedure 7. Recovery Scenario 6 (Case 2)

10. ☐	**Server in Question**: Verify the server state	1. Verify the processes are up and running:
		`$ sudo pm.getprocs`
		Example Output:
		`A 5139 cmha Up 12/21 13:16:25 1 cmha`
		`A 5140 cmplatalarm Up 12/21 13:16:25 1 cmplatalarm`
		`A 5143 cmsnmpsa Up 12/21 13:16:25 1 cmsnmpsa -R 1.3.6.1.4.1.323.5.3.28.1`
		`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]#`
		2. Verify if replication channels are up and running:
		`$ sudo irepstat`
		Example Output:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`BC From SOAM-2 Active 0 0.50 ^0.04%cpu 34B/s A=C2713.145`
		`CC From MP-2 Active 0 0.20 ^0.05 1.57%cpu 35B/s A=C2713.145`
		`-- Policy 1001 DSR_SLDB_Policy [] ----------`
		`1 CC From MP-2 Active 0 0.20 ^0.06 1.51%cpu 35B/s A=C2713.145`
		3. Verify if merging channels are up and running:
		`$ sudo inetmstat`
		Example Output:
		`nodeId InetMerge State dir dSeq dTime updTime info`
		`SOAM-1 Standby To 0 0.00 13:19:33`
		`SOAM-2 Active To 0 0.00 13:19:33`
		`~`
		`~`

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

5. Resolving User Credential Issues after Database Restore

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

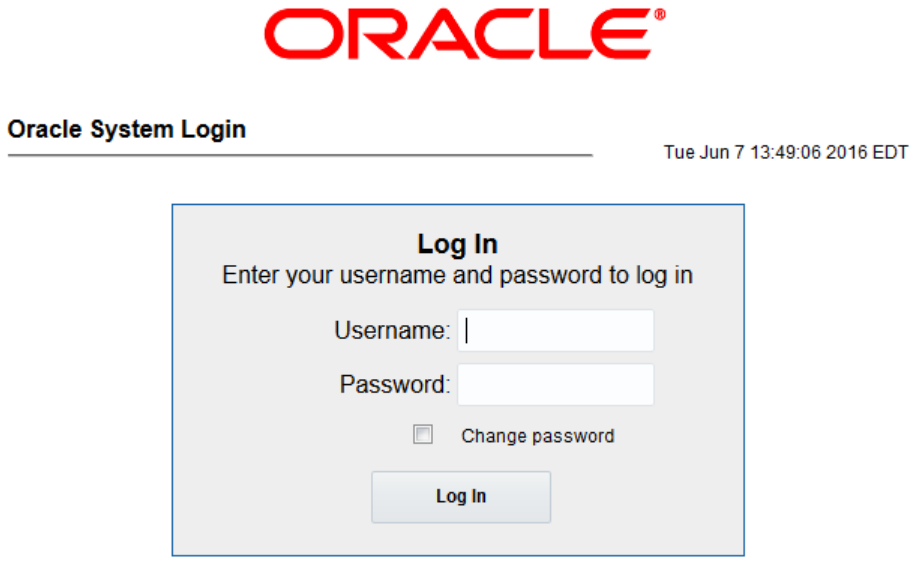
5.1 Restore a Deleted User

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

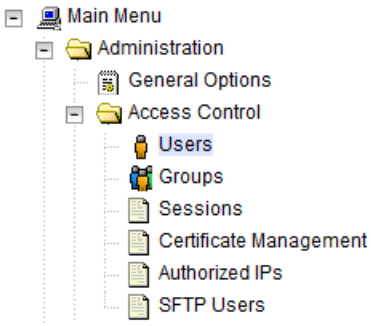
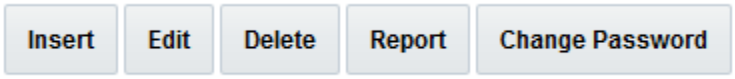
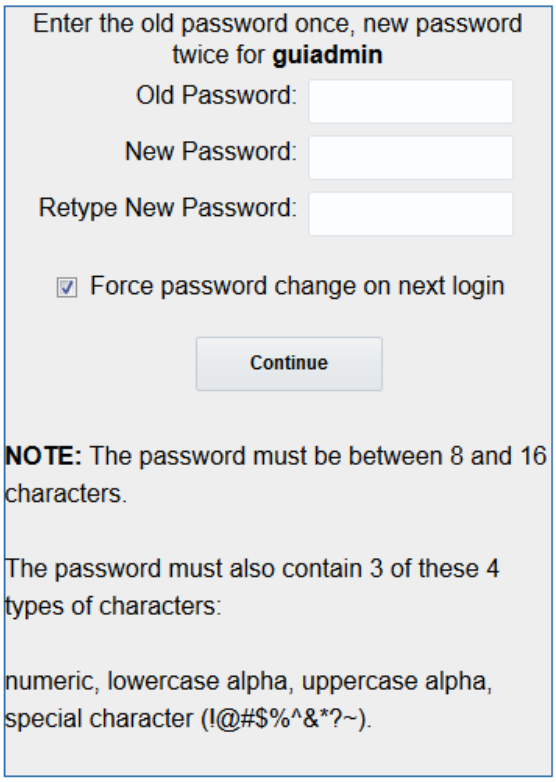
These users were removed before creation of the backup and archive file. They are reintroduced by system restoration of that file.

5.2 Keep a Restored User

Procedure 8. Keep Restored User

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 IP 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

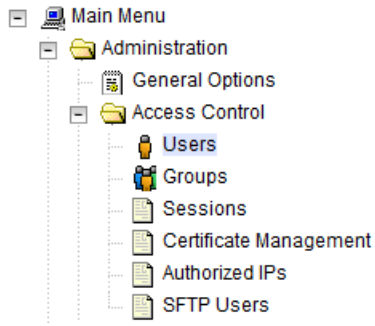
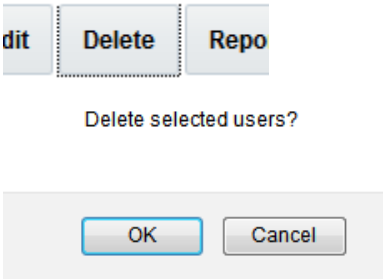
3. ☐	**After Restoration**: Reset user passwords	1. Navigate to **Administration > Access Control > Users**.  2. Select the user. 3. Click **Change Password**.  4. Type a new password.  5. Click **Continue**.

5.3 Remove a Restored User

Procedure 9. Remove the Restored User

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 IP 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.

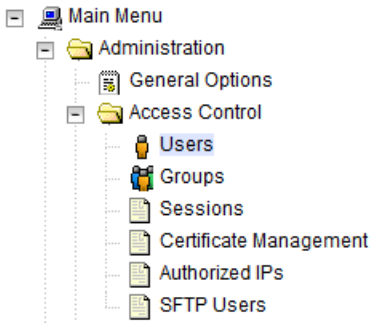
```
- User 'testuser' exists in current database but not in the selected backup
file.
```

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

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 IP 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: 

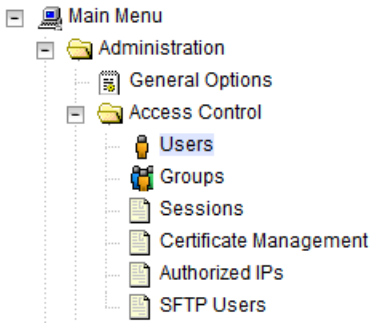
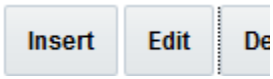
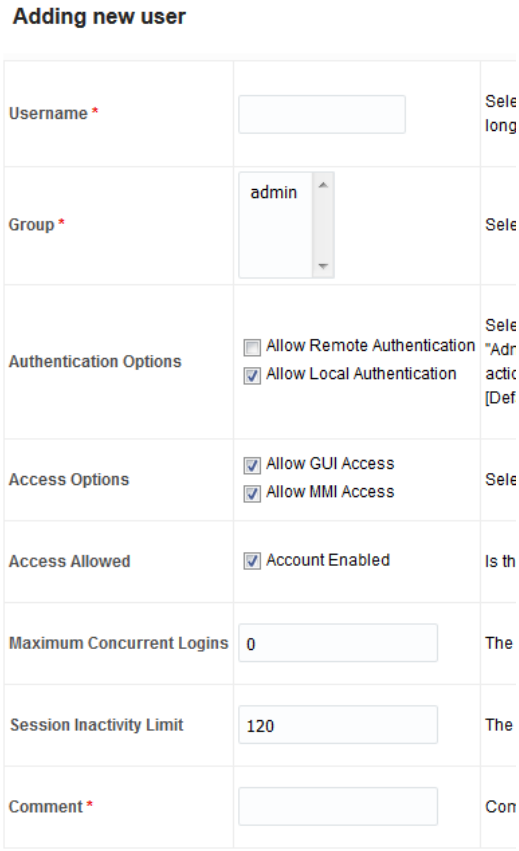
Procedure 10. Restore an Archive That Does Not Contain a Current User

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 IP 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**.
6. ☐	**After Restoration**: Repeat for additional users	Repeat step 5 to recreate additional users.

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

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

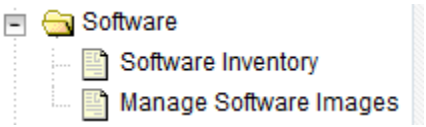
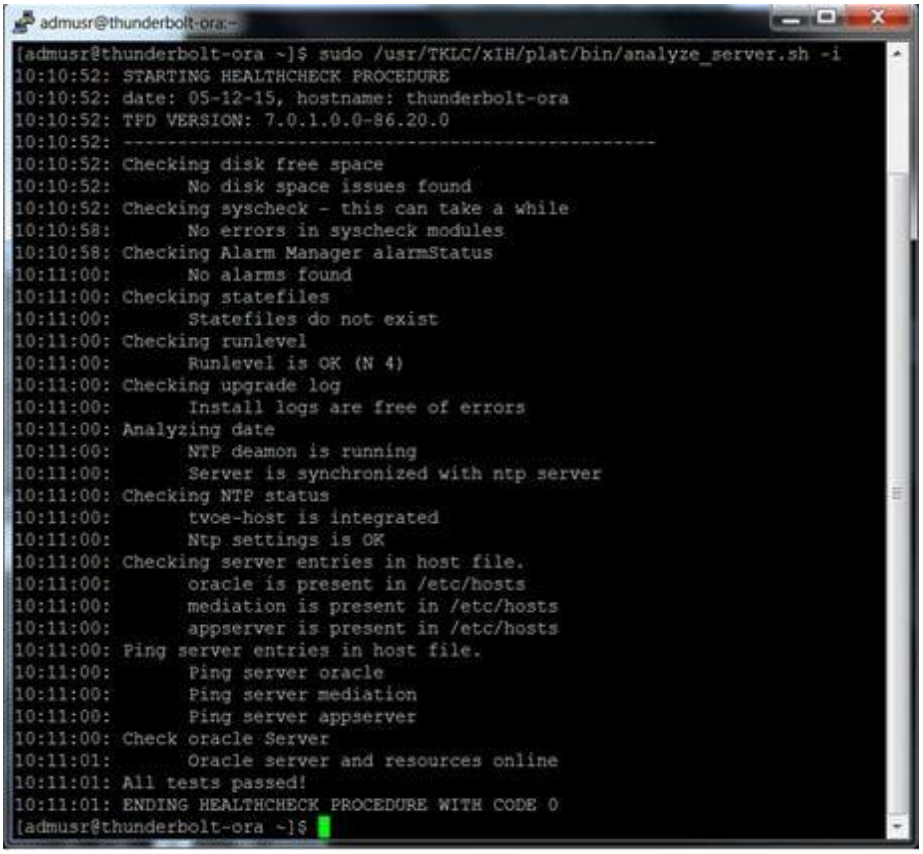
This procedure performs disaster recovery preparation steps for the IDIH.

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

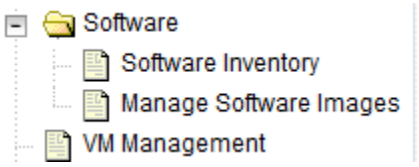
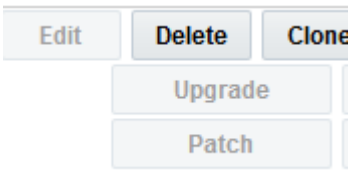
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**PMAC GUI**: Login	1. Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` 2. Login as **pmacadmin** user: 

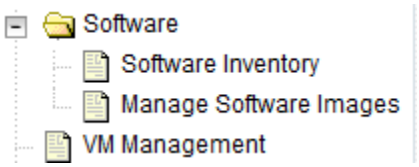
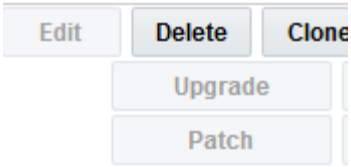
Procedure 11. IDIH Disaster Recovery Preparation

2. ☐	**PMAC GUI**: Verify necessary IDIH images are available	1. Navigate to **Software > Manage Software Images**.  2. Verify the current IDIH TVOE, TPD, Oracle, Application and Mediation images are listed. ***Note***: If the necessary software images are not available, follow the instructions from **Load Application and TPD ISO onto PMAC Server** and steps 1-4 of **IDIH Configuration** from [8] to acquire and transfer the images.
3. ☐	**Oracle Guest**: Login	Establish an SSH session to the Oracle guest, login as **admusr**.
4. ☐	**Oracle Guest**: Perform database health check	Perform a database health check: `$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i` Output: 

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

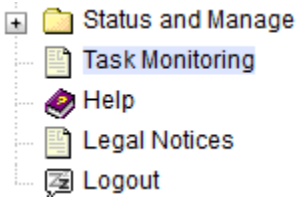
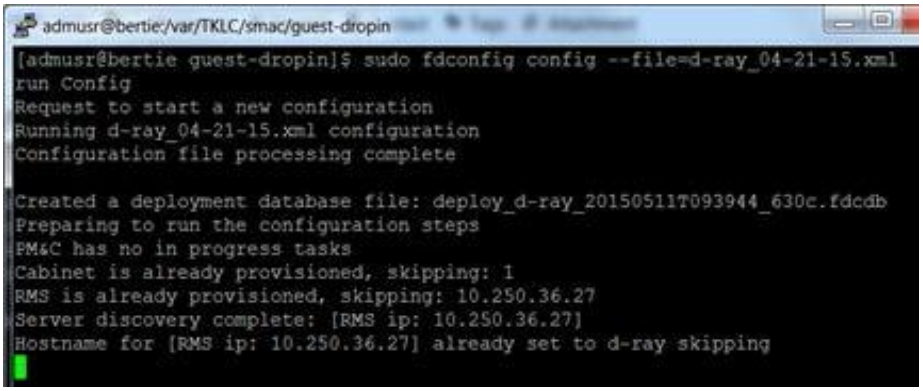
This procedure performs disaster recovery for the IDIH by re-installing the mediation and application servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**: Login	1. Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` 2. Login as **pmacadmin** user: 
2. ☐	Remove existing application server	1. Navigate to **Main Menu > VM Management**.  2. Select the application guest. 3. Click **Delete**. 

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

3. ☐	Remove existing mediation server	1. Navigate to **Main Menu > VM Management**.  2. Select the Mediation guest. 3. Click **Delete**. 
4. ☐	**PMAC**: Establish SSH session and login	Establish an SSH session to the PMAC, login as **admusr**.

5. ☐	**PMAC**: Re-install the mediation and application servers	Execute this command (Enter your upgrade file):
		`$ cd /var/TKLC/smac/guest-dropin`
		`$ screen`
		`$ sudo fdconfig config --file=<hostname-upgrade_xx-xx-xx>.xml`
		 
		!!Warning!!
		If you run the fdconfig without “upgrade” in the XML filename, the database is destroyed and you lose all of the existing data.
		Note: This is a long duration command (45-90 Minutes). If the screen command was run before executing the fdconfig, perform a **screen -dr** to resume the screen session in the event of a terminal timeout etc.

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

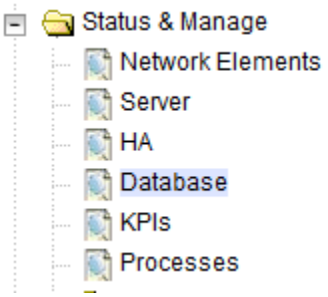
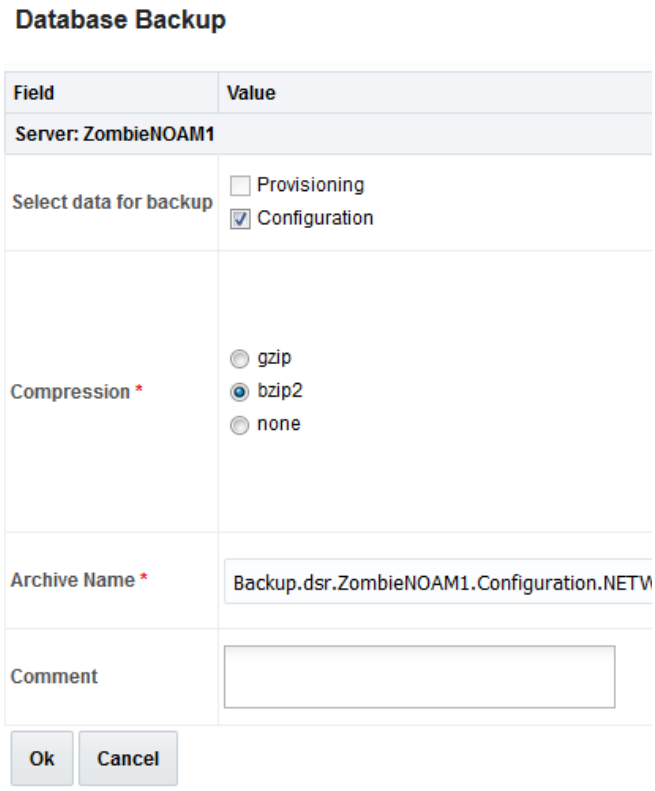
6. ☐	**PMAC GUI**: Monitor the configuration	1. If not already done so, establish a GUI session on the PMAC server. 2. Navigate to **Status and Manage > Task Monitoring**.  3. Monitor the IDIH configuration to completion. Alternatively, you can monitor the fdconfig status through the command line after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

Appendix A. DSR Database Backup

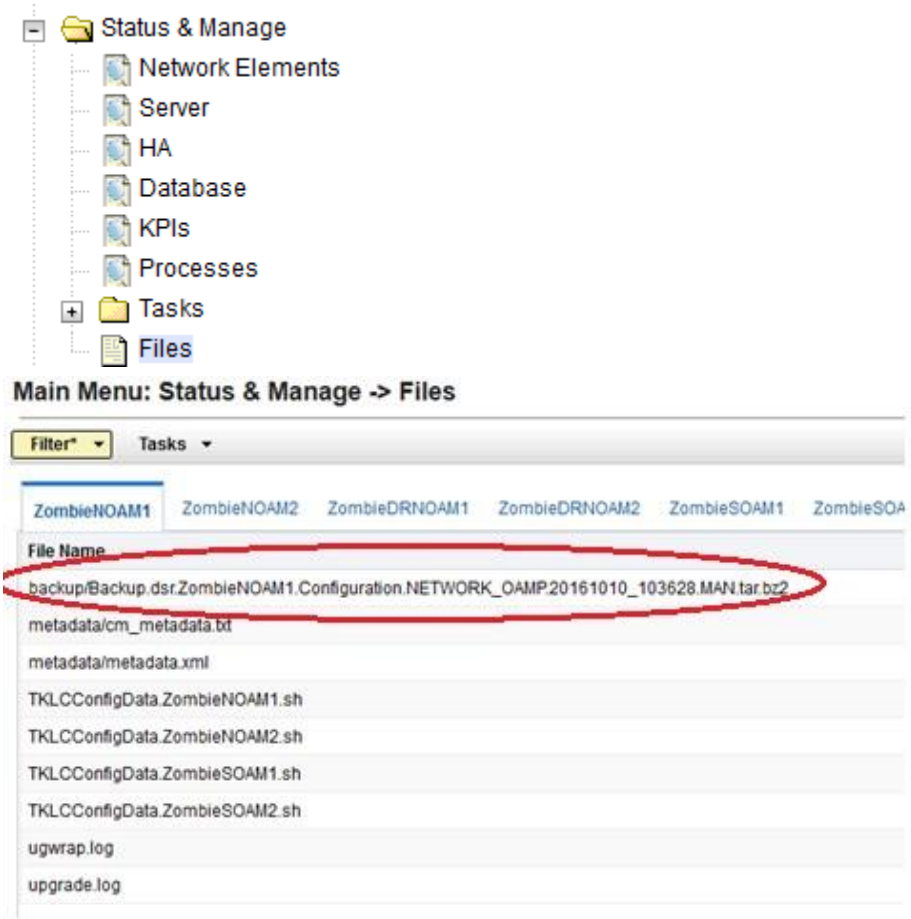
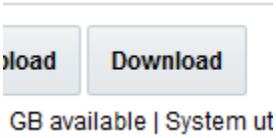
Procedure 13. DSR Database Backup

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 IP 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 13. DSR Database Backup

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

Procedure 13. DSR Database Backup

3. ☐	**NOAM/SOAM VIP**: Verify the backup file existence	1. Navigate to **Status and Manage > Files**.  2. Select the active NOAM or SOAM tab. 3. The files on this server display. Verify the existence of the backup file.
4. ☐	**NOAM/SOAM VIP**: Download the file to a local machine	1. From the previous step, select the backup file. 2. Click **Download**.  3. Click **OK** to confirm the download.
5. ☐	Upload the image to secure location	Transfer the backed up image saved in the previous step to a secure location where the server backup files are located in case of system disaster recovery.
6. ☐	Backup active SOAM	Repeat Steps 2 through 5 to back up the active SOAM.

Appendix B. Recover/Replace Failed 3rd Party Components (Switches, OAs)

The following procedures provide steps to recover 3rd party devices (switches, OAs). Follow the appropriate procedure as needed for your disaster recovery.

Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F)

The intent of this procedure is to recover a failed Aggregation (4948E/4948E-F) Switch. Prerequisites for this procedure are: • A copy of the networking xml configuration files • A copy of HP Misc Firmware DVD or ISO • IP address and hostname of the failed switch • Rack Mount position of the failed switch Refer to Appendix M for the workaround on cipher mismatch issue with Cisco switches. 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. ☐	**Recover failed Aggregation Switches**: Cisco 4948E/4948E-F	Log into the PMAC using SSH as **admusr**.
		Remove the old SSH key of the switch from the PMAC by executing this command from a PMAC command shell:
		`sudo ssh-keygen -R <4948_switch_ip>`
		Refer to procedure **Replace a failed 4948/4948E/4948E-F switch (c-Class system) (netConfig)** to replace a failed Aggregation switch from reference [2].
		Note: You need a copy of the HP Misc Firmware DVD or ISO (or firmware file obtained from the appropriate hardware vendor) and the original networking XML files custom for this installation. These are either stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.
		Note: Copy switch appropriate init file and use it for respective switch:
		Copy the switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy 'switch1A_4948_4948E_init.xml'.
		The templates can be found using the following method:
		1. From the PMAC CLI
		`df | grep –I DSR`
		Sample output:
		`/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso`
		`1118514 1118514 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64`
		`/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso`
		`1118372 1118372 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64`
		`/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso`
		`1117976 1117976 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64`
		2. From the output of step 1, determine the applicable directory of the DSR release being recovered.

Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F)

		3. cd usr/TKLC/smac/html/TPD/<DSR Release dir>/upgrade/overlay/
		Example:
		`cd /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64/upgrade/overlay/`
		4. Locate the **DSR_NetConfig_Templates.zip** file.
		Example:
		`$ ll`
		`total 286`
		`-r--r--r-- 1 root root 611 Feb 21 19:18 change_ilo_admin_passwd.xml`
		`-r--r--r-- 1 root root 107086 Feb 21 19:18 DSR_NetConfig_Templates.zip`
		`-r--r--r-- 1 root root 11642 Feb 21 19:18 DSR_NOAM_FD_Blade.xml`
		`-r--r--r-- 1 root root 13346 Feb 21 19:18 DSR_NOAM_FD_RMS.xml`
		`dr-xr-xr-x 2 root root 2048 Feb 21 19:18 RMS`
		`-r--r--r-- 1 root root 812 Feb 21 19:18 SAMPLE-NetworkElement.xml`
		`-r--r--r-- 1 root root 2309 Feb 21 19:20 TRANS.TBL`
		`-r-xr-xr-x 1 root root 2186 Feb 21 19:18 TVOEcfg.sh`
		`-r-xr-xr-x 1 root root 598 Feb 21 19:18 TVOEclean.sh`
		`-r--r--r-- 1 root root 128703 Feb 21 19:18 UpgradeHCplugin.php-ovl`
		`-r--r--r-- 1 root root 19658 Feb 21 19:18 upgradeHealthCheck-ovl`
		5. Unzip the **DSR_NetConfig_Templates.zip** file and retrieve the required switch init file.
		Example:
		`$ unzip DSR_NetConfig_Templates.zip`
		6. Edit the desired file with site specific details. The existing file from original deployment **/usr/TKLC/smac/etc/switch/xml** can be used as a reference.
		7. Copy the new init file to the **/usr/TKLC/smac/etc/switch/xml** dir.
		Example:
		`$ cp <switch_xml_file> /usr/TKLC/smac/etc/switch/xml/`

Procedure 15. Recover a Failed Enclosure Switch (Cisco 3020)

The intent of this procedure is to recover a failed Enclosure (3020) Switch.

Prerequisites for this procedure are:

- A copy of the networking xml configuration files
- A copy of HP Misc. Firmware DVD or ISO
- IP address and hostname of the failed switch
- Interconnect Bay position of the enclosure switch

Refer to Appendix M for the workaround on cipher mismatch issue with Cisco switches.

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. ☐	**Recover Failed Enclosure Switch**: Cisco 3020	1. Log into the PMAC using SSH as **admusr**. 2. Remove the old SSH key of the switch from the PMAC by executing this command from a PMAC command shell: `sudo ssh-keygen -R <enclosure_switch_ip>` 3. Refer to procedure **Replace a failed 3020 switch (netConfig)** to replace the failed enclosure switch from reference [2]**.** ***Note***: You need a copy of the HP Misc Firmware DVD or ISO and of the original networking xml files custom for this installation. These either be stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.

Procedure 16. Recover a Failed Enclosure Switch (HP 6120XG , HP 6125XLG, HP 6125G)

The intent of this procedure is to recover a failed Enclosure (6120XG/6125XLG/6125G) Switch.

Prerequisites for this procedure are:

- A copy of the networking xml configuration files

Refer to Appendix M for the workaround on cipher mismatch issue with Cisco switches.

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. ☐	**Recover Failed Enclosure Switch**: HP 6120XG/6125XLG/6125G	1. Log into the PMAC using SSH as **admusr**. 2. Remove the old SSH key of the switch from the PMAC by executing this command from a PMAC command shell: `sudo ssh-keygen -R <enclosure_switch_ip>` 3. Refer to procedure **Replace a failed HP (6120XG, 6125G, 6125XLG switch (netConfig)** to replace the failed enclosure switch from reference [2] ***Note***: You need a copy of the HP Misc Firmware DVD or ISO and of the original networking xml files custom for this installation. These are either stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.

Procedure 16. Recover a Failed Enclosure Switch (HP 6120XG , HP 6125XLG, HP 6125G)

Note: Copy switch appropriate init file and use it for respective switch:

4. Copy the switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy 'switch1A_4948_4948E_init.xml'.

The templates can be found by the following method:

a. From the PMAC CLI:

```
df | grep –I DSR
```

Sample output:

```
/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-
x86_64.iso
1118514   1118514          0 100%
/usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64
/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-
x86_64.iso
1118372   1118372          0 100%
/usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64
/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-
x86_64.iso
1117976   1117976          0 100%
/usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64
```

b. From the output of step 1, determine the applicable directory of the DSR release being recovered.

c. `cd usr/TKLC/smac/html/TPD/<DSR Release dir>/upgrade/overlay/`

Example:

```
cd /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-
x86_64/upgrade/overlay/
```

d. Locate the DSR_NetConfig_Templates.zip file.

Example:

```
$ ll
total 286
-r--r--r-- 1 root root    611 Feb 21 19:18 change_ilo_admin_passwd.xml
-r--r--r-- 1 root root 107086 Feb 21 19:18 DSR_NetConfig_Templates.zip
-r--r--r-- 1 root root  11642 Feb 21 19:18 DSR_NOAM_FD_Blade.xml
-r--r--r-- 1 root root  13346 Feb 21 19:18 DSR_NOAM_FD_RMS.xml
dr-xr-xr-x 2 root root   2048 Feb 21 19:18 RMS
-r--r--r-- 1 root root    812 Feb 21 19:18 SAMPLE-NetworkElement.xml
-r--r--r-- 1 root root   2309 Feb 21 19:20 TRANS.TBL
-r-xr-xr-x 1 root root   2186 Feb 21 19:18 TVOEcfg.sh
-r-xr-xr-x 1 root root    598 Feb 21 19:18 TVOEclean.sh
-r--r--r-- 1 root root 128703 Feb 21 19:18 UpgradeHCplugin.php-ovl
-r--r--r-- 1 root root  19658 Feb 21 19:18 upgradeHealthCheck-ovl
```

e. Unzip the **DSR_NetConfig_Templates.zip** file and retrieve the required switch init file.

Example:

```
$ unzip DSR_NetConfig_Templates.zip
```

Procedure 16. Recover a Failed Enclosure Switch (HP 6120XG , HP 6125XLG, HP 6125G)

		f. Edit the desired file with site specific details. The existing file from original deployment **/usr/TKLC/smac/etc/switch/xml** can be used as a reference.
		g. Copy the new init file to the **/usr/TKLC/smac/etc/switch/xml** dir.
		Example:
		`$ cp <switch_xml_file> /usr/TKLC/smac/etc/switch/xml/`
		Note: **While restoring 6120XG switch**, some features enabled on a 6120XG may not restore properly if they reference a port channel that does not currently exist on the switch ahead of the restore operation. Identify any port channels that need to be created on the switch according to the backup file and create them before restoring the configuration:
		`$ sudo /bin/cat <switch_hostname>-backup | /bin/grep "^trunk"`
		Example output:
		`trunk <int list> Trk<id> LACP`
		`trunk <int list> Trk<id> Trunk`
		5. If any port-channels are found, then for each portchannel identified by the above command, use the **netConfig setLinkAggregation** command to create it and the **netConfig showConfiguration** command to verify its configuration:
		6. If an LACP port channel was found, add the port-channel with this command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY2 setLinkAggregation id=<id> addPort=tenGE<int list> mode=active`
		7. If a Trunk port-channel was found (as labeled after the **Trk<id>**), add the port-channel with this command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY2 setLinkAggregation id=<id> addPort=tenGE<int list> mode=static`
		Verify the port-channels were added to the running configuration:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY2 showConfiguration | grep "^trunk"`
		`trunk <int list> Trk<id> LACP`
		`trunk <int list> Trk<id> Trunk`
		8. For all switch types and configurations found, use netConfig to restore the configuration:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> restoreConfiguration service=ssh_service filename=<switch_hostname>-backup`
		Note: This causes the switch to reboot. It takes approximately 120-180 seconds before connectivity is restored.

	Note: For information about Downgrade Firmware on a 6125 Switch, see [10] DSR C-Class Hardware and Software Installation Procedure 1/2.	

Procedure 17. Recover a Failed Enclosure OA

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

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

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

The intent of this procedure is to inhibit A and B level replication on all C-level servers of this site. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, 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 18. 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 19. Un-Inhibit A and B Level Replication on C-level Servers

The intent of this procedure is to Un-inhibit A and B level replication on all C-level servers of this site Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, 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 19. Un-Inhibit A and B Level Replication on C-level Servers

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. 

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`

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

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

The intent of this procedure is to inhibit A and B level replication on all C-level servers of this site when active, standby, and spare SOAMS are lost Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, 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 the script from **/usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh**, if available.
		If the **/usr/TKLC/dsr/tools/** path does not have the **InhibitReplicationToCLevel.sh** script, then use this manual command.
		`/usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh --replication=inhibit --SO_SG_Name=<SOAM server group name>`
		Alternatively to the above script, if the script is not in the specific path:
		`$ for i in $(sudo Imysql.client -B -N -e "`
		`SELECT DISTINCT CS.hostname`
		`FROM appworks.Server CS, appworks.Server PS, appworks.Server2SG C2SG, appworks.Server2SG P2SG, appworks.ServerGroup CSG, appworks.ServerGroup PSG, comcol.ClusterInfo CCI, comcol.ClusterInfo PCI, comcol.ClusterGroupInfo`
		`WHERE CS._h_Server_ID = C2SG._h_Server_ID`
		`AND C2SG._h_SG_ID = CSG._h_SG_ID`
		`AND CSG.clusterId = CCI.clusterId`
		`AND CCI.groups = comcol.ClusterGroupInfo.groupId`
		`AND comcol.ClusterGroupInfo.parentGroup = PCI.groups`
		`AND PCI.clusterId = PSG.clusterId`
		`AND PSG.ServerGroupName='<SOAM_SG_NAME>'`
		`"); do iset -finhibitRepPlans='A B' NodeInfo where "nodeName='$i'"; done`
		Note: SOAM_SG_NAME is the name of the server group found by logging into the active NOAM GUI and navigating to **Configuration > Server Groups**.
		For example, if SOAM1 belongs to the site being recovered, then the server group is SO_SG.
		 	

Procedure 20. 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 F. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost)

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

The intent of this procedure is to Un-inhibit A and B level replication on all C-level servers of this site when active, standby and spare SOAMS are lost. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, 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 21. Un-Inhibit A and B Level Replication on C-Level Servers

2. ☐	**Active NOAM**: Un-Inhibit replication on all C-level servers	Execute the script from **/usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh** if available.
		If the **/usr/TKLC/dsr/tools/** path does not have the **InhibitReplicationToCLevel.sh** script, then use this manual command.
		`/usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh --replication=allow --SO_SG_Name=<SOAM server group name>`
		Alternatively to the above script, if the script is not in the specific path:
		`$ for i in $(sudo Imysql.client -B -N -e "`
		`SELECT DISTINCT CS.hostname`
		`FROM appworks.Server CS, appworks.Server PS, appworks.Server2SG C2SG, appworks.Server2SG P2SG, appworks.ServerGroup CSG, appworks.ServerGroup PSG, comcol.ClusterInfo CCI, comcol.ClusterInfo PCI, comcol.ClusterGroupInfo`
		`WHERE CS._h_Server_ID = C2SG._h_Server_ID`
		`AND C2SG._h_SG_ID = CSG._h_SG_ID`
		`AND CSG.clusterId = CCI.clusterId`
		`AND CCI.groups = comcol.ClusterGroupInfo.groupId`
		`AND comcol.ClusterGroupInfo.parentGroup = PCI.groups`
		`AND PCI.clusterId = PSG.clusterId`
		`AND PSG.ServerGroupName='<SOAM_SG_NAME>'`
		`"); do iset -finhibitRepPlans='' NodeInfo where "nodeName='$i'"; done`
		Note: SOAM_SG_NAME is the name of the server group found by logging into the active NOAM GUI and navigating to **Configuration > Server Groups**.
		For example, if SOAM1 belongs to the site being recovered, then the server group is SO_SG.
		 

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

3. ☐	**Active NOAM**: Verify replication has been Un-Inhibited	After executing above steps to un-inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.
		Verification of replication inhibition on MPs can be done by analyzing NodeInfo output. Un-InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO_SG is set as <**blank>**.
		Execute this command:
		`$ sudo iqt NodeInfo`
		Output:
		`nodeId nodeName hostName nodeCapability inhibitRepPlans siteId excludeTables`
		`A1386.099 NO1 NO1 Active NO_HPC03`
		`B1754.109 SO1 SO1 Active SO_HPC03`
		`C2254.131 MP2 MP2 Active SO_HPC03`
		`C2254.233 MP1 MP1 Active SO_HPC03`

Appendix G. Restore TVOE Configuration from Backup Media

Procedure 22. Restore TVOE Configuration from Backup Media

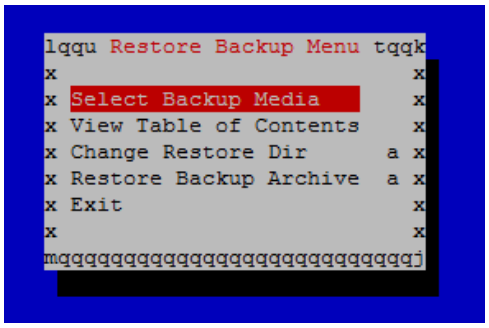
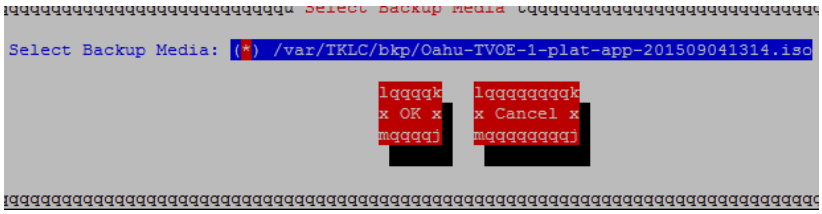
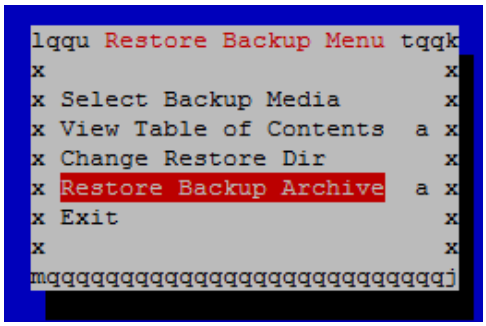
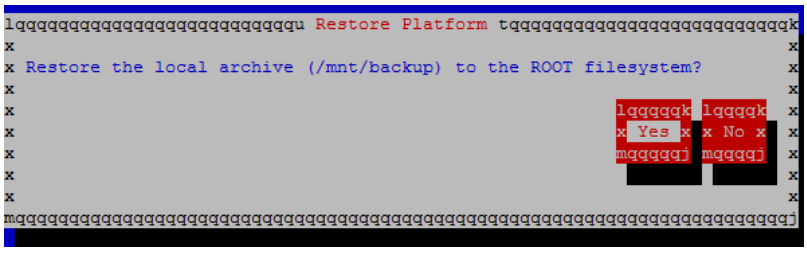
This procedure provides steps to restore the TVOE application configuration from backup media. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Install TVOE application	• If the PMAC is **NOT** hosted on the failed rack mount server, execute **IPM Servers Using PMAC Application** from reference [10]. • If the PMAC is hosted on the failed rack mount server, execute **Installing TVOE on the Management Server** from reference [10].
2. ☐	Establish network connectivity	• If the PMAC is **NOT** hosted on the failed rack mount server, **skip this step**. • If the PMAC is hosted on the failed rack mount server, execute **TVOE Network Configuration**, steps 1-11, from reference [10]. ***Note***: The IP address configured on the TVOE must be one accessible through the network of the machine currently holding the TVOE Backup ISO image. This could be a NetBackup master server, a customer PC, etc.
3. ☐	Restore TVOE backup ISO image to the TVOE host (NetBackup)	If using NetBackup to restore the TVOE backup ISO image, then execute this step; otherwise, skip this step. 1. Execute **Application NetBackup Client Installation Procedures** from reference [8]. 2. Interface with the NetBackup master server and initiate a restore of the TVOE backup ISO image. ***Note***: Once restored, the ISO image is in **/var/TKLC/bkp/** on the TVOE server.

Procedure 22. Restore TVOE Configuration from Backup Media

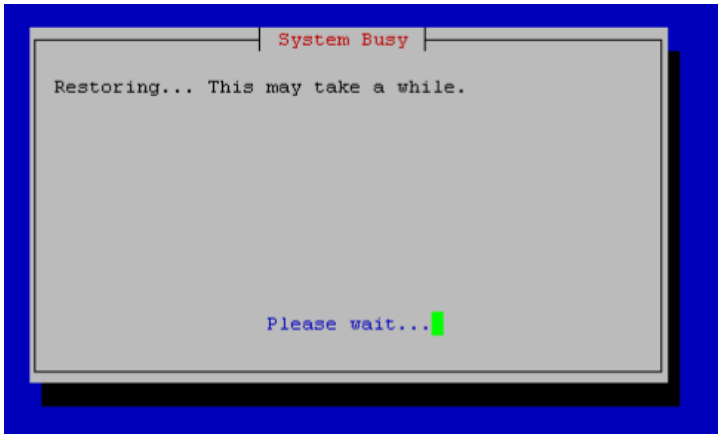
4. ☐	Transfer TVOE backup ISO image to the TVOE host	Restore TVOE backup ISO using SCP.
		Using the IP of the TVOE host, transfer the backup ISO image to the TVOE.
		Linux:
		From the command line of a Linux machine use this command to copy the backup ISO image to the TVOE host:
		`# scp <path_to_image> tvoexfer@<TVOE_IP>:backup/`
		where `<path_to_image>` is the path to the backup ISO image on the local system and `<TVOE_IP>` is the TVOE IP address.
		Note: If the IP is an IPv4 address, then `<TVOE_IP>` is a normal dot-decimal notation (for example, 10.240.6.170).
		Note: If the IP is an IPv6 link local address, then `<TVOE_IP>` needs to be scoped. For example, **[fe80::21e:bff:fe76:5e1c%control]** where control is the name of the interface on the machine initiating the transfer and it must be on the same link as the interface on the TVOE host.
		Note: The control IP address of the TVOE can be used if the TVOE is NOT hosting the PMAC. This method requires first transferring the backup file to the PMAC, and then to the TVOE host.
		IPv4 Example:
		`# scp /path/to/image.iso tvoexfer@10.240.6.170:backup/`
		IPv6 Example:
		`# scp /path/to/image.iso`
		`tvoexfer@[fe80::21e:bff:fe76:5e1c%control]:backup/`
		Windows:
		Use WinSCP to copy the Backup ISO image into the /var/TKLC/bkp directory. Please refer to [10] procedure Using WinSCP to copy the backup image to the customer system.

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

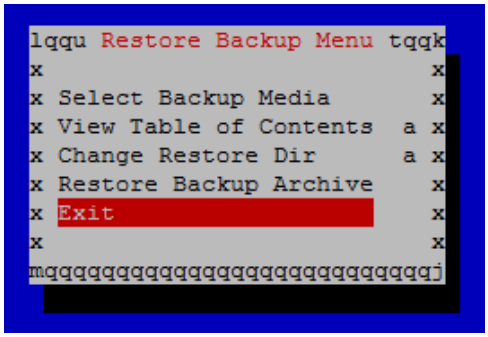
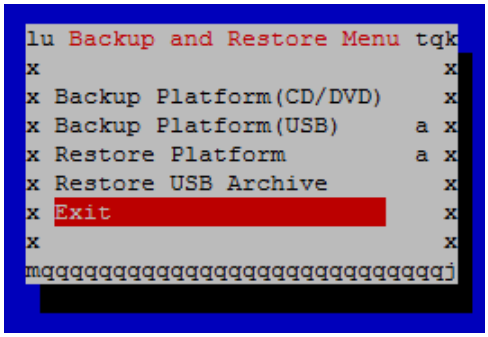
Procedure 22. Restore TVOE Configuration from Backup Media

6. ☐	Restore TVOE backup ISO image	1. Restore the TVOE backup ISO by executing this command: `$ sudo su - platcfg` 2. Navigate to **Maintenance > Backup and Restore > Restore Platform > Select Backup Media**.  3. Select the desired archive.  4. Click **OK**. 5. Click **Restore Backup Archive**.  6. Confirm restore. 

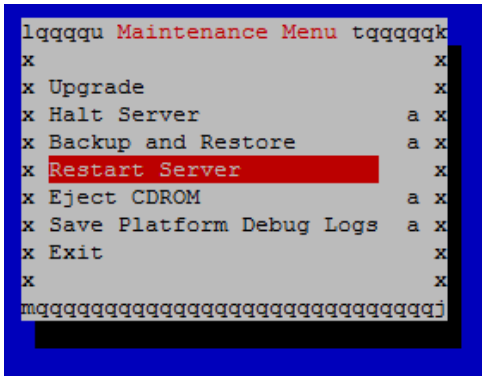
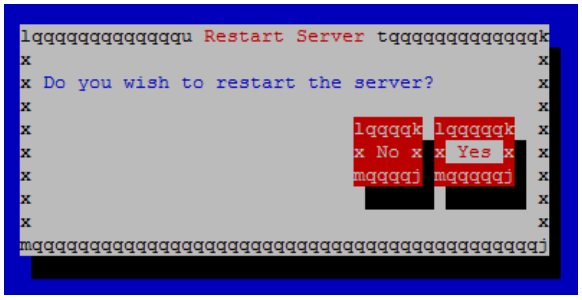
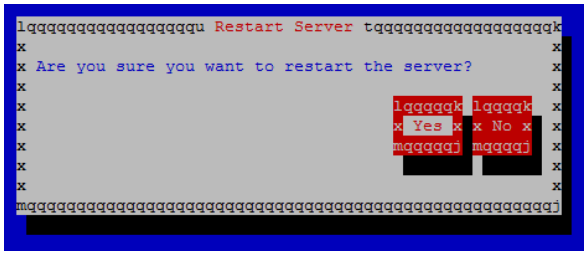
Procedure 22. Restore TVOE Configuration from Backup Media

7. ☐	Monitor TVOE backup process	1. Wait for the restore to complete.  ***Note***: This typically takes less than 5 minutes. 2. Restore complete.  3. **Exit** platcfg.

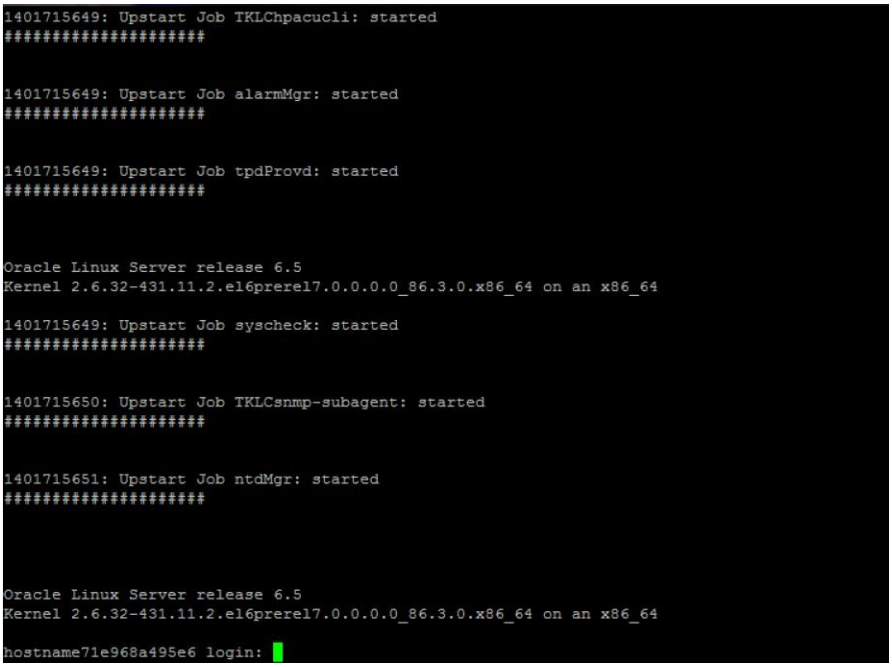
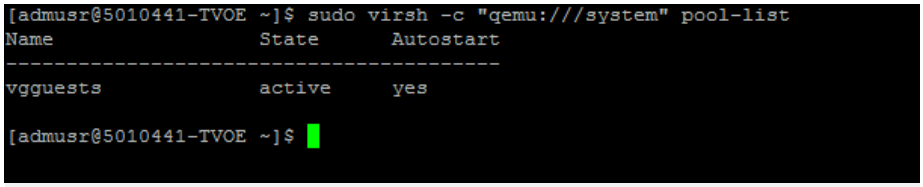
Procedure 22. Restore TVOE Configuration from Backup Media

8. ☐	**TVOE Server**: Exit restore backup menu	Exit the Restore Backup Menu.  

Procedure 22. Restore TVOE Configuration from Backup Media

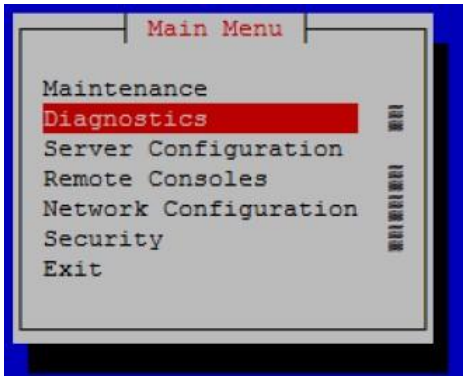
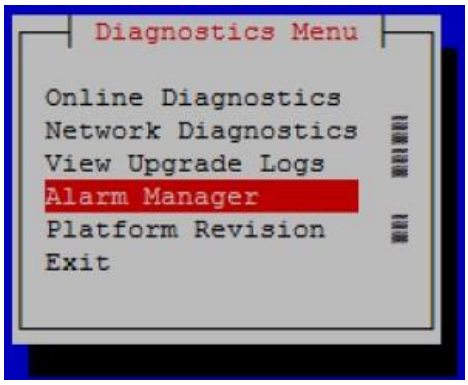
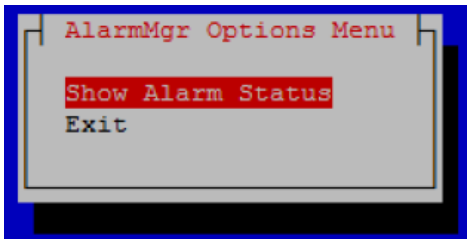
9. ☐	**TVOE Server**: Restart	1. Restart the TVOE server.  2. Click **Yes** to restart.  3. Confirm restart. 

Procedure 22. Restore TVOE Configuration from Backup Media

10. ☐	**TVOE Server**: Wait for restart to successfully complete	
11. ☐	**TVOE Server**: Verify storage pools are active	1. Login as **admusr**. 2. Verify all storage pools are listed and are in the active state: `$ sudo virsh -c "qemu:///system" pool-list`  ***Note***: If any storage pools are missing or inactive, contact My Oracle Support (MOS).

12. ☐	**TVOE Server**: Enable HIDS (Optional)	***Note***: Enabling HIDS is optional. This step is skipped if HIDS is not required to be enabled.
		When enabling HIDS, update the baseline so the restored files are not reported as being tampered with. Execute these commands from the TVOE host remote console to enable HIDS and update the baseline:
		`$ /usr/TKLC/plat/bin/hidsMgr –initialize`
		`LOG: HIDS monitoring has been Initialized`
		`HIDS baseline has been initialized`
		`$ /usr/TKLC/plat/bin/hidsMgr --enable`
		`HIDS monitoring has successfully been enabled`
		New State: ENABLED
		`$ /usr/TKLC/plat/bin/hidsMgr --update --all`
		`HIDS baseline has successfully been updated`

Procedure 22. Restore TVOE Configuration from Backup Media

13. ☐	**TVOE Server**: Verify alarms	1. Verify alarms: `$ sudo su - platcfg` 2. Click **Diagnostics**.  3. Click **Alarm Manager**.  4. Click **Show Alarm Status**.  If there are any failures, contact My Oracle Support (MOS).

Appendix H. Restore PMAC from Backup

Procedure 23. Restore PMAC from Backup Media

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

Prerequisite: TVOE management server has been restored.

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

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

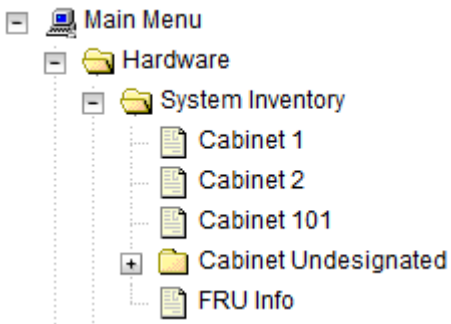
1.	Deploy the PMAC guest	Execute **Install PMAC** from reference [10].
2. □	**PMAC**: Login	Establish an SSH session to the PMAC server, login as **admusr**.

3.	Restore PMAC Backup image to the PMAC host	From the remote backup location, copy the backup file to the deployed PMAC. There are too many possible backup scenarios to cover them all here.
		This example is a simple scp from a redundant PMAC backup location. If using IPv6 addresses, the command requires shell escapes, for example, admusr@[<ipV6addr>]:/<file>
		Note: Execute the scp command from the recovered PMAC and the backup file is pulled/retried from the backup location.
		`$ sudo /usr/bin/scp -p \`
		`admsur@<remoteserver>:/var/TKLC/smac/backup/*.pef \`
		`/var/TKLC/smac/backup/`
		Note: It is important to copy the correct backup file to use in the restore. The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PMAC before the restoration of the data.

4.	**PMAC**: Verify no Alarms are present	Verify no alarms are present. `$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus`

5.	Restore the PMAC Data from Backup	Restore the PMAC data from backup.
		`$ sudo /usr/TKLC/smac/bin/pmacadm restore`
		`PM&C Restore been successfully initiated as task ID 1`
		Check the status of the background task.
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		Note: The result eventually displays PMAC Restore successful.

Procedure 23. Restore PMAC from Backup Media

6. ☐	**PMAC GUI**: Login	1. Open web browser and navigate to the PMAC GUI. 2. Login as **PMACadmin** user: `https://<pmac_network_ip>` 
7. ☐	**PMAC GUI**: Verify restore task completed	1. Navigate to **Task Monitoring**. 2. Verify the restore background task completed successfully. ***Note***: After the restore is complete, you should see **Add Enclosure** tasks start for all previously provisioning servers. These should be allowed to complete before continuing. ***Note***: After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior. ISO images are added in the next step.
8. ☐	**PMAC GUI**: Verify system inventory	1. Navigate to **Hardware > System Inventory**.  2. Verify previously provisioned enclosures are present.

Procedure 23. Restore PMAC from Backup Media

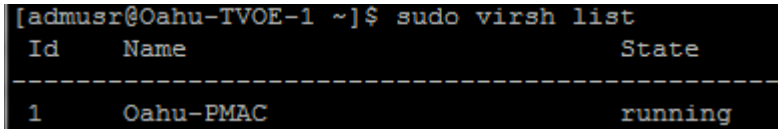
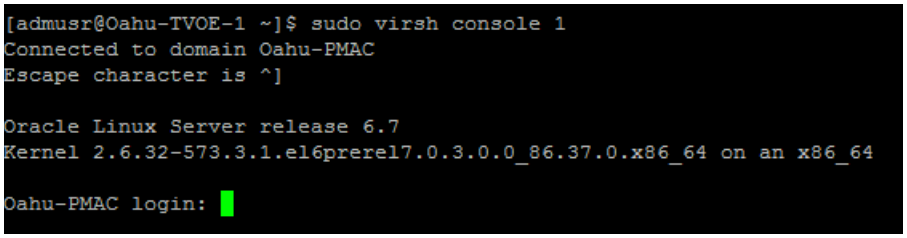
9. ☐	**PMAC**: Verify PMAC	Perform a system health check on the PMAC
		`$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus`
		This command should return no output on a healthy system.
		`$ sudo /usr/TKLC/smac/bin/sentry status`
		All processes should be running, displaying output similar to the following:
		`PM&C Sentry Status`
		`------------------`
		`sentryd started: Mon Jul 23 17:50:49 2012`
		`Current activity mode: ACTIVE`
		`Process PID Status StartTS NumR`
		`------------------ ------ ---------- ------------------`
		`smacTalk 9039 running Tue Jul 24 12:50:29 2012 2`
		`smacMon 9094 running Tue Jul 24 12:50:29 2012 2`
		`hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2`
		`snmpEventHandler 9176 running Tue Jul 24 12:50:29 2012 2`
		`Fri Aug 3 13:16:35 2012`
		`Command Complete.`

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

Procedure 24. Restore PMAC from Backup Server

This procedure provides steps to restore the PMAC application configuration from backup server. Prerequisite: TVOE management server has been restored. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Deploy the PMAC guest	Execute **Install PMAC** from reference [10]. ***Note***: This procedure is for restoring from a NetBackup server, so specify the appropriate options when deploying PMAC for use with NetBackup.
2. ☐	**PMAC TVOE Host**: Login	Establish an SSH session to the PMAC TVOE Host, login as **admusr**.

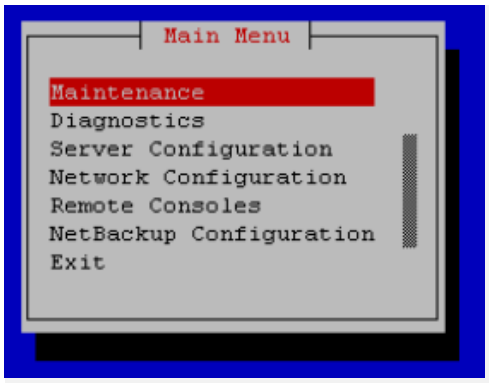
Procedure 24. Restore PMAC from Backup Server

3. ☐	**PMAC TVOE Host**: Log into PMAC guest console	1. On the TVOE host, execute this command: `$sudo virsh list` This produces a listing of currently running virtual machines.  2. Find the VM name for your PMAC and note its ID number in the first column.
4. ☐	Connect to console of the VM using the VM number obtained in Step 3	On the TVOE host, execute this command: `$sudo virsh console <PMAC-VMID>` Where PMAC-VMID is the VM ID you obtained in step 3:  You are now connected to the PMAC guest console. If you wish to return to the TVOE host, you can exit the session by pressing **CTRL +]**.

Procedure 24. Restore PMAC from Backup Server

5. ☐	**PMAC**: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus	Execute these commands on the PMAC.
		`$ sudo /sbin/service iptables stop`
		`iptables: Flushing firewall rules: [`
		`OK ]`
		`iptables: Setting chains to policy ACCEPT: filter [`
		`OK ]`
		`$ sudo /usr/TKLC/smac/etc/services/netbackup start`
		`Modified menu NBConfig`
		`--`
		`show`
		`Set the following menus: NBConfig to visible=1`
		`Modified menu NBInit`
		`--`
		`show`
		`Set the following menus: NBInit to visible=1`
		`Modified menu NBDeInit`
		`--`
		`show`
		`Set the`
		`following menus: NBDeInit to visible=1`
		`Modified menu NBInstall`
		`--`
		`show`
		`Set the following menus: NBInstall to visible=1`
		`Modified menu NBVerifyEnv`
		`--`
		`show`
		`Set the following menus: NBVerifyEnv to visible=1`
		`Modified menu NBVerify`
		`--`
		`show`
		`Set the following menus: NBVerify to visible=1=`

Procedure 24. Restore PMAC from Backup Server

6. ☐	**PMAC**: Verify the TPD platcfg backup menus are visible, then exit the TPD platcfg Utlility	Verify the TPD platcfg backup menus are visible. `$ sudo /bin/su - platcfg`  ***Note***: In the example image above of the TPD platcfg utility Main Menu the backup menu is identified as **NetBackup Configuration**.

7. ☐	**PMAC**: Verify the iptables rules are disabled on the PMAC guest	Verify the iptables rules are disabled on the PMAC guest.
		`$ sudo /sbin/iptables -nL`
		`INPUT (policy ACCEPT)`
		`target prot opt source destination`
		`Chain FORWARD (policy ACCEPT)`
		`target prot opt source destination`
		`Chain OUTPUT (policy ACCEPT)`
		`target prot opt source destination`

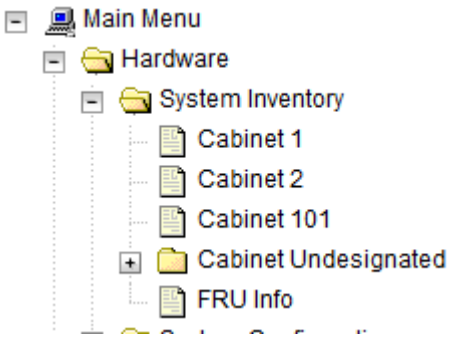
8. ☐	**PMAC**: Install backup utility client software on the PMAC guest	Execute **PMAC NetBackup Client Installation and Configuration** from reference [10] - Start at step 1. ***Note***: The **Initialize PMAC Application** and **Configure PMAC Application** prerequisites can be ignored.
9. ☐	Backup server: verify appropriate PMAC backup exists	This step is likely executed by customer IT personnel. 1. Log into the backup server as the appropriate user using the user password. 2. Execute the appropriate commands to verify the PMAC backup exists for the desired date. ***Note***: The actions and commands required to verify the PMAC backups exis t and the commands required to perform backup and restore on the backup server are the responsibility of the site customer. ***Note***: It is important to select the correct backup file to use in the restore. The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PMAC before the restoration of the data.

Procedure 24. Restore PMAC from Backup Server

10. ☐	**Backup Server**: Verify appropriate PMAC backup exists	This step is likely executed by customer IT personnel. 1. Log into the backup server as the appropriate user using the user password. 2. Execute the appropriate commands to verify the PMAC backup exists for the desired date. 3. Execute the appropriate commands to restore the PMAC management server backup for the desired date. ***Note***: The actions, and commands, required to verify the PMAC backups exist, and the commands required to perform backup and restore on the backup server are the responsibility of the site customer.
11. ☐	**PMAC**: Verify no alarms are present	Verify no alarms are present. `$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus`

12. ☐	Restore the PMAC data from backup	Restore the PMAC data from backup.
		`$ sudo /usr/TKLC/smac/bin/pmacadm restore`
		`PM&C Restore been successfully initiated as task ID 1`
		Check the status of the background task:
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		Note: The result eventually displays PMAC Restore successful.

Procedure 24. Restore PMAC from Backup Server

13. ☐	**PMAC GUI**: Login	1. Open web browser and navigate to the PMAC GUI. `https://<pmac_network_ip>` 2. Login as **PMACadmin** user: 
14. ☐	**PMAC GUI**: Verify restore task completed	1. Navigate to **Task Monitoring**. 2. Verify the restore background task completed successfully. ***Note***: After the restore is complete, you should see **Add Enclosure** tasks start for all previously provisioning servers. These should be allowed to complete before continuing. ***Note***: After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior. ISO images are added in the next step.
15. ☐	**PMAC GUI**: Verify system inventory	1. Navigate to **Hardware > System Inventory**.  2. Verify previously provisioned enclosures are present

Procedure 24. Restore PMAC from Backup Server

16. ☐	**PMAC**: Verify PMAC	Perform a system health check on the PMAC
		`$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus`
		This command should return no output on a healthy system.
		`$ sudo /usr/TKLC/smac/bin/sentry status`
		All processes should be running, displaying output similar to the following:
		`PM&C Sentry Status`
		`------------------`
		`sentryd started: Mon Jul 23 17:50:49 2012`
		`Current activity mode: ACTIVE`
		`Process PID Status StartTS NumR`
		`------------------ ------ ---------- ------------------`
		`smacTalk 9039 running Tue Jul 24 12:50:29 2012 2`
		`smacMon 9094 running Tue Jul 24 12:50:29 2012 2`
		`hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2`
		`snmpEventHandler 9176 running Tue Jul 24 12:50:29 2012 2`
		`Fri Aug 3 13:16:35 2012`
		`Command Complete.`

17. ☐	**PMAC**: Add ISO images to the PMAC	Re-add any needed ISO images to the PMAC by executing procedure **Load Application and TPD ISO onto PMAC Server** from reference [8].

Appendix I. Configure TVOE Hosts

Procedure 25. Configure TVOE

This procedure configures networking on TVOE hosts.

Prerequisite: Server has been IPM'ed with TVOE OS as described in [10].

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

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

<table>
<tr>
<td>1.
</td>
<td>Determine bridge names and interfaces for XMI and IMI, and NetBackup (if used) networks</td>
<td>
1. Determine the bridge names and physical bridge interfaces to be used on the TVOE server for the NOAM XMI and IMI networks.
2. Based on the site survey, determine if you are using VLAN tagging or not, what bonds are used, and also the actual Ethernet interfaces that make up those bonds.
3. If the NetBackup bridge and interface were not previously configured on this server when PMAC was installed, determine those values as well.
4. Fill in the appropriate values in the table below:
<table>
<tr><th>NOAM Guest Interface Name</th><th>TVOE Bridge Name</th><th>TVOE Bridge Interface</th></tr>
<tr><td>xmi</td><td>xmi</td><td>Interface Bond (for example, bond0, bond1, etc.):_____
<TVOE_XMI_Bridge_Interface_Bond>
Interface Name (for example, bond0.3, bond1, bond0.100): _____
<TVOE_XMI_Bridge_Interface></td></tr>
<tr><td>imi</td><td>imi</td><td>Interface Bond:(for example, bond0, bond1, etc.): _____
<TVOE_IMI_Bridge_Interface_Bond>
Interface Name: (for example, bond0.4, bond1, bond0.100): _____
<TVOE_IMI_Bridge_Interface</td></tr>
<tr><td>NetBackup</td><td>NetBackup</td><td>Interface Name (for example, eth11, eth04, eth03, etc.): _____
<TVOE_NetBackup_Bridge_Interface></td></tr>
<tr><td>management</td><td>management</td><td>Interface Name (for example, bond0.2, bond0.37, etc.): _____
<TVOE_Mgmt_Bridge_Interface></td></tr>
</table>
</td>
</tr>
<tr>
<td>2.
</td>
<td>RMS Server: Login</td>
<td>Log in to the TVOE prompt of the RMS server as admusr using the iLO facility.</td>
</tr>
</table>

Procedure 25. Configure TVOE

3. ☐	**RMS Server**: Configure XMI bridge interface bond	1. Verify the XMI bridge interface bond.
		`$ sudo /usr/TKLC/plat/bin/netAdm query --device=<TVOE_XMI_Bridge_Interface_Bond>`
		`Protocol: none`
		`On Boot:  yes`
		`Persistent:  yes`
		`Bonded Mode:active-backup`
		`Enslaving:  eth01 eth02`
		Note: The output below is for illustrative purposes only. The example output shows the control bridge configured.
		If the bond has already been configured, output, similar to what you see above, displays. If this is so, skip to the next step; otherwise, continue with this step.
		2. Create bonding interface and associate subordinate interfaces with bond:
		`$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_XMI_Bridge_Interface_Bond> --onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		`Interface <TVOE_XMI_Bridge_Bond> added`
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_XMI_Bridge_Bond_Ethernet1> --type=Ethernet --master=<TVOE_XMI_Bridge_Interface_Bond> --slave=yes --onboot=yes`
		`Interface <TVOE_XMI_Bridge_Bond_Ethernet1> updated`
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_XMI_Bridge_Bond_Ethernet2> --type=Ethernet --master=<TVOE_XMI_Bridge_Interface_Bond> --slave=yes --onboot=yes`
		`Interface <TVOE_XMI_Bridge_Bond_Ethernet2> updated`
		`$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES --val=<TVOE_XMI_Bridge_Interface_Bond>,[bondX,bondX+1, …,bondN]`
		Note: All other existing bonds should be included in the **val=** statement, for example, if TVOE_XMI_Bridge_Bond = bond1, val=bond0,bond1.
		`$ sudo syscheckAdm net ipbond –enable`

Procedure 25. Configure TVOE

4. ☐	**RMS Server**: Create XMI bridge interface, if needed. (Only for VLAN tagging interfaces)	If you are using VLAN tagging for the XMI bridge interface, then you must create the VLAN interface first.
		`$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_XMI_Bridge_Interface> --onboot=yes`
		`Interface <TVOE_XMI_Bridge_Interface> created.`

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

Procedure 25. Configure TVOE

6. ☐	**RMS Server**: Configure IMI bridge interface bond	1. Verify the IMI bridge interface bond.
		`$ sudo /usr/TKLC/plat/bin/netAdm query --device=<TVOE_IMI_Bridge_Interface_Bond>`
		Protocol: none
		On Boot: yes
		Persistent: yes
		Bonded Mode: active-backup
		Enslaving: eth01 eth02
		Note: The output below is for illustrative purposes only. The example output shows the control bridge configured.
		If the bond has already been configured, output, similar to what you see above, displays. If this is so, skip to the next step; otherwise, continue with this step.
		2. Create bonding interface and associate subordinate interfaces with bond:
		`$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_IMI_Bridge_Interface_Bond> --onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		Interface <TVOE_IMI_Bridge_Bond> added
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_IMI_Bridge_Bond_Ethernet1> --type=Ethernet --master=<TVOE_IMI_Bridge_Bond> --slave=yes --onboot=yes`
		`Interface <TVOE_IMI_Bridge_Bond_Ethernet1> updated`
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_IMI_Bridge_Bond_Ethernet2> --type=Ethernet --master=<TVOE_IMI_Bridge_Bond> --slave=yes --onboot=yes`
		`Interface <TVOE_IMI_Bridge_Bond_Ethernet2> updated`
		3. Execute these 2 commands ONLY IF <TVOE_XMI_Bridge_Bond> is **different** from <TVOE_IMI_Bridge_Bond>.
		`$ sudo syscheckAdm net ipbond --set --var=DEVICES --val=<TVOE_XMI_Bridge_Interface_Bond>, <TVOE_IMI_Bridge_Interface_Bond>,[other bonds…]`
		`$ sudo syscheckAdm net ipbond –enable`

Procedure 25. Configure TVOE

7. ☐	**RMS Server**: Create IMI bridge interface	If you are using VLAN tagging for the IMI bridge interface, then you must create the VLAN interface first.
		`$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_IMI_Bridge_Interface> --onboot=yes`
		`Interface <TVOE_IMI_Bridge_Interface> created.`

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

Procedure 25. Configure TVOE

9. ☐	**RMS Server iLO**: Create management bridge and assign TVOE management IP	1. Execute this step only if the TVOE host is a rack mount server and is NOT the PMAC server.
		Note: The output below is for illustrative purposes only. The site information for this system determines the network interfaces (network devices, bonds, and bond enslaved devices) to configure.
		2. If <TVOE_Management_Bridge_Interface>, or the bond it is based on (if using tagged interface), has not yet been created, then execute the next 3 commands; otherwise, skip to the **EXAMPLE** section:
		`$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Mgmt_Bridge_Interface_Bond> --onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		Interface <TVOE_Management_Bridge_Interface> added
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_Mgmt_Bridge_Bond_Interface1> --type=Ethernet --master=<TVOE_Mgmt_Bridge_Interface_Bond> --slave=yes --onboot=yes`
		Interface <mgmt_ethernet_interface1> updated.
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_Mgmt_Bridge_Bond_Interface2> --type=Ethernet --master-<TVOE_Mgmt_Bridge_Interface_Bond> --slave=yes --onboot=yes`
		Interface <mgmt_ethernet_interface2> updated
		EXAMPLE 1: Create Management bridge using untagged interfaces
		`$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=management --bootproto=none --onboot=yes --address=<TVOE_Mgmt_IP_Address> --netmask=<TVOE_Mgmt_Netmask/Prefix> --bridgeInterfaces=<TVOE_Mgmt_Bridge_Interface>`
		EXAMPLE 2: Create Management bridge using tagged interfaces
		`$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Management_Bridge_Interface>`
		`$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=management --address=<TVOE_Mgmt_IP_Address> --netmask=<TVOE_Mgmt_Netmask/Prefix> --onboot=yes --bridgeInterfaces=<TVOE_Mgmt_Bridge_Interface>`

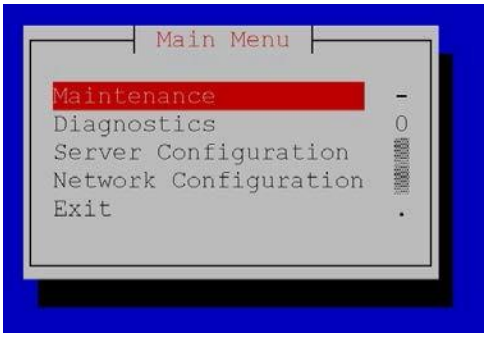
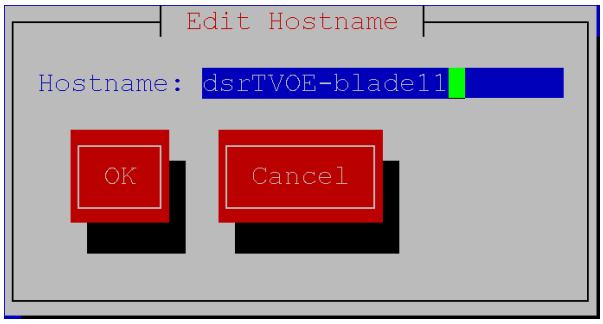
Procedure 25. Configure TVOE

10. ☐	**RMS Server iLO**: Add default route	Add a default route using the xmi or management address (if configured). `$ sudo /usr/TKLC/plat/bin/netAdm add --route=default --gateway=<TVOE_Mgmt_gateway_IP_address> --device=<management or xmi>` Route to management created.

11. ☐	**RMS Server**: Verify bridge creation status	Verify the XMI and IMI bridges have been created successfully (Example output for illustrative purposes only).
		`$ brctl show`
		`[root@SunNetra1Tvoe admusr]# brctl show`
		`bridge name bridge id STP enabled interfaces`
		`control 8000.002128a1a5a8 no bond0`
		`vnet0`
		`vnet12`
		`vnet15`
		`vnet2`
		`vnet7`
		`imi 8000.002128a1a5a8 no bond0.641`
		`vnet10`
		`vnet14`
		`vnet17`
		`vnet5`
		`management 8000.002128a1a5a8 no bond0.637`
		`vnet1`
		`xmi 8000.002128a1a5a8 no bond0.638`
		`vnet13`
		• Verify **imi** and **xmi** are listed under the bridge name column.
		• Verify <TVOE_XMI_Bridge_Interface> is listed under the interfaces column for xmi.
		• Verify <TVOE_IMI_Bridge_Interface> is listed under the interfaces column for imi.
		• Verify the <TVOE_Mgmt_Bridge_Interface> is listed under the interface column for <TVOE_Mgmt_Bridge_Interface>

12. ☐	**RMS Server iLO**: Create NetBackup bridge (Optional)	Perform this command if you have a dedicated NetBackup interface within your NOAM guests (and if the NetBackup bridge was NOT configured when setting up the PMAC earlier). `$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=NetBackup --onboot=yes --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface>`

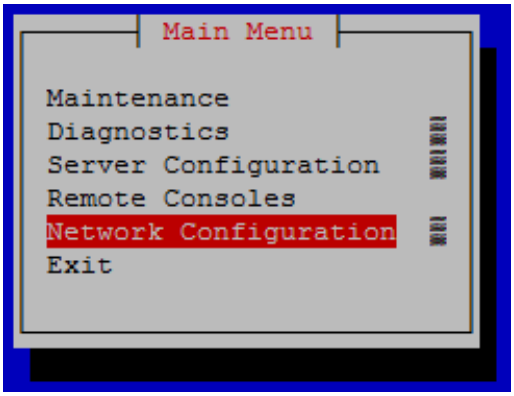
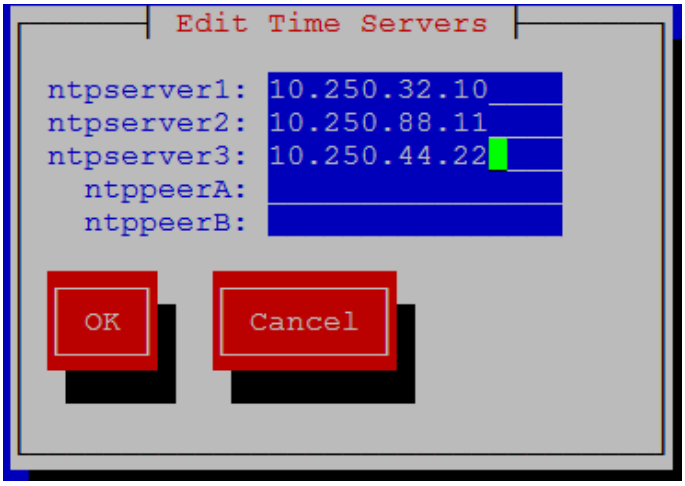
Procedure 25. Configure TVOE

13. ☐	**RMS Server iLO**: Set hostname	`$ sudo su - platcfg`  1. Navigate to **Server Configuration > Hostname > Edit** and enter a new hostname for your server:  2. Click **OK** and continue to click **Exit** until you are at the platcfg main menu again. ***Note***: Although the new hostname has been properly configured and committed at this point, it does not display on your command prompt unless you log out and log back in again.

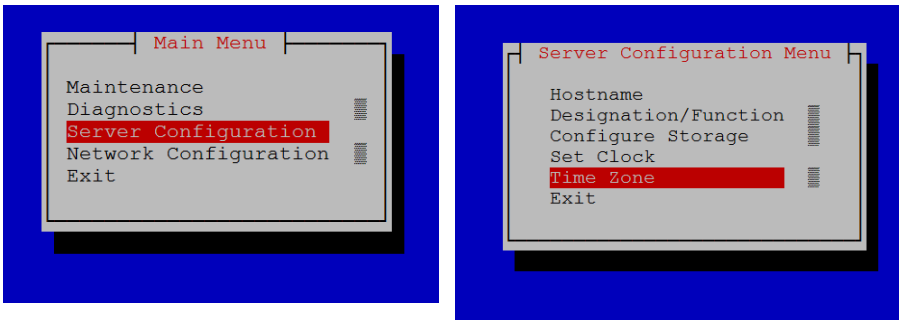
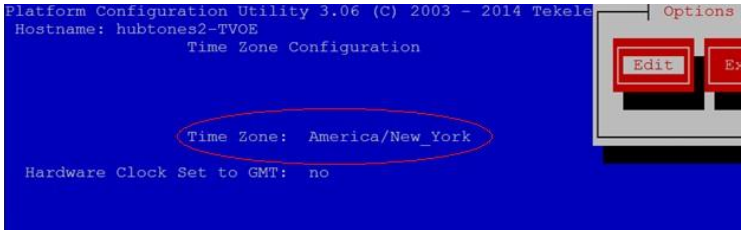
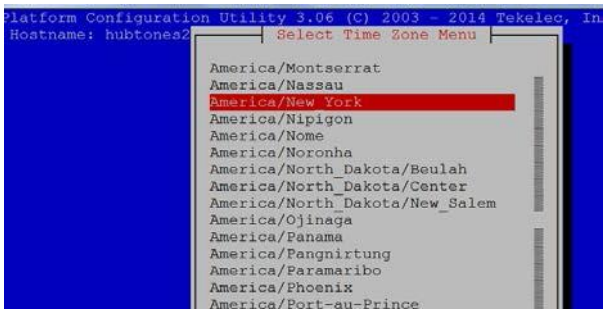
Procedure 25. Configure TVOE

14. ☐	**RMS Server iLO**: Configure SNMP	1. From the platcfg main menu, navigate to **Network Configuration > SNMP Configuration > NMS Configuration**.  2. Click **Edit**. 3. Click **Add a New NMS Server**.  4. Enter the following NMS servers, clicking **OK** after each one and then selecting the **Add NMS** option again: • Enter the Hostname/IP of the customer NMS server, for port enter 162, and for Community String enter the community string provided in the customer NAPD Document. • Enter the IP of the NOAM VIP, for port enter 162, and for Community String enter the community string provided in the customer NAPD Document 5. Click **Exit**. 6. Click **Yes** when prompted to restart the Alarm Routing Service. 7. Once Done, click **Exit** to quit to the platcfg main menu.

Procedure 25. Configure TVOE

15. ☐	**RMS Server iLO**: Configure NTP	1. Select **Network Configuration**.  2. Select **NTP**. 3. Click **Edit**.  • ntpserver1: Enter customer provided NTP server #1 IP address. • ntpserver2: Enter customer provided NTP server #2 IP address. • ntpserver3: Enter customer provided NTP server #3 IP address. 4. Click **OK**. 5. Click **Exit** to return to the platcfg menu.

Procedure 25. Configure TVOE

16. ☐	**RMS Server iLO**: Configure timezone	`$ sudo su - platcfg` 1. Navigate to **Server Configuration > Time Zone**.   2. If the time zone displayed matches the time zone you desire, then you can continue to hit Exit until you are out of the platcfg program. If you want a different time zone, then proceed with this instruction. 3. Click **Edit**.  4. Select the desired time zone from the list and click **Enter**. 5. Continue clicking **Exit** until you are out of the platcfg program.
17. ☐	**RMS Server iLO**: Reboot server	Reboot the server. `$ sudo su - platcfg`

Appendix J. Create NOAM/SOAM Virtual Machines

Procedure 26. Create NOAM Guest VMs

This procedure creates a DSR NOAM virtual machine (referred to as a **guest**) on a TVOE server blade or TVOE RMS. It is repeated for every NOAM server you want to install.

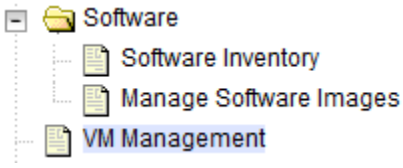
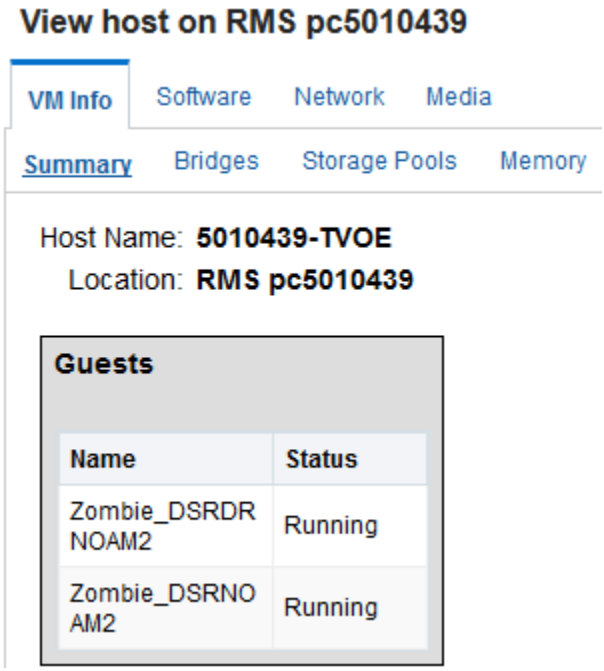
Prerequisite: TVOE has been installed and configured on the target blade server or RMS

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

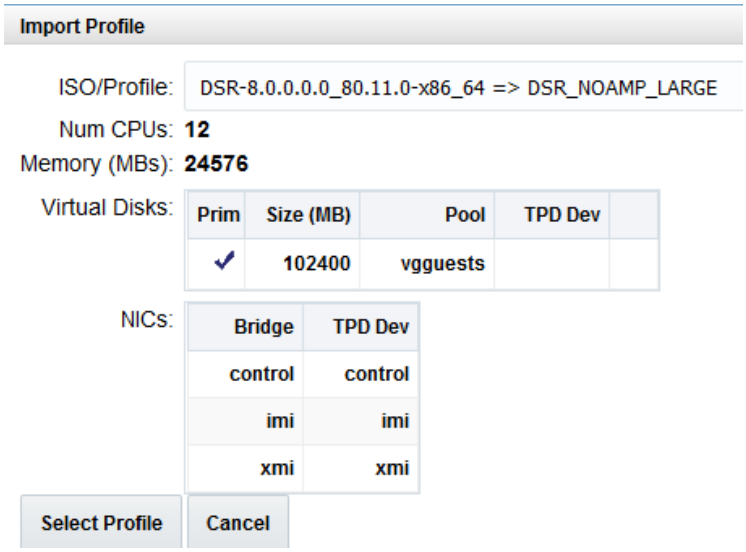
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

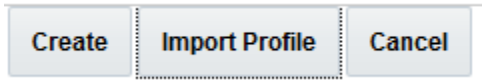
1. ☐	**PMAC GUI**: Login	1. Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` 2. Login as **pmacadmin** user: 

Procedure 26. Create NOAM Guest VMs

2. ☐	**PMAC GUI**: Navigate to VM management of the target server blade	1. Navigate to **Main Menu > VM Management**.  2. Select the TVOE server blade or rack mounted server from the **VM Entities** listing on the left side of the screen. The selected server's guest machine configuration displays in the remaining area of the window.  3. Click **Create Guest**.

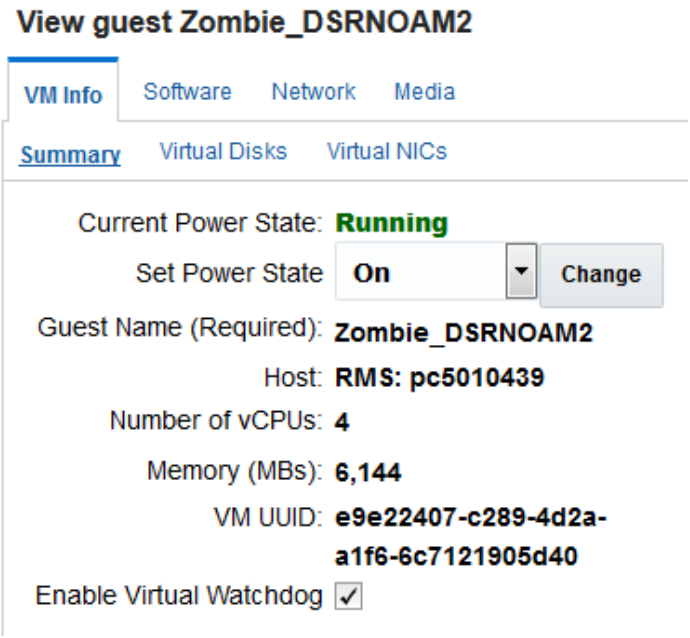
Procedure 26. Create NOAM Guest VMs

<table>
<tr>
<td>3.
☐</td>
<td>PMAC GUI:
Configure VM guest parameters</td>
<td>
1. Click Import Profile.


2. From the ISO/Profile drop-down box, select the entry that matches depending on the hardware that your NOAM VM TVOE server is running on and your preference for NetBackup interfaces:
<table>
<tr><th>NOAM VM TVOE Hardware Type(s)</th><th>Dedicated Netbackup Interface?</th><th>Navigate to Profile (<Application ISO NAME>)</th></tr>
<tr><td>HP DL380 Gen 8 RMS,
HP BL460 Gen 9 RMS,
HP BL460 Gen 8 Blade,
HP BL460 Gen 9 Blade</td><td>No</td><td>DSR_NOAMP_LARGE</td></tr>
<tr><td>HP DL380 Gen 8 RMS,
HP BL460 Gen 9 RMS,
HP BL460 Gen 8 Blade,
HP BL460 Gen 9 Blade</td><td>Yes</td><td>DSR_NOAMP_LARGE_NBD</td></tr>
</table>
Note: Application_ISO_NAME is the name of the DSR Application ISO to be installed on this NOAM
3. Click Select Profile.
4. Click Create


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

Procedure 26. Create NOAM Guest VMs

<table>
<tr>
<td>4.
</td>
<td>PMAC GUI:
Wait for guest creation to complete</td>
<td>1. Navigate to Main Menu > Task Monitoring to monitor the progress of the guest creation task. A separate task displays for each guest creation you start.
2. Wait or refresh the screen until you see the guest creation task has completed successfully.
<table>
<tr><td>Create Guest</td><td>RMS: pc5010439
Guest:
Zombie_DSRNOAM2</td><td>Guest creation completed (Zombie_DSRNOAM2)</td></tr>
</table>
</td>
</tr>
<tr>
<td>5.
</td>
<td>PMAC GUI:
Verify guest machine is running</td>
<td>1. Navigate to Main Menu > VM Management.
2. Select the TVOE server blade on which the guest machine was just created.
3. Look at the list of guests present on the blade and verify you see a guest that matches the name you configured and that its status is Running.
 

4. VM creation for this guest is complete. Repeat from step 2 for any remaining NOAM VMs (for instance, the standby NOAM) that must be created.</td>
</tr>
</table>

Procedure 27. Create SOAM Guest VMs

This procedure creates a DSR SOAM virtual machine (referred to as a **guest**) on a TVOE server blade. It is repeated for every SOAM server you want to install.

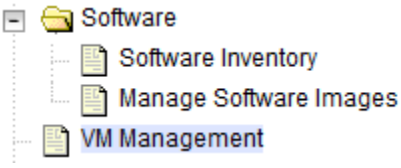
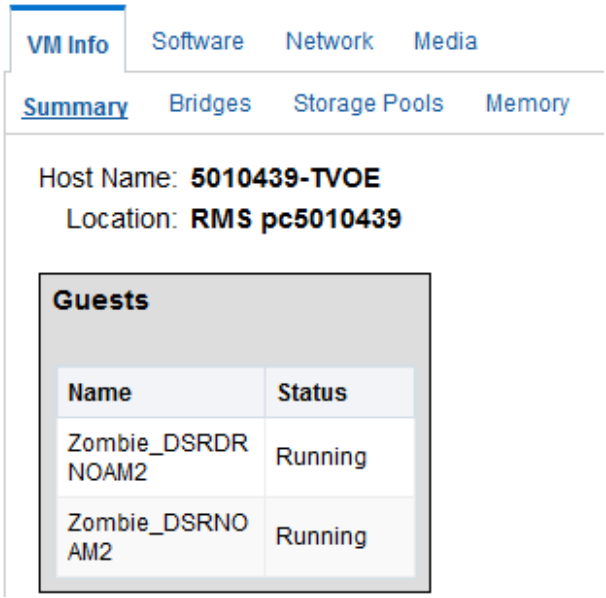
Prerequisite: TVOE has been installed and configured on the target blade server.

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

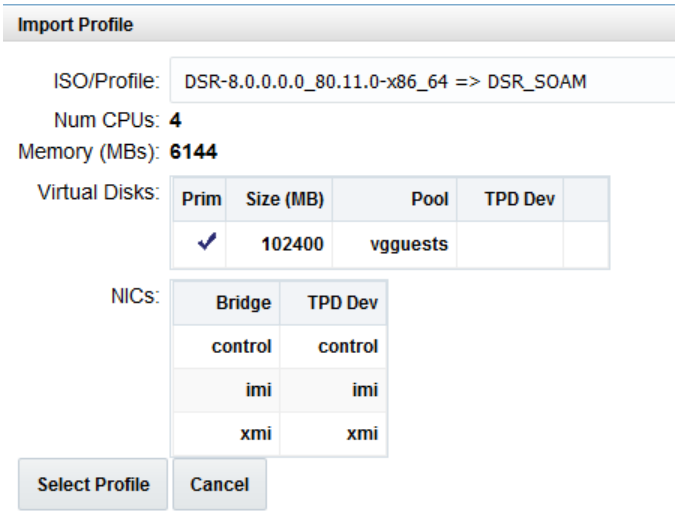
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

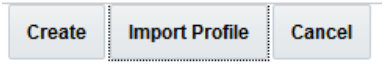
1. ☐	**PMAC GUI**: Login	1. Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` 2. Login as **pmacadmin** user: 

Procedure 27. Create SOAM Guest VMs

2. ☐	**PMAC GUI**: Navigate to VM management of the target server blade	1. Navigate to **Main Menu > VM Management**.  2. Select the TVOE server blade or rack mounted server from the **VM Entities** listing on the left side of the screen. The selected server's guest machine configuration displays in the remaining area of the window.  3. Click **Create Guest**.

Procedure 27. Create SOAM Guest VMs

<table>
<tr>
<td>3.
☐</td>
<td>PMAC GUI:
Configure VM guest parameters</td>
<td>
1. Click Import Profile.


2. From the ISO/Profile drop-down box, select the entry that matches depending on the hardware that your SOAM VM TVOE server is running on and your preference for NetBackup interfaces.
<table>
<tr><th>SOAM VM TVOE Hardware Type(s)</th><th>Dedicated Netbackup Interface?</th><th>Navigate to Profile (<Application ISO NAME>)</th></tr>
<tr><td>HP BL460 Gen 8 Blade,
HP BL460 Gen 9 Blade</td><td>No</td><td>DSR_SOAM</td></tr>
<tr><td>HP BL460 Gen 8 Blade,
HP BL460 Gen 9 Blade</td><td>Yes</td><td>DSR_SOAM_NBD</td></tr>
</table>
Note: Application_ISO_NAME is the name of the DSR Application ISO to be installed on this SOAM
3. Click Select Profile.
4. Edit the name, if you want. For instance: DSR_SOAM_A or DSR_SOAM_B. This is not the ultimate hostname. It is just an internal tag for the VM host manager.
5. Click Create.


</td>
</tr>
<tr>
<td>4.
☐</td>
<td>PMAC GUI:
Wait for guest creation to complete</td>
<td>
1. Navigate to Main Menu > Task Monitoring to monitor the progress of the guest creation task. A separate task displays for each guest creation you start.
2. Wait or refresh the screen until you see that the guest creation task has completed successfully.


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

Procedure 27. Create SOAM Guest VMs

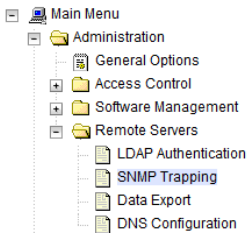
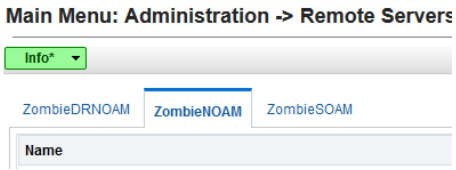
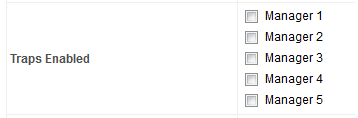
5. ☐	**PMAC GUI**: Verify guest machine is running	1. Navigate to **Main Menu > VM Management**. 2. Select the TVOE server blade on which the guest machine was just created. 3. Look at the list of guests present on the blade and verify you see a guest that matches the name you configured and that its status is **Running**.  4. VM creation for this guest is complete. Repeat from Step 2 for any remaining NOAM VMs (for instance, the standby SOAM) that must be created.

Appendix K. SNMP Configuration

Procedure 28. Configure SNMP

This workaround configures SNMP with **SNMPv2c and SNMPv3** as the enabled versions for SNMP Traps configuration, as PMAC does not support SNMPv3. 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) N**OAM VIP GUI**: Login	***Note***: This workaround step should be performed only in the following cases: 1. If SNMP is not configured. 2. If SNMP is already configured and **SNMPv3** is selected as enabled version. ***Note***: This is a workaround step to configure SNMP with 'SNMPv2c and SNMPv3' as the enabled versions for SNMP Traps configuration, since PMAC does not support SNMPv3. 1. If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 3. Log into the NOAM GUI as the **guiadmin** user: 

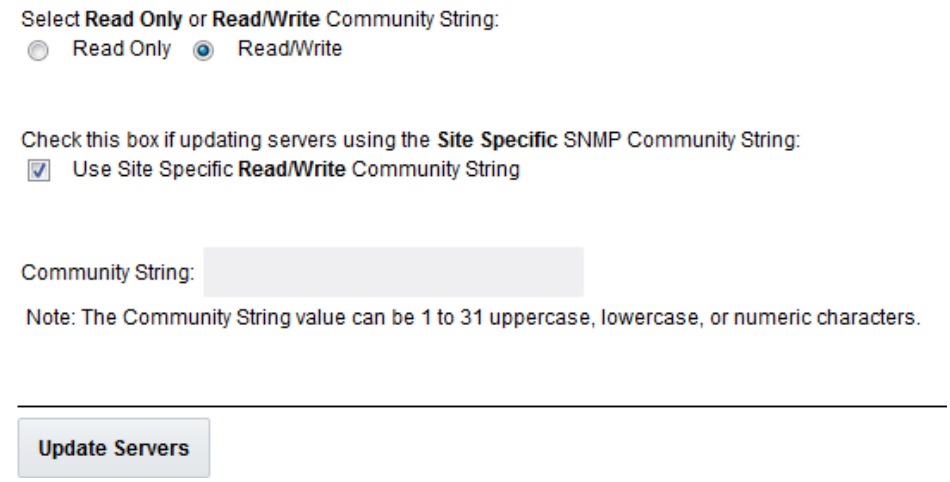
Procedure 28. Configure SNMP

2. ☐	**NOAM VIP GUI**: Configure system-wide SNMP trap receiver(s)	1. Navigate to **Administration > Remote Servers > SNMP Trapping**.  2. Select the Server Group tab for SNMP trap configuration:  3. Type the **IP address** or **hostname** of the Network Management Station (NMS) where you want to forward traps. This IP should be reachable from the NOAMP's XMI network. If already configured SNMP with **SNMPv3** as enabled version, another server needs to be configured here. 4. Continue to fill in additional secondary, tertiary, etc., Manager IPs in the corresponding slots if desired.  5. Set the Enabled Versions as **SNMPv2c and SNMPv3**.  6. Check **Traps Enabled** checkboxes for the Manager servers being configured.  7. Type the **SNMP Community Name**.  8. Leave all other fields at their default values. 9. Click **OK**.

Procedure 28. Configure SNMP

3. ☐	**PMAC GUI**: Login	1. Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` 2. Login as **guiadmin** user: 

Procedure 28. Configure SNMP

4. ☐	**PMAC GUI**: Update the TVOE host SNMP community string	1. Navigate to **Administration > Credentials > SNMP Community String Update**. 2. Check the **Use Site Specific Read/Write Community String** checkbox.  3. Click **Update Servers**. 4. Click **OK**. 

Appendix L. Backup Directory

Procedure 29. Backup Directory

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 29. 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 M. netConfig backupConfiguration/restoreConfiguration/upgradeFirmware with TPD Cipher Change

Beginning with TPD 7.6.0.0.0_88.50.0 and later, the cipher list is restricted to allow only a limited number of ciphers for ssh access to the servers. As a result, netConfig backup and restore operations are not functional with Cisco switches (3020, 4948s) since these switches use other ciphers. Executing these commands with the restricted ciphers would fail as shown here:

```
[admusr@p5-pmac ~]$ sudo netConfig --device=3020_ip backupConfiguration
service=ssh_ip filename=backup
Command failed: backupConfiguration
Error saving to SSH service
[admusr@p5-pmac ~]$
```

To avoid this issue while maintaining a focus on improved security, the Procedure 30 must be executed before and after netConfig backup and restore operations.

Procedure 30. Turn Off Cipher List Before backupConfiguation/restoreConfiguration/upgradeFirmware Command

This procedure prepares the PMAC to avoid the cipher mismatch issue with Cisco switches. This is performed before the netConfig backup or restore operations.

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. ☐	Turn off cipher list	4. From the PMAC shell enter:
		`sudo vi /etc/ssh/sshd_config`
		5. Add # in the beginning of the following three lines to comment them out, the result is:
		`#Ciphers aes256-ctr,aes192-ctr,aes128-ctr`
		`#MaxAuthTries 4`
		`#LoginGraceTime 1m`

2. ☐	Restart sshd	`sudo service sshd restart`

3. ☐	Run the netConfig backupConfiguation/restoreConfiguration/upgradeFirmware command	For a backup operation:
		`[admusr@pmac ~]$ sudo /usr/TKLC/plat/bin/netConfig backupConfiguration --device=<switch_name> service=<ssh_service> filename=<switch_name>-backup`
		For a restore operation:
		`[admusr@pmac ~]$ sudo /usr/TKLC/plat/bin/netConfig restoreConfiguration --device=<switch_name> service=<ssh_service> filename=<switch_name>-backup`
		For a upgrade operation:
		`[admusr@pmac ~]$ sudo /usr/TKLC/plat/bin/netConfig upgradeFirmware --device=<switch_name> service=<ssh_service> filename=<Cisco IOS>`

Procedure 31. Resume Cipher List After backupConfiguation/restoreConfiguration/upgradeFirmware Command

This procedure restores the PMAC restricted cipher list after perform the netConfig backup and restore operations.

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. ☐	Resume the cipher list	1. From the PMAC shell enter:
		`sudo vi /etc/ssh/sshd_config`
		2. Add # in the beginning of the following three lines to comment them out, the result is:
		`Ciphers aes256-ctr,aes192-ctr,aes128-ctr`
		`MaxAuthTries 4`
		`LoginGraceTime 1m`

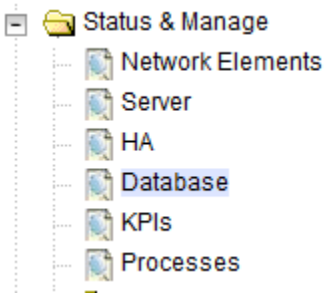
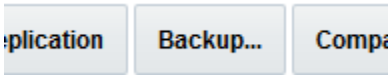
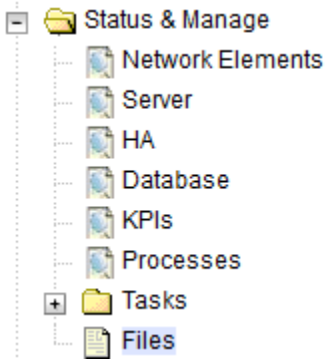
2. ☐	Restart sshd	`sudo service sshd restart`

Appendix N. DSR Database Restore

Procedure 32. DSR Database Restore

The intent of this procedure is to restore the provision and configuration information from an NOAM 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 VIP**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 

Procedure 32. DSR Database Restore

2. ☐	**NOAM VIP**: Restore configuration data for the system	3. Navigate to **Status and Manage > Database**.  4. Select the active NOAM server and click **Disable Provisioning**.  5. Click **OK**.
3. ☐	**NOAM VIP**: Verify the restore file existence	1. Navigate to **Status and Manage > Files**.  2. Select the NOAM with OAM Max HA Role. 3. Select **Restore**. 4. Select the backup file to be used in the restore and click [Ok]. The Database Restore Confirm screen displays. 5. If there are any inconsistencies between the current state of the system and the information found in the backup file, a message displays indicating **Incompatible database selected**. If this is the case, mark the **Force** checkbox, and click **OK**. If not, simply click **OK** to start the restore process. The system begins restoring the database. After the restore is completed, the user is logged out of the NOAM GUI. Allow up to ten minutes for the restore to complete before the GUI returns to the login prompt.
4. ☐	**NOAM VIP**: Enable Provisioning	1. On the NOAM GUI navigate to **Status and Manage** >**Database** 2. Enable Provisioning by clicking on **Enable Provisioning** button at the bottom left hand side of the GUI form 3. Click **Ok** on the pop-up window, Provisioning will now be enabled Log into the Application GUI using the NOAM VIP as user with admin privileges.

Procedure 32. DSR Database Restore

5. ☐	**NOAM VIP**: Allow provisioning	1. Allow replication on all servers in this order: a. Active NOAM server b. Standby NOAM server c. Active SOAM server d. Standby SOAM server e. Active MP servers f. Standby MP servers 2. Navigate to **Status and Manage > HA**. 3. Click **Edit**. 4. Select the **Standby NOAM** and change the **Max Allowed HA Role** to **Active**. 5. Verify proper configuration displays.

Appendix O. 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 on the Support telephone menu:

1. Select 2 for **New Service Request**.
2. Select 3 for **Hardware, Networking and Solaris Operating System Support**.
3. Select one of the following options:

For technical issues such as creating a new Service Request (SR), select **1**.

For non-technical issues such as registration or assistance with MOS, select **2**.

You are connected to a live agent who can assist you with MOS registration and opening a support ticket. MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

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

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

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

- Loss of the system ability to provide any required critical or major trouble notification

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

Locate Product Documentation on the Oracle Help Center

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

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the **Oracle Communications** subheading, click the **Oracle Communications documentation** link. The Communications Documentation page appears. Most products covered by these documentation sets display under the headings **Network Session Delivery and Control Infrastructure** or **Platforms**.
4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release displays. 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.