Oracle® Communications

Diameter Signaling Router

Rack Mount Server Disaster Recovery Guide

Release 8.4

F12329-01

April 2019

Oracle Communications DSR Rack Mount Server Disaster Recovery User's Guide, Release 8.4

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

List of Tables

List of Figures

List of Procedures

1. Introduction

This document is a guide to describe procedures used to execute disaster recovery for DSR Rack Mount Server deployment. This includes recovery of partial or complete loss RMS servers. The audience for this document includes GPS groups such as Software Engineering, Product Verification, Documentation, and Customer Service including Software Operations and First Office Application. This document can also be executed by Oracle customers, as long as Oracle Customer Service personnel are involved and/or consulted. This document provides step-by-step instructions to execute disaster recovery for DSR. Executing this procedure also involves referring to and executing procedures in existing support documents.

Note that components dependent on DSR might need to be recovered as well, for example IDIH, PMAC, and SDS (Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen9 Only).

Note that this document only covers the disaster recovery scenarios of DSR Rack Mount Server deployments.

1.1 References

[1] TPD Initial Product Manufacture

[2] Platform 7.2 Configuration Procedure Reference

[3] DSR FABR Feature Activation Procedure

[4] DSR RBAR Feature Activation Procedure

[5] DSR MAP-Diameter Feature Activation Procedure

[6] PM&C Disaster Recovery Guide

[7] DSR PCA Activation Guide

[8] DSR Rack Mount Server Installation Guide

[9] DSR Hardware and Software Installation Procedure 1/2

[10] DCA Framework and Application Activation and Deactivation Guide

[11] DSR Security Guide

[12] DSR DTLS Feature Activation Procedure

[13] DSR/SDS NOAM Failover User's Guide

1.2 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CD	Compact Disk
DSR	Diameter Signaling Router
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
FRU	Field Replaceable Unit
IDIH	Integrated Diameter Intelligence Hub

Acronym	Definition
iLO	Integrated Lights Out manager
IPFE	IP Front End
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 (e.g. TPD)
PCA	Policy and Charging Application
PMAC	Platform Management & Configuration
RMS	Rack Mounted Server
SAN	Storage Area Network
SDS	Subscriber Database Server
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtual Operating Environment
VM	Virtual Machine

1.3 Terminology

An alphabetized list of terms used in the document.

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).
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.
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.

1.4 How to Use this Document

When executing the procedures in this document, there are a few key points to ensure you understand procedure convention. These points are:

1. Before beginning a procedure, completely read the instructional text (it displays immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.
2. Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.
3. If a procedural STEP fails to execute successfully or fails to receive the desired output, STOP the procedure. It is recommended to contact My Oracle Support (MOS) for assistance, as described in Appendix N before attempting to continue.

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

- Each step has a checkbox that the user should check-off to keep track of the progress of the procedure.
- Any sub-steps within a step are referred to as step X.Y. The example in Figure 1 shows steps 1 and step 2 and substep 2.1.
- The title box describes the operations to be performed during that step.
- GUI menu items, action links, and buttons to be clicked on are in bold Arial font.
- GUI fields and values to take note of during a step are in bold Arial font.
- Each command that the user enters, as well as any response output, is formatted in `10-point Courier` font.

	Title/Instructions	**Directive/Result Steps**
1. ☐	Change directory	Change to the backout directory. `$ cd /var/TKLC/backout`
2. ☐	Verify Network Element data	View the Network Elements configuration data; verify the data; save and print report. 1. Select **Configuration > Network Elements** to view Network Elements Configuration screen.

Figure 1. Example Procedure Steps Used in This Document

1.5 Optional Features

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

Table 3. Optional Features

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

Feature	Document
Map-Diameter Interworking (MAP-IWF)	DSR MAP-Diameter IWF Feature Activation Procedure
Policy and Charging Application (PCA)	DSR PCA Activation Guide
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation Procedure

2. General Description

The DSR disaster recovery procedure has 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 have 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 have 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 have failed.
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)

Procedure	State of NOAM and/or SOAM server(s)
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: For failed aggregation switches (HP DL380 Gen 8 Only), refer to Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only).

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

Note: A failed server in disaster recovery context refers to a server that has suffered partial or complete software 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 that at least one NOAM servers intact. All SOAM servers have failed (including SOAM spares-If equipped) and are recovered using base recovery of hardware and software. Database is restored on the SOAM server and replication will recover the database of the remaining servers.

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

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 Server Outage with Both NOAMs Failed and 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.

2.6 Partial Service Outage with Corrupt Database

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

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

3. Procedure Overview

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

3.1 Required Materials

The following items are needed for disaster recovery:

1. A hardcopy of this document and hardcopies of all documents in the reference list.
2. Hardcopy of all NAPD performed at the initial installation and network configuration of this customer's site. If the NAPD cannot be found, escalate this issue within My Oracle Support (MOS) until the NAPD documents can be located.
3. DSR recent backup files: electronic backup file (preferred) or hardcopy of all DSR configuration and provisioning data.
4. Latest Network Element report: Electronic file or hardcopy of Network Element report.
5. The XML configuration files used to configure the Cisco 4948 aggregation switches, available on the PMAC Server (or PMAC backup).
6. The switch backup files taken after the switch is configured, available on the PMAC server (or PMAC backup).
7. The network element XML file used for the initial configuration.
8. Firmware files as provide by hardware vendor.
9. NetBackup files if they exist. This may require the assistance of the customer's NetBackup administrator.
10. PMAC and TVOE backups (if available).
11. One (1) target release DSR media or a target-release ISO.
12. One (1) target release SDS Media or a target-release ISO (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only).
13. Three (3) target release iDIH Media or target-release ISOs.

14. Site specific VM Placement and Socket Pinning workbook used during deployment (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 only).
15. Latest RADIUS shared secret encryption key file backup (DpiKf.bin.encr).
16. List of activated and enabled features.

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

3.2 Disaster Recovery Strategy

Disaster recovery procedure execution is performed as part of a disaster recovery strategy with 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 3.1 Required Materials.
4. From the failure conditions, determine the Recovery Scenario and procedure to follow (using Figure 2 and Table 4. Recovery Scenarios.
5. Execute appropriate recovery procedures (listed in Table 4. Recovery Scenarios).

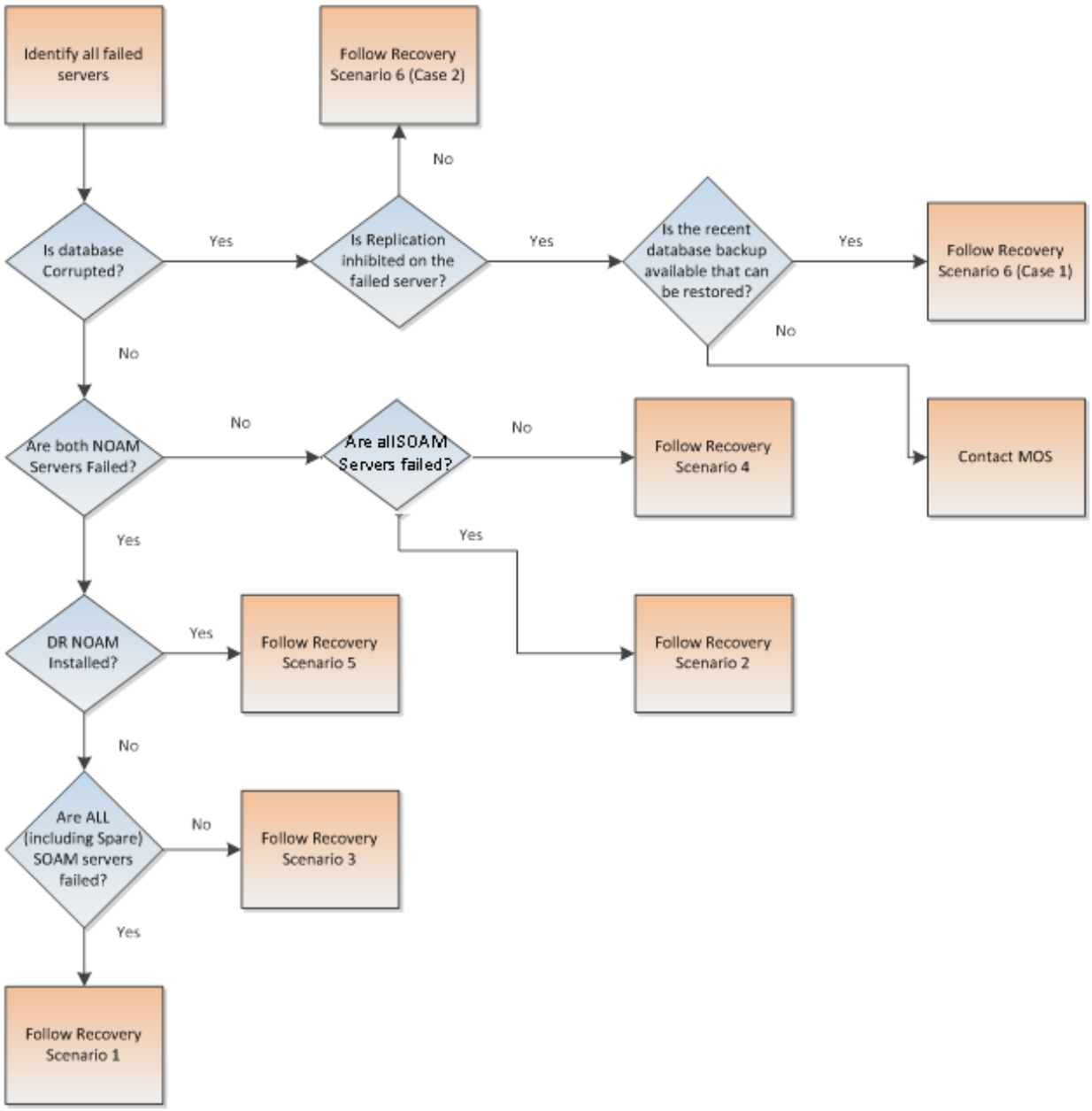


Figure 2. Determining Recovery Scenario

4. Disaster Recovery Procedure

Before disaster recovery, properly evaluate the outage scenario. Call My Oracle Support (MOS) before executing this procedure to ensure the proper recovery planning is performed.

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 available in the system since the system is DRed. In this case, 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.DSRNO1.Configuration.NETWORK_OAMP.20180328_021502.AUTO.tar
- Backup.dsr.DSRSO1.Configuration.SYSTEM_OAM.20180328_021502.AUTO.tar
- X7201TVOE-plat-app-201803281022.iso
- backupPmac_20180328_050002.pef5.1.1

4.1 Recovery Scenario 1 (Complete Server Outage)

For a complete server outage, TVOE is recovered on all rack mount servers. The VMs are re-created and configured. The database restored on one of the NOAM and SOAM servers.

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
  - Recover the base hardware
  - Recover the virtual machines
  - Recover the software

- Recover **PMAC**
- Recover active **NOAM** guest
  - Recover the NOAM database
  - Reconfigure the application
- Recover standby **NOAM** guest
  - Reconfigure the application
- Recover query server (SDS only) guest
  - Reconfigure the application
- Recover all **SOAM** and MP/DP guest
  - Recover the SOAM database
  - Reconfigure the application
- Recover I**DIH**, if necessary
- Restart processes and re-enable provisioning and replication.

Procedure 1. Recovery Scenario 1

S T E P #	This procedure performs recovery if both NOAM servers are failed and all SOAM servers 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 the Required Materials section.
2. ☐	Create a backup directory, if needed	Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.
3. ☐	Replace failed equipment	Work with the hardware vendor to replace the failed equipment.
4. ☐	**Recover PMAC and PMAC TVOE Host**: Configure BIOS settings and update firmware	1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]: • **HP DL380 Gen8**: Configure HP Gen 8 Server BIOS Settings • **Oracle X5-2/Netra X5-2/X6-2/X7-2**: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings • **HP DL380 Gen9**: Configure HP Gen9 Server BIOS Settings 2. Verify and/or upgrade server firmware by executing the **Upgrade Rack Mount Server Firmware** procedure from reference [8]. ***Note:*** Determine VM placement and pinning by following: • Section 3.1, item 14; and • In reference [8], Appendix S VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1 Gbps NICs) and CPU Pinning in HP DL380 Gen 9 (Onboard 1 Gbps NICs) for Pinning Information on HP DL380 Gen 9.

Procedure 1. Recovery Scenario 1

5. ☐	**Recover PMAC, TVOE Hosts, and Switch**: Backups available	This step assumes TVOE and PMAC backups are available. If backups are **NOT** available, **skip this step**. 1. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers. 2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup. 3. Proceed to step 7.
6. ☐	**Recover PMAC, TVOE Hosts, and Switch**: 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**. Execute these procedures from reference [8]: • **Install and Configure TVOE on First RMS (PMAC Host)** • **Install PMAC** • **Initialize the PMAC Application**
7. ☐	Recover failed Cisco 4948 aggregation switches (HP DL380 only)	Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 GEN 9, **skip this step**. Recover failed Cisco 4948 aggregation switches, if needed: 1. Back up available configuration files. Refer to Appendix C Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only) to recover failed Cisco 4948 aggregation switches. 2. Back up configuration files NOT available. Execute the **Configure Cisco 4948E-F Aggregation Switches (HP DL 380 Gen 8 Only)** section from reference [8].
8. ☐	Configure PMAC (no backup)	If PMAC backup was **NOT** restored in step 5. , execute this step; otherwise, skip this step. Execute these procedures from reference [8]: • **Configure PMAC Server (NetBackup Only)** • **Add RMS to the PMAC Inventory**
9. ☐	Install/Configure additional rack mount servers	1. Execute the **Install TVOE on Additional Rack Mount Servers** procedure from reference [8]. 2. **If backups are available**, restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers. **If backups are NOT available**, execute the **Configure TVOE on Additional Rack Mount Servers** procedure from reference [8].
10. ☐	Configure BIOS settings and update firmware on additional rack mount servers	1. Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]: • **HP DL380 Gen8**: Configure HP Gen 8 Server BIOS Settings • **Oracle X5-2/Netra X5-2/X6-2/X7-2**: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings • **HP DL380 Gen9**: Configure HP Gen9 Server BIOS Settings 2. Verify and/or upgrade server firmware by executing the **Upgrade Rack Mount Server Firmware** procedure from reference [8].

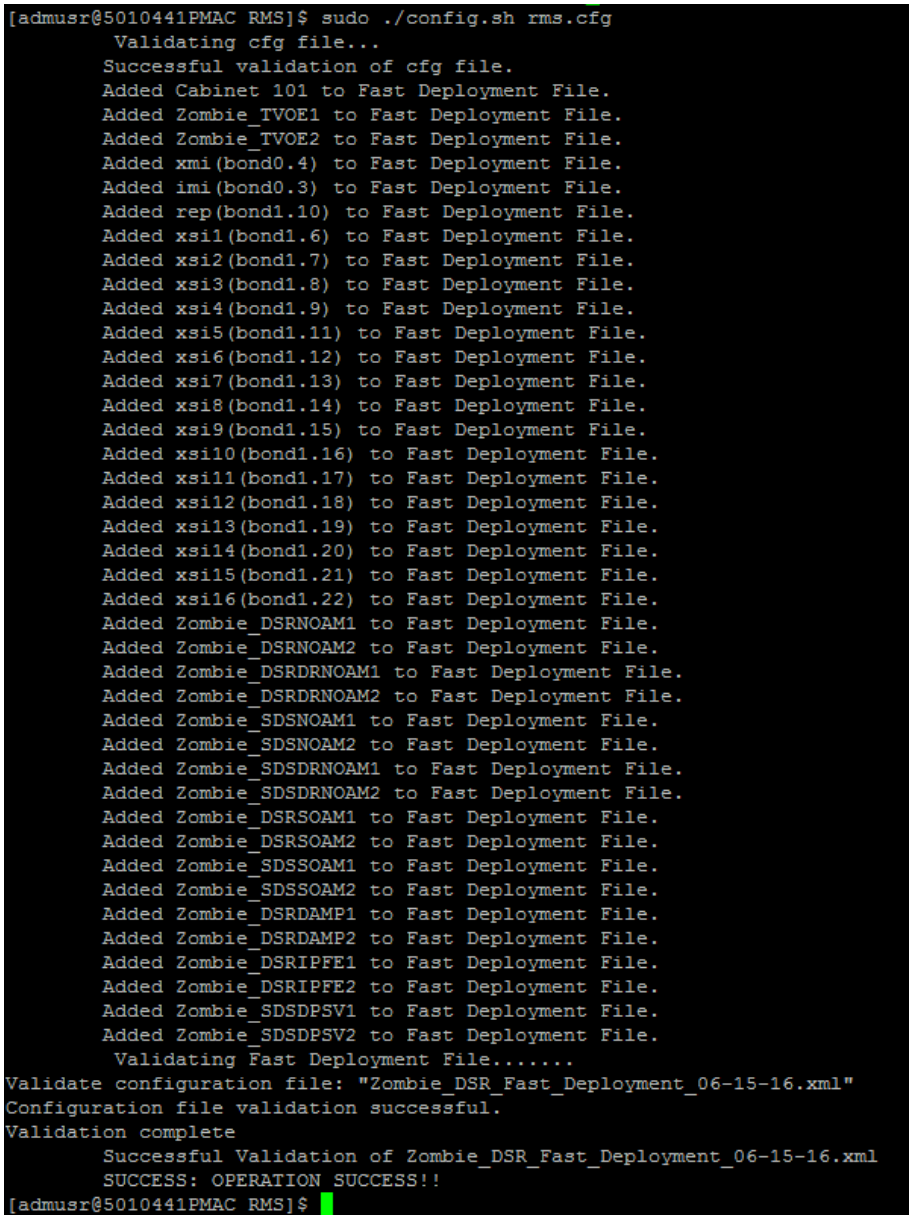
Procedure 1. Recovery Scenario 1

11. ☐	Determine VM placement and socket pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 only)	HP DL380 GEN 8, **skip this step**. Determine VM placement and pinning by following: 1. Section 3.1, item 14; and 2. In reference [8], Appendix S VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1 Gbps NICs) and CPU Pinning in HP DL380 Gen 9 (Onboard 1 Gbps NICs) for Pinning Information on HP DL380 Gen 9.
12. ☐	Deploy redundant PMAC, if required	Refer to the **Deploy Redundant PMAC (Optional)** procedure to re-deploy and configure any redundant PMACs previously configured.
13. ☐	**PMAC**: Determine if the fdconfig file exists from the initial deployment	1. Type: `[admusr@melbourne-pmac-1 ~]$ ll /usr/TKLC/smac/etc/fdc/` 2. Examine the results and verify if the **rms config file <hostname>.cfg** exists. ***Note:*** There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS.
14. ☐	Create fdconfig backup file, if it does not already exist	Execute this step ONLY If the fdconfig backup file does **NOT** exist. 1. Create the needed file(s) by executing the **Virtual Machine/Network Fast Deployment** section from reference [8]. **WARNING** It is very important to ensure the file(s) created only affects the TVOE server(s) and the guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service. 2. Skip to step 23. if this step was executed.
15. ☐	**PMAC**: Load ISOs into PMAC, if not done already	If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the **Virtual Machine/Network Fast Deployment** section from reference [8].
16. ☐	**PMAC**: Edit/Update configuration file	Edit the fdconfig file to include only the required/failed servers. ***Notes***: • Comment out configuration items that are not needed. • Create a separate configuration file for EACH rack mount server being deployed. • The Cabinet ID in the config file needs to match the cabinet already defined in PMAC. The following items are mandatory: • siteName • tpdIso • dsrIso (if DSR VMs are being configured) • sdsIso (if SDS VMs are being configured) • NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured)

Procedure 1. Recovery Scenario 1

		• XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured) • XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured) • DSRNOAM1XMIIPADDRESS (if DSRNOAM1 is being configured) • DSRNOAM2XMIIPADDRESS (if DSRNOAM2 is being configured) • DSRDRNOAM1XMIIPADDRESS (if DSRDRNOAM1 is being configured) • DSRDRNOAM2XMIIPADDRESS (if DSRDRNOAM2 is being configured) • SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured) • SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured) • SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured) • SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured) ***Notes***: • Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8]. • Comment out SDS and DSR profile items if corresponding products are not used. • For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9, refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8]. • VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName. • VM locations should not be changed from their **RMSx** format. Each RMS should correspond to a separate rack mount server. **WARNING** Ensure the file(s) created only affect the TVOE server(s) and guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.
17. ☐	**PMAC**: Copy the backed up fdc file to the RMS directory	Copy the fdconfig backup file to the RMS directory. `$ sudo cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file> /usr/TKLC/smac/etc/RMS/`

Procedure 1. Recovery Scenario 1

18. ☐	**PMAC**: Execute the config.sh script	Execute **config.sh** against the modified backup config file. ***Note:*** If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again. `$ sudo ./config.sh <config file>` Example output: 

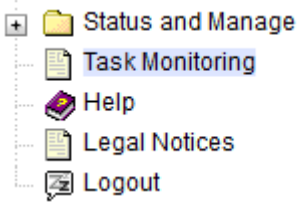
```
[admusr@5010441PMAC RMS]$ sudo ./config.sh rms.cfg
        Validating cfg file...
       Successful validation of cfg file.
       Added Cabinet 101 to Fast Deployment File.
       Added Zombie_TVOE1 to Fast Deployment File.
       Added Zombie_TVOE2 to Fast Deployment File.
       Added xmi(bond0.4) to Fast Deployment File.
       Added imi(bond0.3) to Fast Deployment File.
       Added rep(bond1.10) to Fast Deployment File.
       Added xsi1(bond1.6) to Fast Deployment File.
       Added xsi2(bond1.7) to Fast Deployment File.
       Added xsi3(bond1.8) to Fast Deployment File.
       Added xsi4(bond1.9) to Fast Deployment File.
       Added xsi5(bond1.11) to Fast Deployment File.
       Added xsi6(bond1.12) to Fast Deployment File.
       Added xsi7(bond1.13) to Fast Deployment File.
       Added xsi8(bond1.14) to Fast Deployment File.
       Added xsi9(bond1.15) to Fast Deployment File.
       Added xsi10(bond1.16) to Fast Deployment File.
       Added xsi11(bond1.17) to Fast Deployment File.
       Added xsi12(bond1.18) to Fast Deployment File.
       Added xsi13(bond1.19) to Fast Deployment File.
       Added xsi14(bond1.20) to Fast Deployment File.
       Added xsi15(bond1.21) to Fast Deployment File.
       Added xsi16(bond1.22) to Fast Deployment File.
       Added Zombie_DSRNOAM1 to Fast Deployment File.
       Added Zombie_DSRNOAM2 to Fast Deployment File.
       Added Zombie_DSRDRNOAM1 to Fast Deployment File.
       Added Zombie_DSRDRNOAM2 to Fast Deployment File.
       Added Zombie_SDSNOAM1 to Fast Deployment File.
       Added Zombie_SDSNOAM2 to Fast Deployment File.
       Added Zombie_SDSDRNOAM1 to Fast Deployment File.
       Added Zombie_SDSDRNOAM2 to Fast Deployment File.
       Added Zombie_DSRSOAM1 to Fast Deployment File.
       Added Zombie_DSRSOAM2 to Fast Deployment File.
       Added Zombie_SDSSOAM1 to Fast Deployment File.
       Added Zombie_SDSSOAM2 to Fast Deployment File.
       Added Zombie_DSRDAMP1 to Fast Deployment File.
       Added Zombie_DSRDAMP2 to Fast Deployment File.
       Added Zombie_DSRIPFE1 to Fast Deployment File.
       Added Zombie_DSRIPFE2 to Fast Deployment File.
       Added Zombie_SDSDPSV1 to Fast Deployment File.
       Added Zombie_SDSDPSV2 to Fast Deployment File.
        Validating Fast Deployment File.......
Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml"
Configuration file validation successful.
Validation complete
       Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml
       SUCCESS: OPERATION SUCCESS!!
[admusr@5010441PMAC RMS]$
```

Procedure 1. Recovery Scenario 1

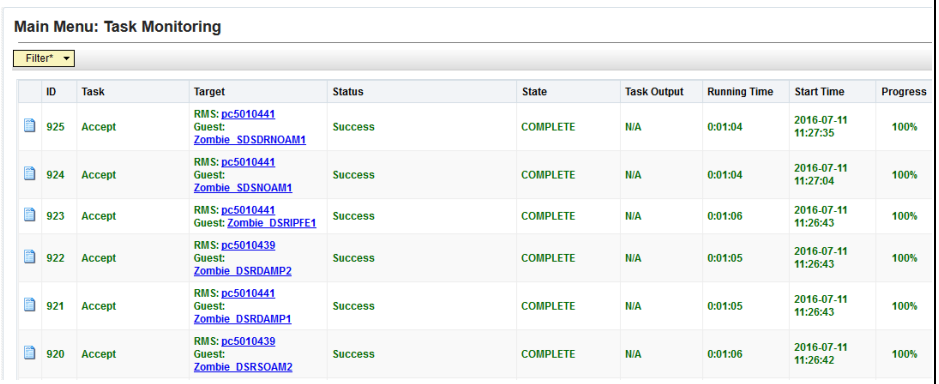
<table>
<tr>
<td>19. ☐</td>
<td>PMAC: Execute fast deployment</td>
<td>With the file generated from the config.sh script, execute the following command to start fast deployment:

<pre>$ screen
$ sudo fdconfig config --file=<fd_config.xml></pre>

Note: This is a long duration command. 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.</td>
</tr>
<tr>
<td>20. ☐</td>
<td>PMAC GUI: Monitor the configuration</td>
<td>1. If not already done, establish a GUI session on the PMAC server.
2. Navigate to Task Monitoring.



3. Monitor the configuration to completion:



Note: If a failure occurs with fdconfig, logs can be accessed in /var/TKLC/log/fdconfig/fdconfig.log file.

<pre>[admusr@melbourne-pmac-1 fdconfig]$ sudo fdconfig dumpsteps --
file=deploy_melbourne_20170329T202458_701b.fdcdb
Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb"
Here are the steps that were generated
--------------- begin ----------------
Dump of DB steps:
NUM PHS DLY INFRA ID SVRTYPE CMD ELEMENT PRE STATE TO BGTS COMMAND TEXT
----
1 1 0 pmac Fast_Deployment 0 21 0 Complete 300 0 Check PM&C is
available
2 1 0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet
3 1 0 pmac Fast_Deployment 0 3 melbourne_RMS3 1 Skipped 900 0 Add Rms
4 2 0 pmac Fast_Deployment 1</pre>
4. Restart the fdconfig after a failure has occurred and has been resolved:

<pre>$ sudo fdconfig restart --
file=deploy_melbourne_20170329T202458_701b.fdcdb</pre></td>
</tr>
</table>

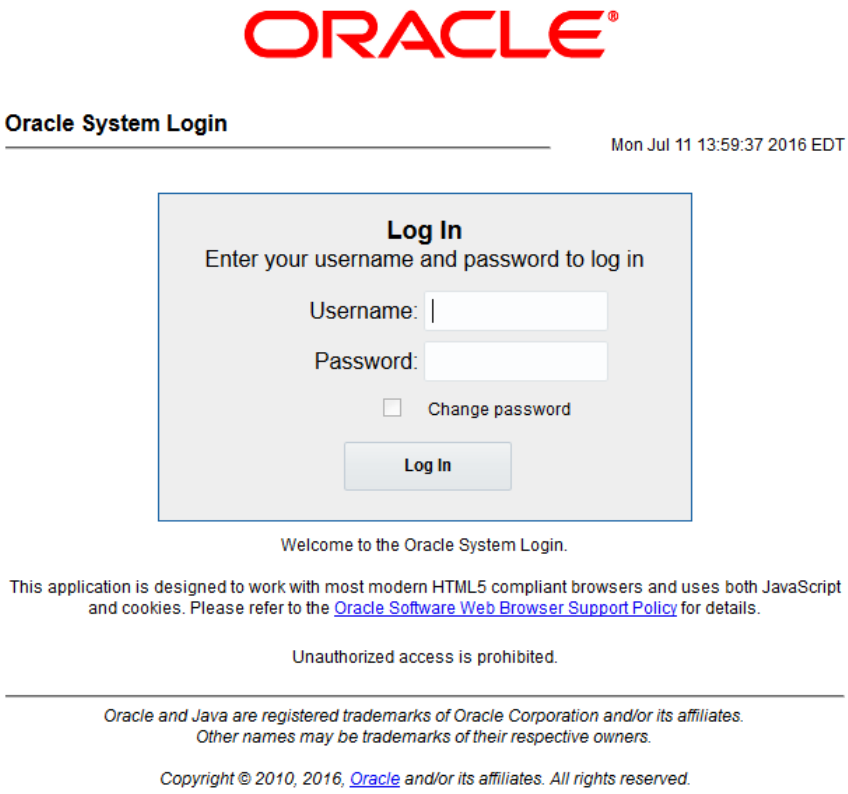
Procedure 1. Recovery Scenario 1

21. ☐	**PMAC**: Repeat for each rack mount server configuration file	Repeat steps 13. -20. for each rack mount server/configuration file, if required.

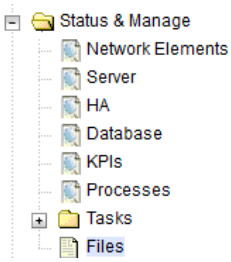
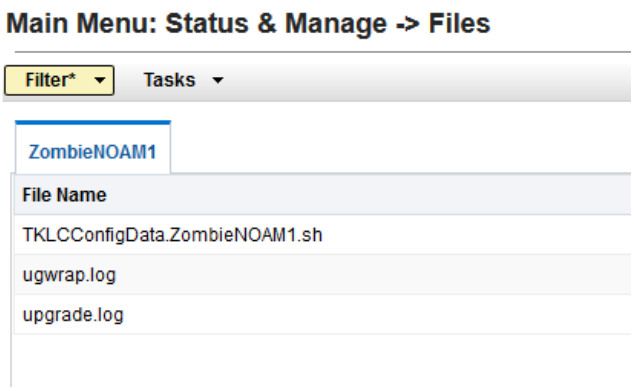
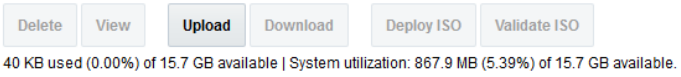
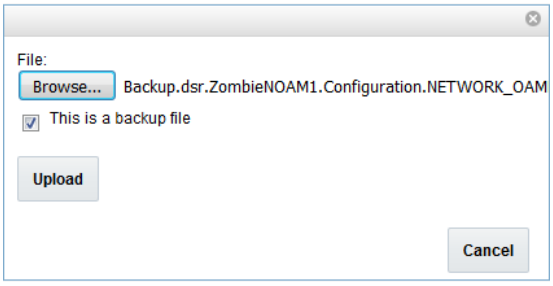
22. ☐	**PMAC**: Back up FDC file	1. Copy the updated fdc file to the fdc backup directory:
		`$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> /usr/TKLC/smac/etc/fdc/`
		2. Change permissions:
		`$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/<fdc_file>`

23. ☐	Perform CPU pinning	Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the **CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only)** procedure from reference [8].
24. ☐	Obtain latest database backup and network configuration data	1. Obtain the most recent database backup file from external backup sources (for example, file servers) or tape backup sources. 2. Obtain most recent **RADIUS shared secret encryption key** from the **DpiKf.bin.encr** file on external backup sources (only when the RADIUS key revocation MOP has been executed on the system). 3. 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.
25. ☐	Execute DSR installation procedure for the first NOAM	Verify the networking data for network elements. ***Notes*** • Use the backup copy of network configuration data and site surveys from step 2. • SDS disaster recovery actions can and should be worked simultaneously to allow faster recovery of the complete solution (that is, stale DB on DP servers do not receive updates until SDS-SOAM servers are recovered). The following steps accommodate both DSR and SDS disaster recovery steps. ***Important***: While creating the first NOAMs in this step, it is important that the server hostname is the same as one of the NOAM hostnames used prior to the disaster. **DSR**: 1. Configure the first NOAM server by executing the **Configure First NOAM NE and Server** procedure from reference [8]. 2. Configure the NOAM server group by executing the **Configure the NOAM Server Group** procedure from reference [8]. **SDS**: 1. Configure the first SDS NOAM server by executing **Configure First SDS NOAM NE and Server** procedure from reference [8]. 2. Configure the SDS NOAM server group by executing the **Configure the SDS NOAM Server Group** procedure from reference [8]. 3. Skip to step 31.

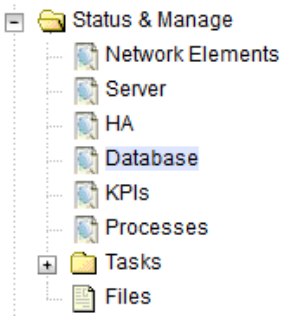
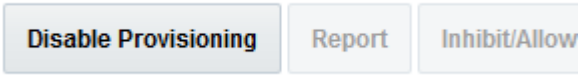
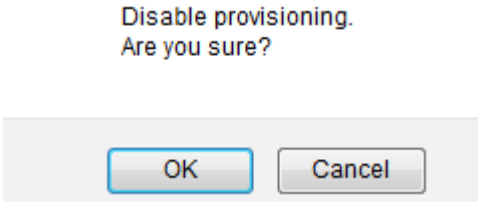
Procedure 1. Recovery Scenario 1

26. ☐	**NOAM GUI**: Login DSR only. If SDS, skip to step 31.	Log into the NOAM GUI as the **guiadmin** user. 

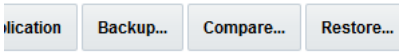
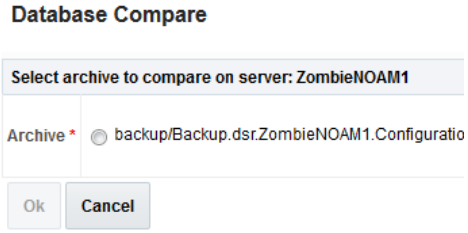
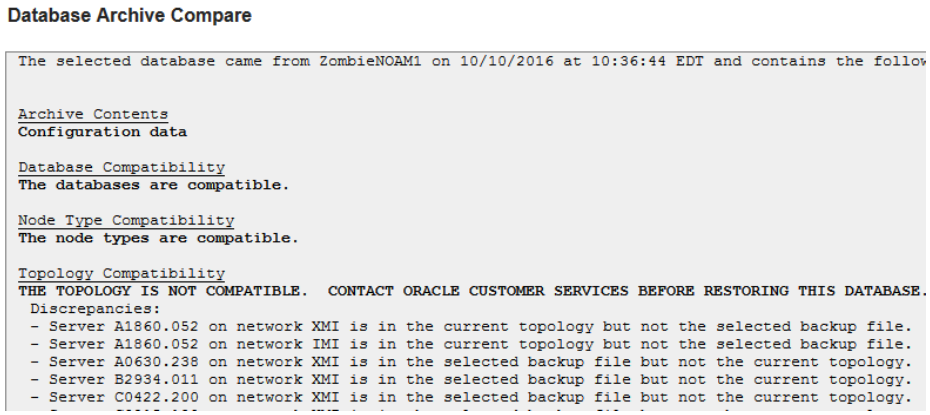
Procedure 1. Recovery Scenario 1

27. ☐	**NOAM GUI**: Upload the backup database file. DSR only. If SDS, skip to step 31.	1. Navigate to **Status & Manage > Files**.  2. Select the active NOAM server.  3. Click **Upload** and select the **NO Provisioning and Configuration** file backed up after initial installation and provisioning.  4. Click **Browse** and locate the backup file. ***Note:*** If there is no backup file, refer to Appendix L Backup Directory to create the backup directory. 5. Click **Open**. 6. Mark the **This is a backup file** checkbox. 7. Click **Upload**.  The file takes a few seconds to upload depending on the size of the backup data. The file is visible on the list of entries after the upload is complete.

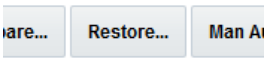
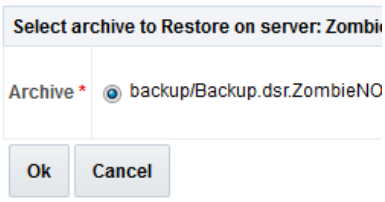
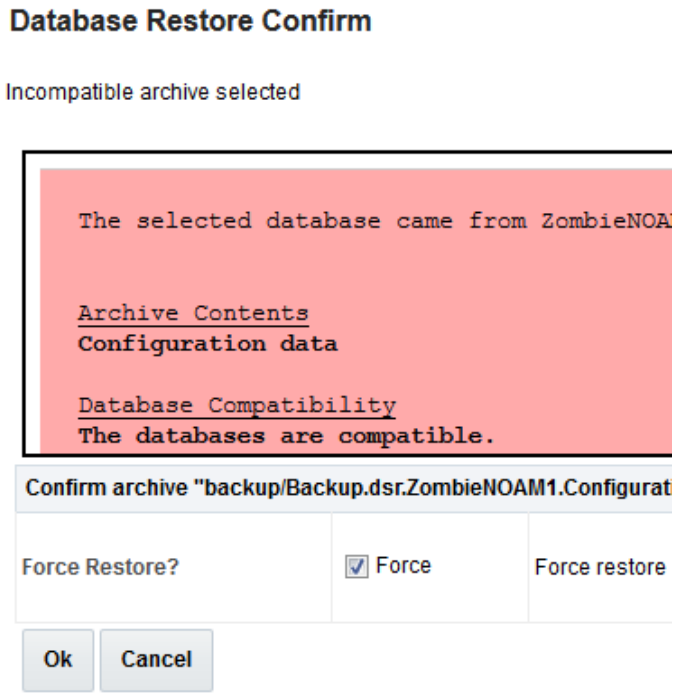
Procedure 1. Recovery Scenario 1

28. ☐	**NOAM GUI**: Disable provisioning. DSR only. If SDS, skip to step 31.	1. Navigate **to Status & Manage > Database**.  2. Click **Disable Provisioning**.  3. Click **OK** to disable Provisioning. 

Procedure 1. Recovery Scenario 1

29. ☐	**NOAM GUI**: Verify the archive contents and database compatibility. DSR only. If SDS, skip to step 31.	1. Select the **Active NOAM** server and click **Compare**.  2. Click the button for the restored database file uploaded as a part of step 27. 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

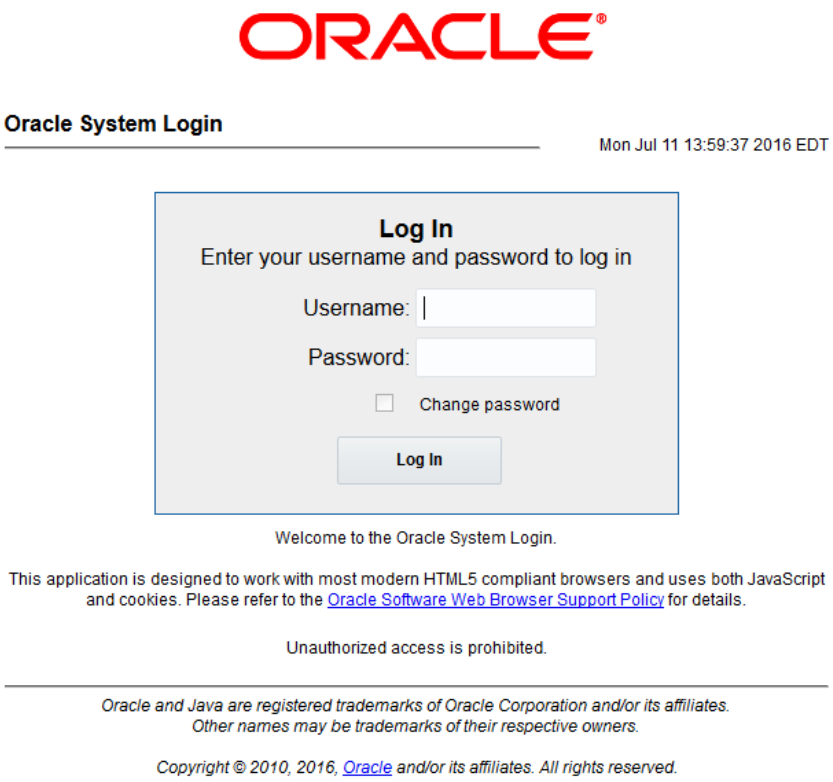
30. ☐	**Active NOAM**: Restore the database. DSR only. If SDS, skip to step 31.	1. From **Status & Manage > Database**. 2. Select the active NOAM server and click Restore.  3. Select the proper backup provisioning and configuration file.  4. Click OK. 5. If you get errors related to the warnings highlighted in the previous step, then it is expected. If no other errors display, then 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 the XMI NO GUI since the restored topology is old data. 6. Go to step 37.

Procedure 1. Recovery Scenario 1

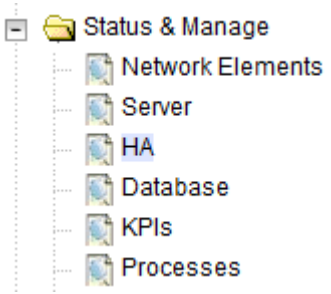
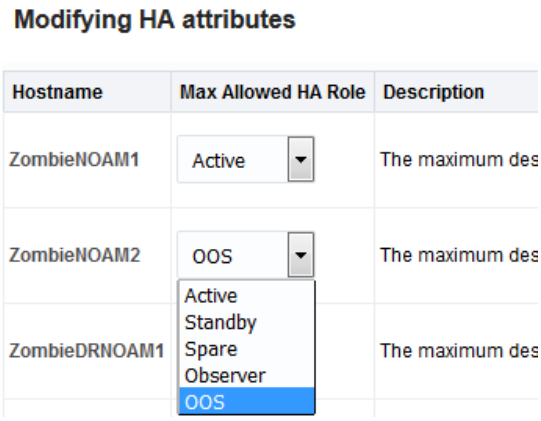
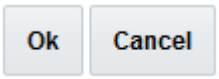
31. ☐	**SDS NOAM**: Transfer SDS configuration and provisioning backup database files.
	SDS only. If DSR, skip to step 37.
		Using the IP of the recovered SDS NOAM, transfer the uncompressed backup database files to the **/var/TKLC/db/filemgmt** directory.
		Linux:
		1. From the command line of a Linux machine, copy the configuration backup file to the SDS NOAM guest:
		`# scp <path_to_configuration_db_file> admusr@<SDS_NOAM_IP>:/var/TKLC/db/filemgmt`
		2. From the command line of a Linux machine, copy the provisioning backup file to the SDS NOAM guest:
		`# scp < path_to_provisioning_db _file> admusr@<SDS_NOAM_IP>:/var/TKLC/db/filemgmt`
		where **<path_to_db_file>** is the path to the backup database file on the local system and **<SDS_NOAM_IP>** is the recovered SDS NOAM IP address.
		Windows:
		Use WinSCP to copy the backup database files into the **/var/TKLC/db/filemgmt** directory. Refer to the **Using WinSCP** procedure in reference [9] to copy the backup image to the customer system.

32. ☐	**SDS NOAM**: Login. SDS only. If DSR, skip to step 37.	Establish an SSH session to the SDS active NOAM XMI IP address and login as **admusr**.
33. ☐	**SDS NOAM**: Stop running applications. SDS only. If DSR, skip to step 37.	Issue the following command to stop running applications. Leave database running: `$ sudo prod.stop --ignore-cap` ***Note:*** This step may take several minutes to complete.
34. ☐	**SDS NOAM**: Restore configuration database. SDS only. If DSR, skip to step 37.	Restore the configuration DB by executing the following command: `$ sudo idb.restore -n -t /var/TKLC/db/filemgmt -v <full path to configuration archive file name>`
35. ☐	**SDS NOAM**: Restore provisioning database. SDS only. If DSR, skip to step 37.	Refer to Appendix I Restore Provisioning Database to restore the provisioning database.
36. ☐	**SDS NOAM**: Start running applications. SDS only. If DSR, skip to step 37.	Start the SDS application by executing the following command: `$ sudo prod.start`

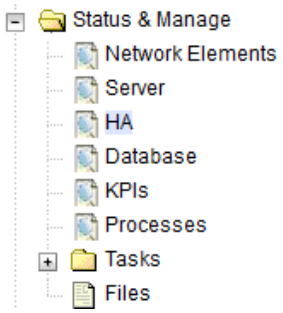
Procedure 1. Recovery Scenario 1

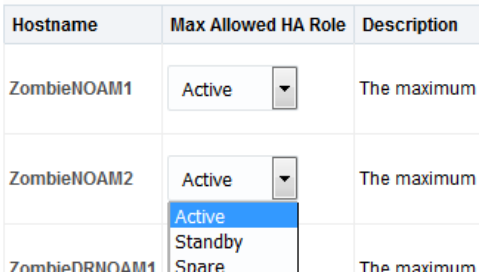
37. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user: 
38. ☐	**NOAM VIP GUI**: Monitor and confirm database restore	1. Wait for **5-10 minutes** for the system to stabilize with the new topology: 2. Monitor the Info tab for **Success**. This indicates the restore is complete and the system is stabilized. Ignore these alarms for NOAM and MP servers until all the servers are configured: • Alarms with Type Column as **REPL**, **COLL, HA** (with mate NOAM), **DB** (about Provisioning Manually Disabled). ***Notes***: • Do not pay attention to alarms until all the servers in the system are completely restored. • The Configuration and Maintenance information is in the same state it was when backed up during initial backup.

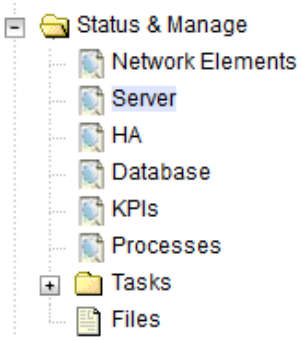
Procedure 1. Recovery Scenario 1

39. ☐	**Active NOAM**: Set failed servers to OOS	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Set the Max Allowed HA Role option to **OOS** for the failed servers.  4. Click **OK**. 
40. ☐	**NOAM VIP GUI**: Recover standby NOAM	Install the second NOAM server: **DSR**: Execute the **Configure the Second NOAM Server** procedure, steps 1 and 3-6, from reference [8]. **SDS**: Execute the **Configure the Second SDS NOAM Server** procedure, steps 1 and 3-6, from reference [8].
41. ☐	Install NetBackup client (optional)	If NetBackup is used, execute the **Install NetBackup Client (Optional)** procedure from reference [8].

Procedure 1. Recovery Scenario 1

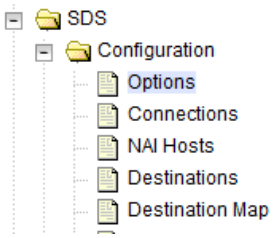
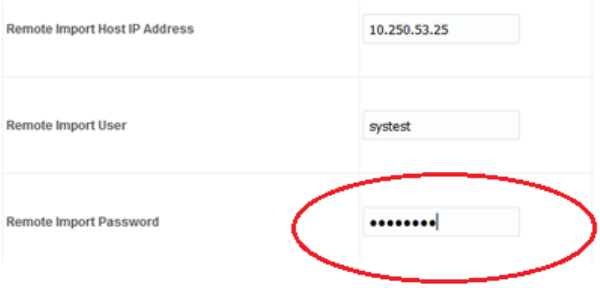
<table>
<tr>
<td>42. ☐</td>
<td>NOAM VIP GUI:
Set HA on standby NOAM</td>
<td>1. Navigate to Status & Manage > HA.
 

2. Click Edit.
3. Select the standby NOAM server and set it to Active.
Modifying HA attributes
 

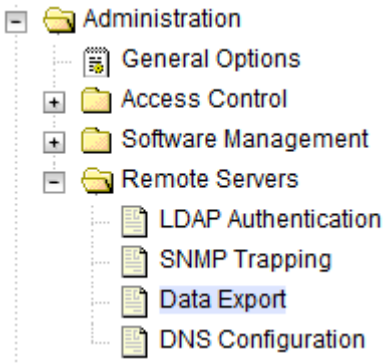
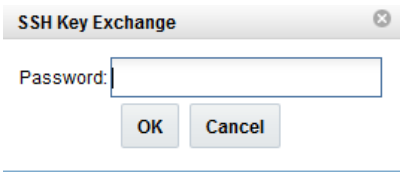
4. Click OK.</td>
</tr>
<tr>
<td>43. ☐</td>
<td>NOAM VIP GUI:
Restart DSR application</td>
<td>1. Navigate to Status & Manage > Server.
 

2. Select the recovered standby NOAM server and click Restart.
 
</td>
</tr>
<tr>
<td>44. ☐</td>
<td>Active NOAM:
Correct the recognized authority table</td>
<td>1. Establish an SSH session to the active NOAM and login as admusr.
2. Execute this command:
<pre>$ sudo top.setPrimary
- Using my cluster: A1789
- New Primary Timestamp: 11/09/15 20:21:43.418
- Updating A1789.022: <DSR_NOAM_B_hostname>
- Updating A1789.144: <DSR_NOAM_A_hostname></pre></td>
</tr>
</table>

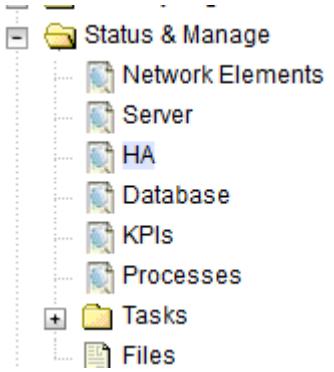
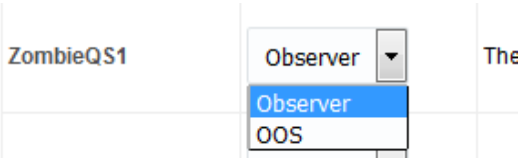
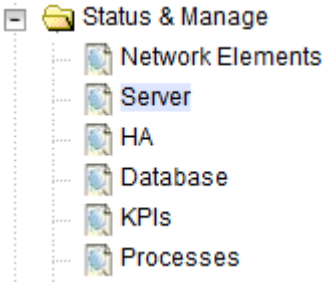
Procedure 1. Recovery Scenario 1

45. ☐	**NOAM VIP GUI**: Perform Keyexchange with remote import server. SDS only. If DSR, skip to step 47.	1. Navigate to **SDS > Configuration > Options**.  2. Unmark the **Remote Import Enabled** checkbox.  3. Click **Apply**. ***Note:*** Navigate to **SDS > Configuration > Options** again to clear the banner. 4. Enter the **Remote Import Password**.  5. Click **Apply**.  ***Note:*** Navigate to **SDS > Configuration > Options** again to clear the banner. 6. Mark the **Remote Import Enabled** checkbox. 
46. ☐	**NOAM VIP GUI**: Repeat for remote export server. SDS only. If DSR, skip to step 47.	Repeat step 45. for the remote export server.

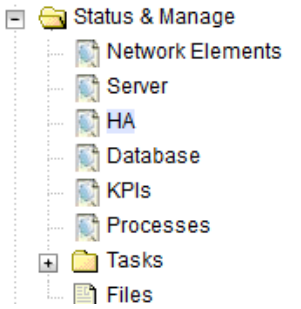
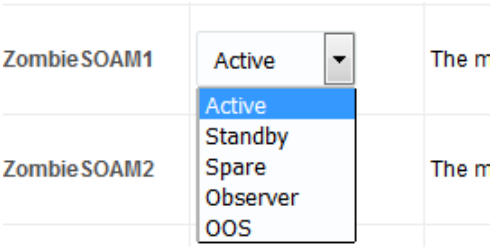
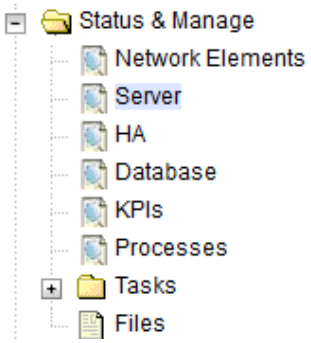
Procedure 1. Recovery Scenario 1

47. ☐	**NOAM VIP GUI**: Perform Keyexchange with export server	1. Navigate to **Administration > Remote Servers > Data Export**.  2. Click **SSH Key Exchange**.  3. Type the **Password** and click **OK**. 
48. ☐	**NOAM VIP GUI**: Recover query servers. SDS only. If DSR, skip to step 51.	Execute the **Configuring SDS Query Servers** procedure, steps 1 and 4-7, from reference [8].

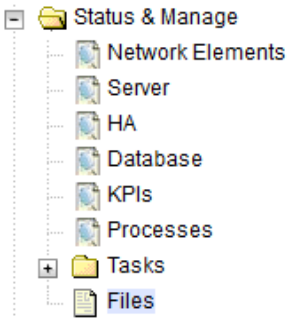
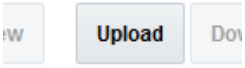
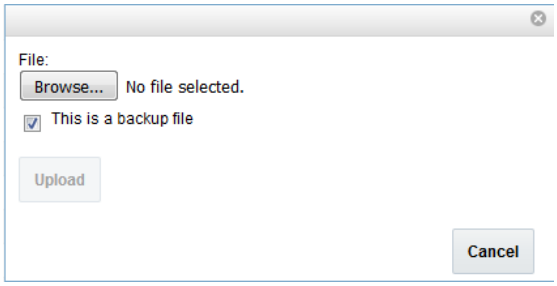
Procedure 1. Recovery Scenario 1

49. ☐	**SDS NOAM VIP GUI**: Set HA on query server. SDS only. If DSR, skip to step 51.	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Select the query server and select **Observer**.  4. Click **OK**.
50. ☐	**SDS NOAM VIP GUI**: Restart SDS application. SDS only. If DSR, skip to step 51.	1. Navigate to **Status & Manage > Server**.  2. Select the recovered query server and click **Restart**. 
51. ☐	**NOAM VIP GUI**: Stop replication to the C-level servers of this site. DSR only. If SDS, skip to step next step. 	**Warning** Before continuing this procedure, replication to C-level servers **MUST** be inhibited at the SOAM site being recovered. 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.

Procedure 1. Recovery Scenario 1

52. ☐	**NOAM VIP GUI**: Recover active SOAM server	Install the SOAM servers. **DSR**: Execute the **Configure the SOAM Servers** procedure, steps 1-3 and 5-9, from reference [8]. ***Note:*** If you are using NetBackup, also execute step 12. **SDS**: Execute the **Configure the SDS DP SOAM Servers** procedure, steps 1-3 and 5-8, from reference [8].
53. ☐	**NOAM VIP GUI**: Set HA on the SOAM server	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Select the SOAM server and set it to **Active**.  4. Click **OK**.
54. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered NOAM server and click **Restart**. 

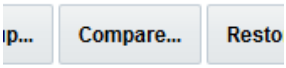
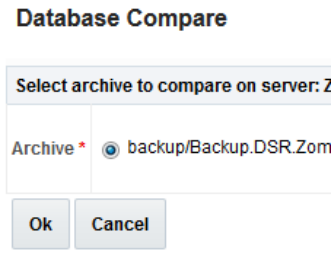
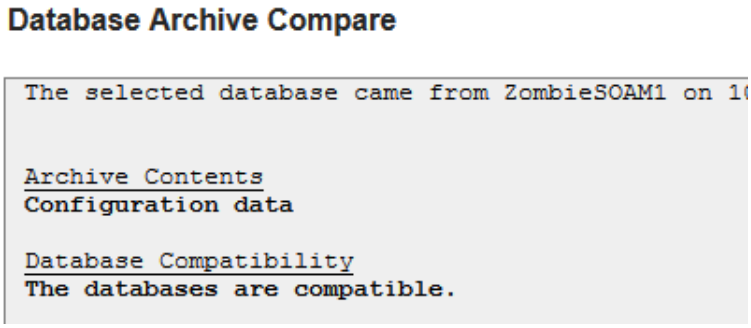
Procedure 1. Recovery Scenario 1

55. ☐	**NOAM VIP GUI**: Upload the backup SOAM database file. DSR only. If SDS, skip to step 60.	1. Navigate to **Status & 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. Mark the **This is a backup file** checkbox. 5. Click **Open**. 6. Click **Upload**.  The file takes a few seconds to upload depending on the size of the backup data and displays on the list of entries when it has completed the upload.

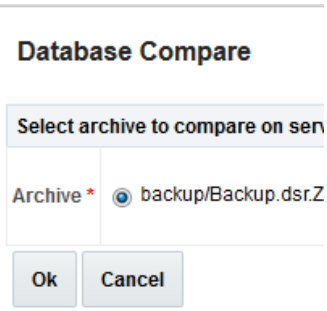
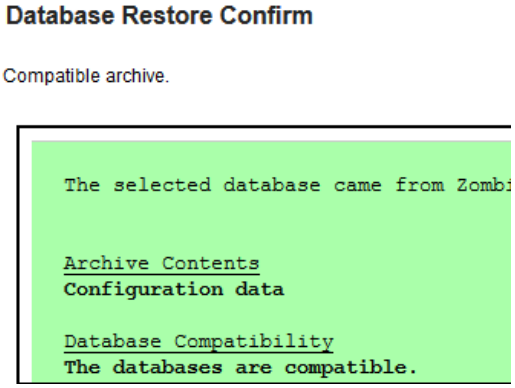
Procedure 1. Recovery Scenario 1

56. ☐	**Recovered SOAM GUI**: Login. DSR only. If SDS, skip to step 60.	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

57. ☐	**Recovered SOAM GUI**: Verify the archive contents and database compatibility. DSR only. If SDS, skip to step 60.	1. Navigate to **Status & Manage > Database**. 2. Select the **Active SOAM** server and click **Compare**.  3. Click the button for the restored database file uploaded as a part of step 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.

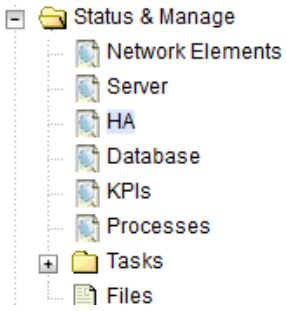
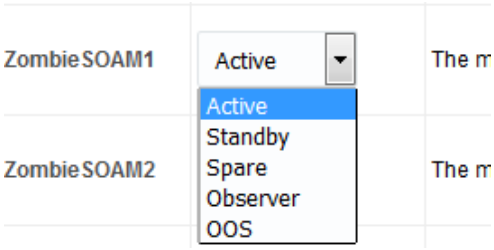
Procedure 1. Recovery Scenario 1

58. ☐	**Recovered SOAM GUI**: Restore the database. DSR only. If SDS, skip to step 60.	1. Select the **Active SOAM** server and click **Restore**. 2. Select the backup provisioning and configuration file.  3. Click **OK**.  4. If the Node Type Compatibility error displays, it is expected. If no other errors display, mark the **Force** checkbox and click **OK** to proceed with the DB restore. ***Notes***: • After the restore has started, the user is logged out of XMI SOAM GUI since the restored topology is old data. • If the spare SOAM is in another network and is unreachable, the database restore cannot be done. **Workaround**: If the spare SOAM is unreachable and ping (from recovered SOAM server to spare SOAM server) hangs (as evidenced by **ps -ef | grep ping** showing the same ping process and its child for more than 10 seconds), then kill the hung ping processes and the restore proceeds.
59. ☐	**Recovered SOAM GUI**: Monitor and confirm database restoral. DSR only. If SDS, skip to step 60.	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. ***Notes***: • Do not pay attention to alarms until all the servers in the system are completely restored. • The Configuration and Maintenance information is in the same state it was when backed up during initial backup.

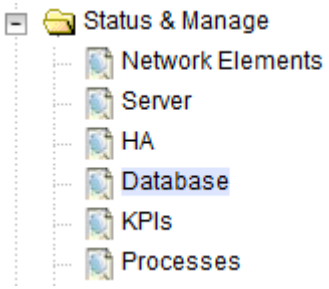
Procedure 1. Recovery Scenario 1

60. ☐	**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: 
61. ☐	**NOAM VIP GUI**: Recover the remaining SOAM servers (standby, spare)	**DSR**: Execute the **Configure the SOAM Servers** procedure, steps 1-3 and 5-9, from reference [8]. ***Note:*** If you are using NetBackup, also execute step 12. **SDS**: Execute the **Configure the SDS DP SOAM Servers** procedure, steps 1-3 and 5-8, from reference [8].

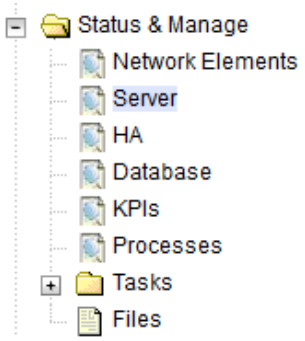
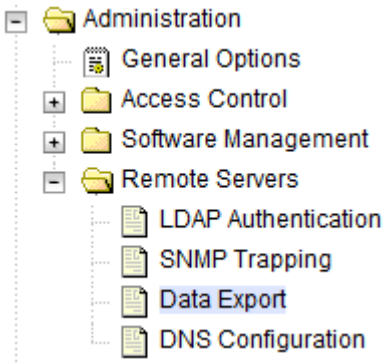
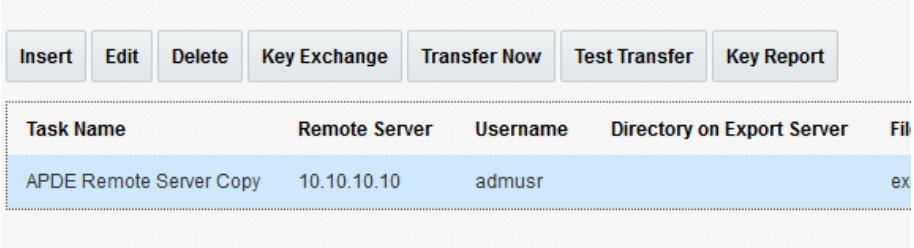
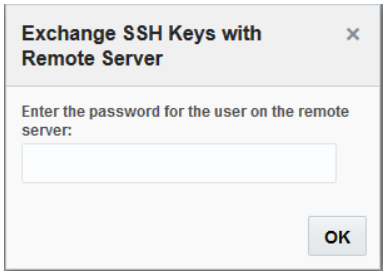
Procedure 1. Recovery Scenario 1

62. ☐	**NOAM VIP GUI**: Set HA on SOAM server	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Select the SOAM server and set it to **Active**.  4. Click **OK**.

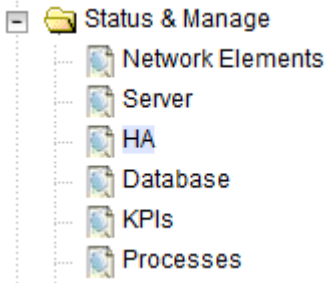
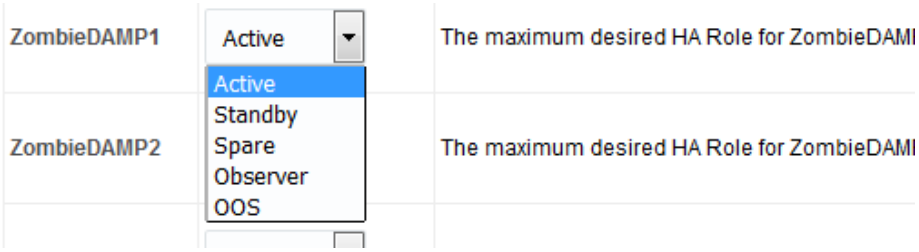
Procedure 1. Recovery Scenario 1

63. ☐	**NOAM VIP GUI**: Start replication on working C-level servers. DSR only. If SDS, skip to next step.	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 & 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)** — Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only • 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) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only 3. Verify the replication on all the working servers is allowed. This can be done by examining the Repl Status table. **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

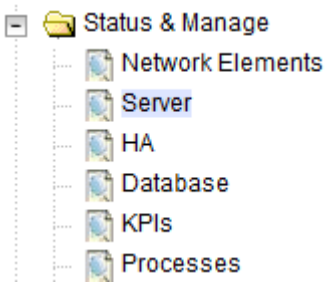
Procedure 1. Recovery Scenario 1

64. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**. 
65. ☐	**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**. 

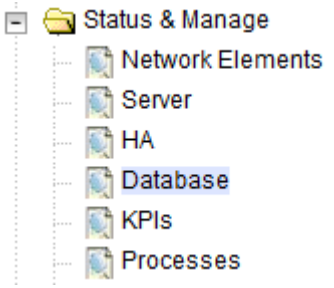
Procedure 1. Recovery Scenario 1

66. ☐	Activate PCA feature. DSR only	If you have PCA installed in the system being recovered, re-activate PCA by executing the **PCA Activation on Entire Network** procedure on the recovered NOAM server from [7]. ***Note:*** If not all SOAM sites are recovered at this point, then repeat the activation for each "new" SOAM site that comes online.
67. ☐	**NOAM VIP GUI**: Recover the C-level server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs	**DSR**: Execute the **Configure the MP Servers** procedure, steps 1 and 9-13, from reference [8]. ***Note:*** Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. **SDS** (Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only): Execute the **Configure the SDS DP Servers** procedure, steps 1 and 5-8, from reference [8]. Repeat this step for any remaining failed MP servers.
68. ☐	**NOAM VIP GUI**: Set HA on all C-level servers	1. Navigate to **Status & Manage -> HA**.  2. Click **Edit**. 3. For each recovered C-Level with a Max Allowed HA Role set to **OOS**, set it to **Active**.  4. Click **OK**.

Procedure 1. Recovery Scenario 1

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

Procedure 1. Recovery Scenario 1

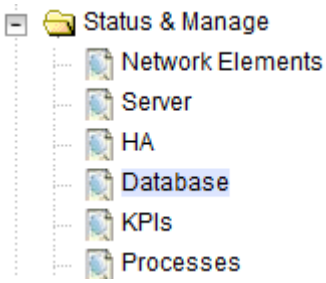
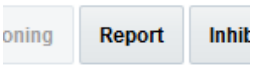
<table>
<tr>
<td>70. ☐</td>
<td>NOAM VIP GUI: Start replication on all C-Level servers.
DSR only. If SDS, then skip to next step.</td>
<td>Un-Inhibit (start) replication to the ALL C-level servers.
1. Navigate to Status & Manage > Database.
 

2. If the Repl Status is set to Inhibited, click Allow Replication using this order:
• Active NOAMP Server
• Standby NOAMP Server
• Active SOAM Server
• Standby SOAM Server
• Spare SOAM Server (if applicable) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only)
• Active DR NOAM Server
• Standby DR NOAM Server
• MP/IPFE Servers
• SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only
3. Verify the replication on all servers is allowed. This can be done by checking the Repl Status.
<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>71. ☐</td>
<td>Active NOAM: Perform keyexchange between the active-NOAM and recovered servers</td>
<td>1. Establish an SSH session to the active NOAM and login as admusr.
2. Perform a keyexchange from the active NOAM to each recovered server:

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


Note: If an export server is configured, perform this step.</td>
</tr>
</table>

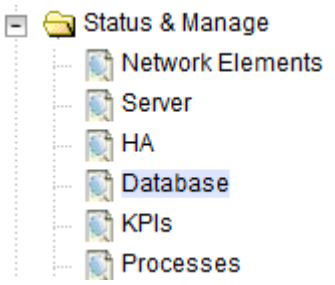
Procedure 1. Recovery Scenario 1

72. ☐	**Active NOAM**: Activate optional features. DSR only. If SDS, then skip to next step.	Establish an SSH session to the active NOAM and login as **admusr**. **Note for PCA Feature Activation:** If you have PCA installed in the system being recovered, re-activate the PCA by executing the **PCA Activation on Entire Server** procedure on the recovered NOAM server from [6]. ***Notes***: • If not all SOAM sites are recovered at this point, then repeat the activation for each "new" SOAM site that comes online. • If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature. Refer to section 1.5 Optional Features to activate any features that were previously activated.
73. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status & Manage > Database**.  2. Select the active NOAM server and click **Report**.  The following screen displays: **Main Menu: Status & Manage -> Database [Report]** dsr Database Status Report Report Generated: Tue Oct 11 13:24:26 2016 EDT From: Active Network OAM&P on host ZombieNOAM1 Report Version: 8.0.0.0.0-80.9.0 User: guiadmin General Hostname : ZombieNOAM1 Database Birthday : 2016-07-11 11:21:50 EDT Appworks Database Version : 6.0 Application Database Version : Capacities and Utilization Disk Utilization 8.4%: 585M used of 7.0G total, 6.0G available Memory Utilization 0.0%: used of total, 0M available 3. Click **Save** and save the report to your local machine.

Procedure 1. Recovery Scenario 1

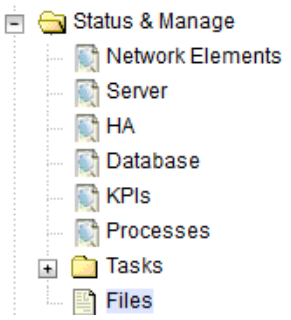
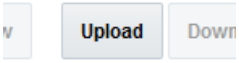
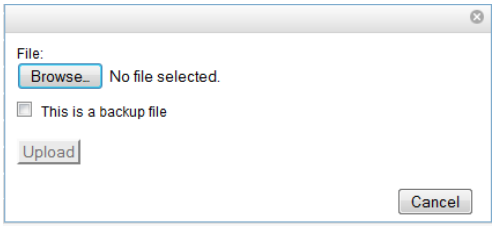
74. ☐	**Active NOAM**: Verify replication between servers	1. Log into the active NOAM as **admusr** using SSH terminal.
		2. Execute this command:
		`$ sudo irepstat –m`
		Example output:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`Oahu-DAMP-1 -- Active`
		`  BC From Oahu-SOAM-2  Active   0   0.50 ^0.15%cpu 25B/s  A=me`
		`  CC To   Oahu-DAMP-2  Active   0   0.10  0.14%cpu 25B/s  A=me`
		`Oahu-DAMP-2 -- Stby`
		`  BC From Oahu-SOAM-2  Active   0   0.50 ^0.11%cpu 31B/s  A=C3642.212`
		`  CC From Oahu-DAMP-1  Active   0   0.10 ^0.14 1.16%cpu 31B/s A=C3642.212`
		`Oahu-IPFE-1 -- Active`
		`  BC From Oahu-SOAM-2  Active   0   0.50 ^0.03%cpu 24B/s  A=C3642.212`
		`Oahu-IPFE-2 -- Active`
		`  BC From Oahu-SOAM-2  Active   0   0.50 ^0.03%cpu 28B/s  A=C3642.212`
		`Oahu-NOAM-1 -- Stby`
		`  AA From Oahu-NOAM-2  Active   0   0.25 ^0.03%cpu 23B/s`
		`Oahu-NOAM-2 -- Active`
		`  AA To   Oahu-NOAM-1  Active   0   0.25 1%R 0.04%cpu 61B/s`
		`  AB To   Oahu-SOAM-2  Active   0   0.50 1%R 0.05%cpu 75B/s`
		`Oahu-SOAM-1 -- Stby`
		`  BB From Oahu-SOAM-2  Active   0   0.50 ^0.03%cpu 27B/s`
		`Oahu-SOAM-2 -- Active`
		`  AB From Oahu-NOAM-2  Active   0   0.50 ^0.03%cpu 24B/s`
		`  BB To   Oahu-SOAM-1  Active   0   0.50 1%R 0.04%cpu 32B/s`
		`  BC To   Oahu-IPFE-1  Active   0   0.50 1%R 0.04%cpu 21B/s`
		`  BC To   Oahu-SS7MP-2 Active   0   0.50 1%R 0.04%cpu 21B/s`
		`irepstat ( 40 lines) (h)elp (m)erged`

Procedure 1. Recovery Scenario 1

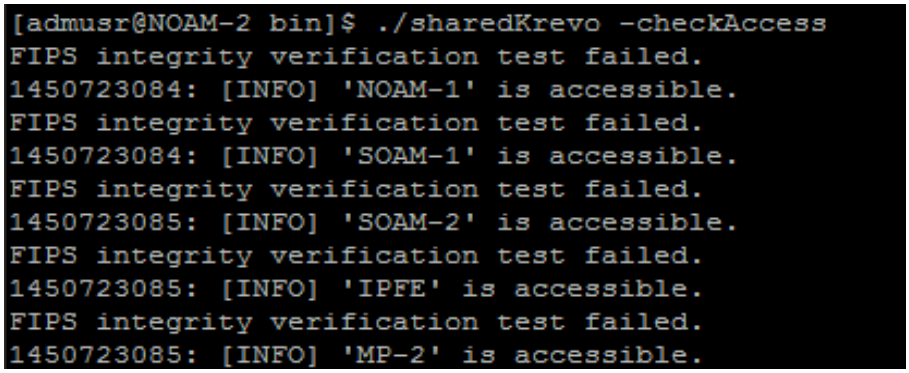
75. ☐	**NOAM VIP GUI**: Verify the database states	1. Navigate to **Status & Manager > Database**.  2. Verify the OAM Max HA Role is either **Active** or **Standby** for NOAM and SOAM; Application Max HA Role for MPs is **Active**; and status is **Normal**.

Network Element	Server	Role	OAM Max HA Role
ZombieDRNOAM	ZombieDRNOAM1	Network OAM&P	Active
ZombieNOAM	ZombieNOAM2	Network OAM&P	Standby
ZombieSOAM	ZombieSOAM2	System OAM	N/A
ZombieNOAM	ZombieNOAM1	Network OAM&P	Active
ZombieSOAM	ZombieSOAM1	System OAM	Active
ZombieDRNOAM	ZombieDRNOAM2	Network OAM&P	Standby
ZombieSOAM	ZombieDAMP2	MP	Standby
ZombieSOAM	ZombieSS7MP2	MP	Active
ZombieSOAM	ZombieSS7MP1	MP	Active
ZombieSOAM	ZombieIPFE1	MP	Active
ZombieSOAM	ZombieIPFE2	MP	Active

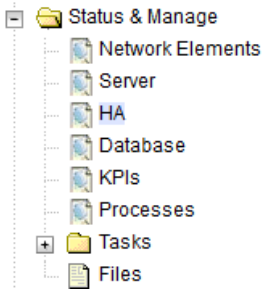
Procedure 1. Recovery Scenario 1

76. ☐	**NOAM VIP GUI**: Upload the backed up RADIUS key file (RADIUS only). DSR only. If SDS, skip to the next step.	If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator. 1. Navigate to **Status & Manage > Files**.  2. Select the active NOAM server tab. Click **Upload** and select the **RADIUS shared secret encryption key** file backed up after initial installation and provisioning or after key revocation execution.  3. Click **Browse**. 4. Locate the **DpiKf.bin.encr** file. 5. Click **Upload**.  The file takes a few seconds to upload depending on the size of the file. The file is visible on the list of entries after the upload is complete. ***Note:*** This file should be deleted from the operator's local servers as soon as key file is uploaded to the active NOAM server.

Procedure 1. Recovery Scenario 1

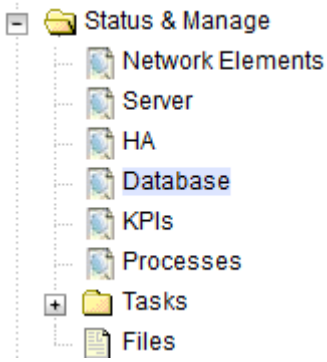
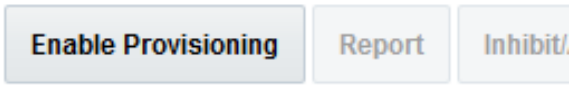
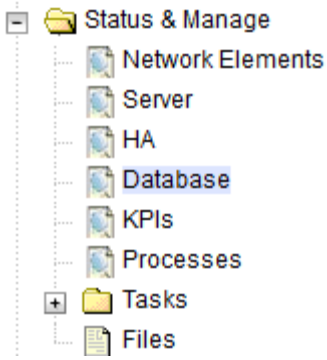
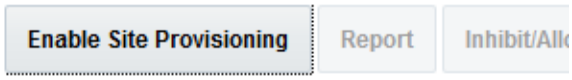
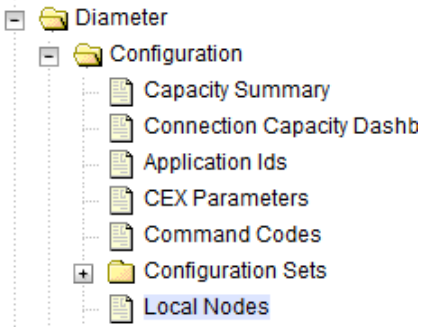
77. ☐	**NOAM VIP**: Copy and distribute RADIUS key file on active NOAM (RADIUS only) — Part 1	If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.
		1. Log into the active NOAM VIP as **admusr** user using SSH terminal.
		2. Copy the key file:
		`$ cd /usr/TKLC/dpi/bin`
		`$ ./sharedKrevo -decr`
		`$ sudo rm /var/TKLC/db/filemgmt/<backed up key file name>`
		3. Make sure all servers in the topology are accessible.
		`$ ./sharedKrevo –checkAccess`
		 
		[admusr@NOAM-2 bin]$ ./sharedKrevo -checkAccess
		FIPS integrity verification test failed.
		1450723084: [INFO] 'NOAM-1' is accessible.
		FIPS integrity verification test failed.
		1450723084: [INFO] 'SOAM-1' is accessible.
		FIPS integrity verification test failed.
		1450723085: [INFO] 'SOAM-2' is accessible.
		FIPS integrity verification test failed.
		1450723085: [INFO] 'IPFE' is accessible.
		FIPS integrity verification test failed.
		1450723085: [INFO] 'MP-2' is accessible.
		Note: If all the servers are not accessible, then contact My Oracle Support (MOS).

Procedure 1. Recovery Scenario 1

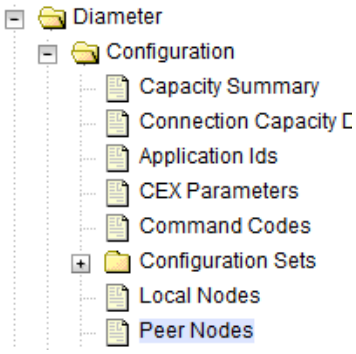
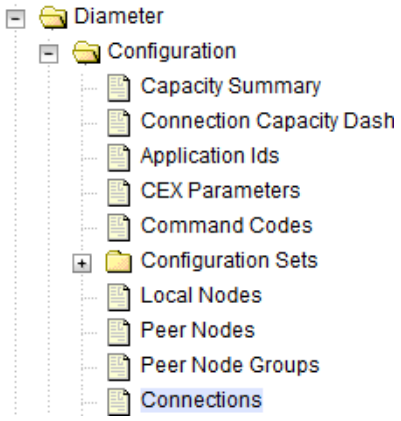
<table>
<tr>
<td>78. ☐</td>
<td>NOAM VIP: Copy and distribute the RADIUS key file on active NOAM (RADIUS only) — Part 2</td>
<td>
Distribute key file to all the servers in the topology:
<pre>$ ./sharedKrevo -synchronize
$ ./sharedKrevo -updateData</pre>
Example output:
<pre>1450723210: [INFO] Key file on Active NOAM and IPFE are same.
1450723210: [INFO] NO NEED to sync key file to IPFE.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723210: [INFO] Key file on Active NOAM and MP-2 are same.
1450723210: [INFO] NO NEED to sync key file to MP-2.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723211: [INFO] Key file on Active NOAM and MP-1 are same.
1450723211: [INFO] NO NEED to sync key file to MP-1.
[admusr@NOAM-2 bin]$ ./sharedKrevo -updateData
1450723226: [INFO] Updating data on server 'NOAM-2'
1450723227: [INFO] Data updated to 'NOAM-2'
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723228: [INFO] Updating data on server 'SOAM-2'
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723230: [INFO] 1 rows updated on 'SOAM-2'...
1450723230: [INFO] Data updated to 'SOAM-2'
[admusr@NOAM-2 bin]$</pre>
Note: For any errors refer My Oracle Support (MOS).
</td>
</tr>
<tr>
<td>79. ☐</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>

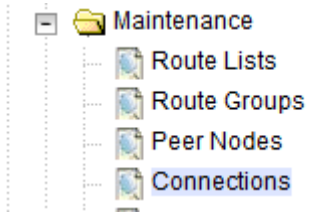
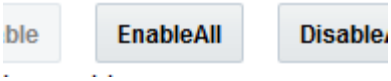
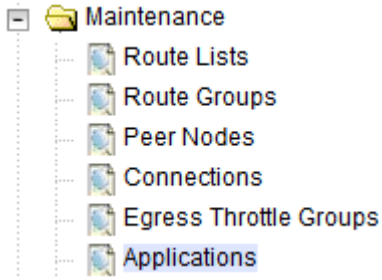
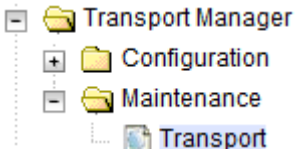
Procedure 1. Recovery Scenario 1

80. ☐	**NOAM GUI**: Enable provisioning	1. Navigate to **Status & Manage > Database**.  2. Click **Enable Provisioning**.  3. Click **OK**.
81. ☐	**SOAM GUI**: Enable site provisioning. DSR only. If SDS, then skip to step 91.	1. Navigate to **Status & Manage > Database**.  2. Click **Enable Site Provisioning**.  3. Click **OK**.
82. ☐	**SOAM VIP GUI**: Verify the local node information. DSR only. If SDS, then skip to step 91.	1. Navigate to **Diameter > Configuration > Local Node**.  2. Verify all the local nodes are shown.

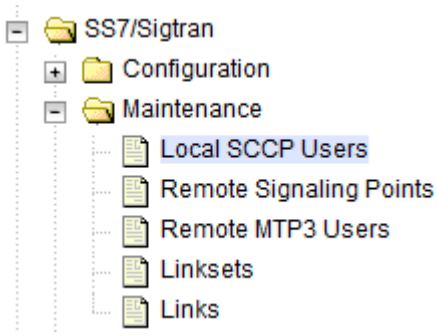
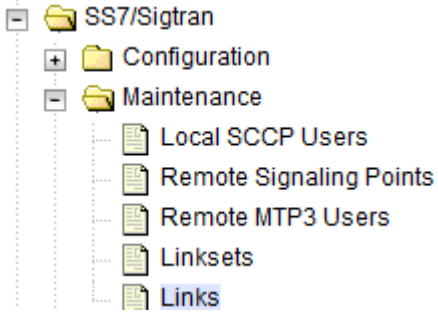
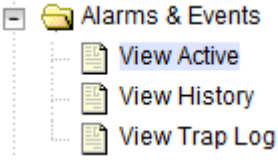
Procedure 1. Recovery Scenario 1

83. ☐	**SOAM VIP GUI**: Verify the peer node information. DSR only. If SDS, then skip to step 91.	1. Navigate to **Diameter > Configuration > Peer Node**.  2. Verify all the peer nodes are shown.
84. ☐	**SOAM VIP GUI**: Verify the connections information. DSR only. If SDS, then skip to step 91.	1. Navigate to **Diameter > Configuration > Connections**.  2. Verify all the connections are shown.
85. ☐	**MP Servers**: Disable SCTP Auth Flag. DSR only. If SDS, then skip to step 91.	For SCTP connections without DTLS enabled, refer to the **Enable/Disable DTLS (SCTP Diameter Connections Only)** section in reference [8]. Execute this procedure on all failed MP servers.

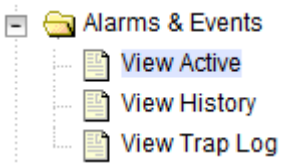
Procedure 1. Recovery Scenario 1

86. ☐	**SOAM VIP GUI**: Enable connections, if needed. DSR only. If SDS, then skip to step 91.	1. Navigate to **Diameter > Maintenance > Connections**.  2. Select each connection and click **Enable**. Alternatively, 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
87. ☐	**SOAM VIP GUI**: Enable optional features. DSR only. If SDS, then skip to step 91.	1. Navigate to **Diameter > Maintenance > Applications**.  2. Select the optional feature application configured in step 72. 3. Click **Enable**. 
88. ☐	**SOAM VIP GUI**: Re-enable transports, if needed. DSR only. If SDS, then skip to step 91.	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

89. ☐	**SOAM VIP GUI**: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 91.	1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.  2. Click the **Enable** button corresponding to MAPIWF Application Name. 3. Verify the SSN Status is **Enabled**.
90. ☐	**SOAM VIP GUI**: Re-enable links, if needed. DSR only. If SDS, then skip to step 91.	1. Navigate to **SS7/Sigtran > Maintenance > Links**.  2. Click **Enable** for each link.  3. Verify the Operational Status for each link is **Up**.
91. ☐	**SOAM VIP GUI**: Examine all alarms	1. Navigate to **Alarms & Events > View Active**.  2. Examine all active alarms and refer to the on-line help on how to address them. If needed, contact My Oracle Support (MOS).

Procedure 1. Recovery Scenario 1

92. ☐	**NOAM 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).
93. ☐	Restore GUI usernames and passwords	If applicable, execute the section 5 **Resolve User Credential Issues after Database Restore** procedure to recover the user and group information restored.
94. ☐	Back up and archive all the databases from the recovered system	Execute the **DSR Database Backup** procedure to back up the configuration databases.
95. ☐	Recover IDIH, if configured	If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.
96. ☐	SNMP workaround	Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases: 1. If SNMP is not configured in DSR/SDS. 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 will recover the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure; detailed steps are in Procedure 2. The major activities are summarized as follows:

- Recover **standby NOAM** server (if needed) by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover **Query Server** (if needed) by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover **active SOAM** server by recovering base hardware, software, and database
  - Recover the base hardware

  - Recover the software
  - Recover the database
- Recover any failed **SOAM and MP/DP** 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/DP servers.
- Recover IDIH if necessary

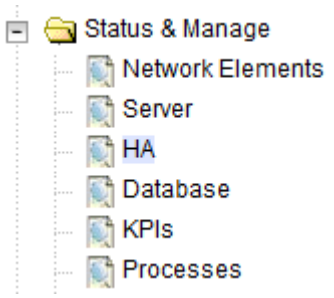
Procedure 2. Recovery Scenario 2

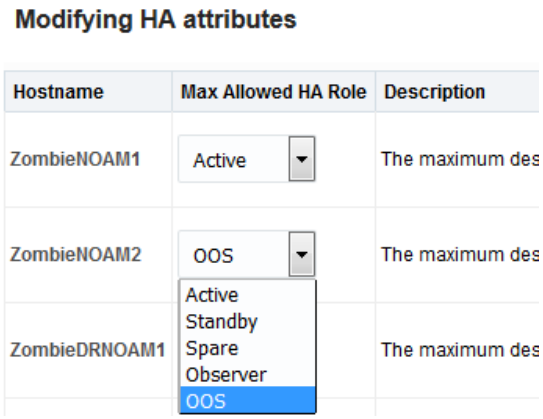
S T E P #	This procedure performs recovery if at least one NOAM server is available, but all SOAM servers in a site have failed. This includes any SOAM server that is in another location. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Workarounds	Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist. Refer to Appendix K 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.

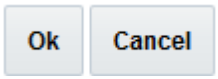
Procedure 2. Recovery Scenario 2

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 & Manage > HA.


2. Click Edit.


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


</td>
</tr>
<tr>
<td>5. ☐</td>
<td>Replace failed equipment</td>
<td>Work with the hardware vendor to replace the failed equipment.</td>
</tr>
<tr>
<td>6. ☐</td>
<td>Recover PMAC TVOE Host: (if required) Configure BIOS settings and update firmware</td>
<td>
1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:

HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings
Oracle X5-2/Netra X5-2/X6-2/X7-2: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings
HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings

2. Verify and/or upgrade server firmware by executing the Upgrade Rack Mount Server Firmware procedure from reference [8].
</td>
</tr>
</table>

Procedure 2. Recovery Scenario 2

7. ☐	**Recover PMAC and PMAC TVOE Host**: Backups available	If PMAC is located on the failed rack mount server(s), execute this step; otherwise, skip to step 11. This step assumes TVOE and PMAC backups are available. If backups are NOT available, skip this step. 1. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers. 2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup. 3. Proceed to step 11.
8. ☐	**Recover PMAC and PMAC TVOE Host**: 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 these procedures from reference [8]: • **Install and Configure TVOE on First RMS (PMAC Host)** • **Install PMAC** • **Initialize the PMAC Application** 2. Proceed to next step.
9. ☐	**Configure PMAC**: No Backup	If PMAC backup was **NOT** restored in step 7. , execute this step; otherwise, skip this step. Execute these procedures from reference [8]: • **Configure PMAC Server (NetBackup Only)** • **Add RMS to the PMAC Inventory**
10. ☐	Install/Configure additional rack mount servers	This step assumes TVOE backups are available on any additional rack mount servers; otherwise, skip this step. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on additional rack mount servers.
11. ☐	Install/Configure additional rack mount servers	If TVOE backups were NOT performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step. 1. Execute these procedures from reference [8]: • Install TVOE on Additional Rack Mount Servers • Configure TVOE on Additional Rack Mount Servers 2. Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]: • **HP DL380 Gen8**: Configure HP Gen 8 Server BIOS Settings • **Oracle X5-2/Netra X5-2/X6-2/X7-2**: Configure Oracle X5-2/Netra X5-2/X6-2/X7-2 Server BIOS Settings • **HP DL380 Gen9**: Configure HP Gen9 Server BIOS Settings

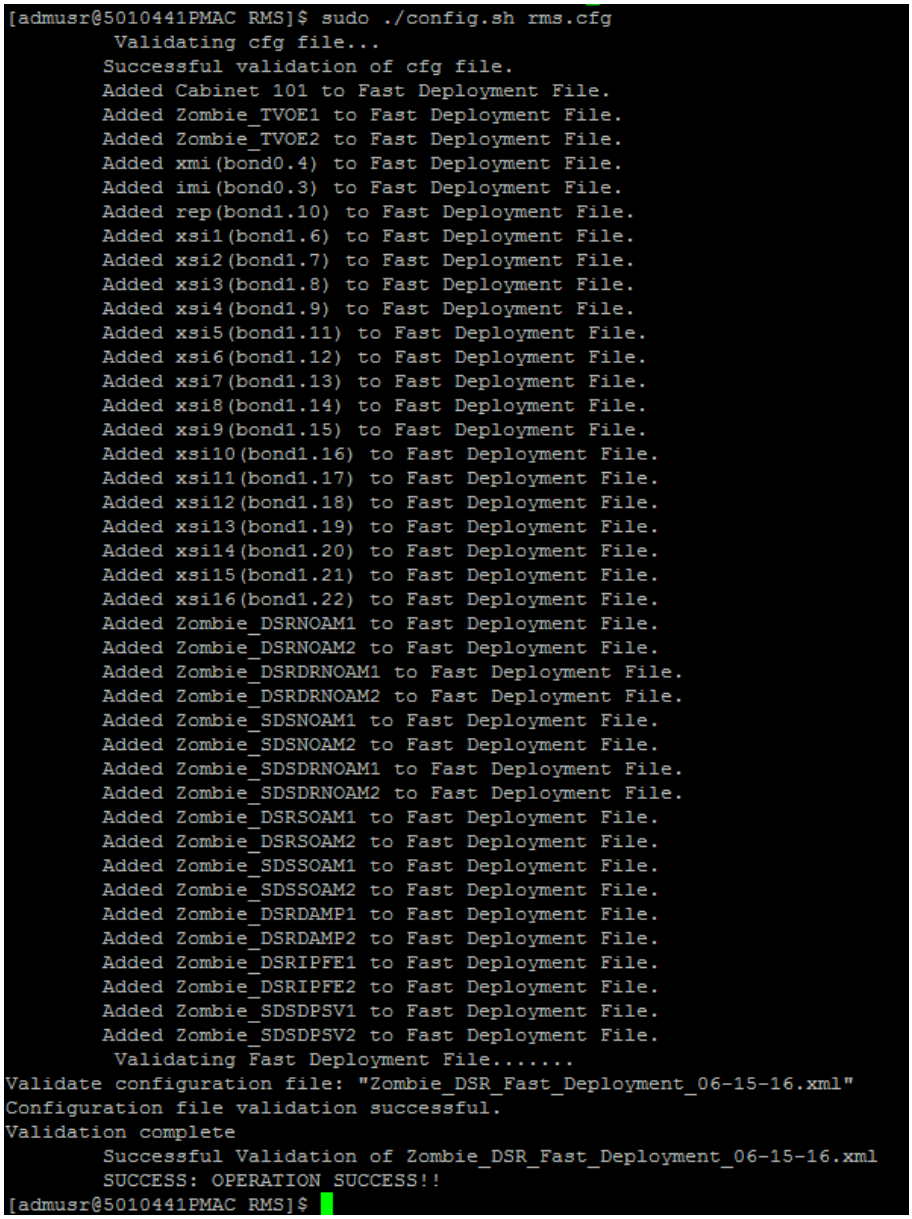
Procedure 2. Recovery Scenario 2

12. ☐	Determine VM placement and socket pinning (Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only)	HP DL380 GEN 8, **skip this step**. Determine VM placement and pinning by following section 3.1, item 14.
13. ☐	Deploy redundant PMAC	If the redundant PMAC is located on the failed rack mount server(s), execute this step; otherwise, skip to the next step. Refer to the **Deploy Redundant PMAC (Optional)** procedure to re-deploy and configure any redundant PMACs previously configured.
14. ☐	**PMAC**: Determine if the fdconfig file exists from the initial deployment	1. Type: `[admusr@melbourne-pmac-1 ~]$ ll /usr/TKLC/smac/etc/fdc/` 2. Examine the results and verify if the **rms config file <hostname>.cfg** exists. ***Note:*** There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS. 3. If the file exists, skip to step 16.
15. ☐	Create fdconfig backup file, if it does not already exist	Execute this step ONLY If the fdconfig backup file does **NOT** exist. 1. Create the needed file(s) by executing the **Virtual Machine/Network Fast Deployment** section from reference [8]. **WARNING** It is very important to ensure the file(s) created only affects the TVOE server(s) and the guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service. 2. Skip to step 24.
16. ☐	**PMAC**: Load ISOs into PMAC, if not done already	If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the **Virtual Machine/Network Fast Deployment** section from reference [8].
17. ☐	**PMAC**: Edit/Update configuration file	Edit the fdconfig file to include only the required/failed servers. ***Notes***: • Comment out configuration items that are not needed. • Create a separate configuration file for EACH rack mount server being deployed. • The Cabinet ID in the config file needs to match the cabinet already defined in PMAC. The following items are mandatory: • siteName • tpdIso • dsrIso (if DSR VMs are being configured)

Procedure 2. Recovery Scenario 2

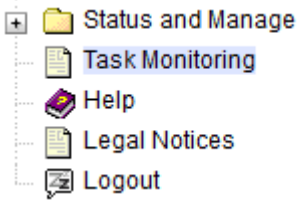
		• sdsIso (if SDS VMs are being configured) • NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured) • XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured) • XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured) • DSRNOAM1XMIIPADDRESS (if DSRNOAM1 is being configured) • DSRNOAM2XMIIPADDRESS (if DSRNOAM2 is being configured) • DSRDRNOAM1XMIIPADDRESS (if DSRDRNOAM1 is being configured) • DSRDRNOAM2XMIIPADDRESS (if DSRDRNOAM2 is being configured) • SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured) • SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured) • SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured) • SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured) ***Notes***: • Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8]. • Comment out SDS and DSR profile items if corresponding products are not used. • For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9, refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8]. • VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName. • VM locations should not be changed from their **RMSx** format. Each RMS should correspond to a separate rack mount server. **WARNING** Ensure the file(s) created only affect the TVOE server(s) and guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.
18. ☐	**PMAC**: Copy the backed up fdc file to the RMS directory	Copy the fdconfig backup file to the RMS directory. `$ sudo cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file> /usr/TKLC/smac/etc/RMS/`

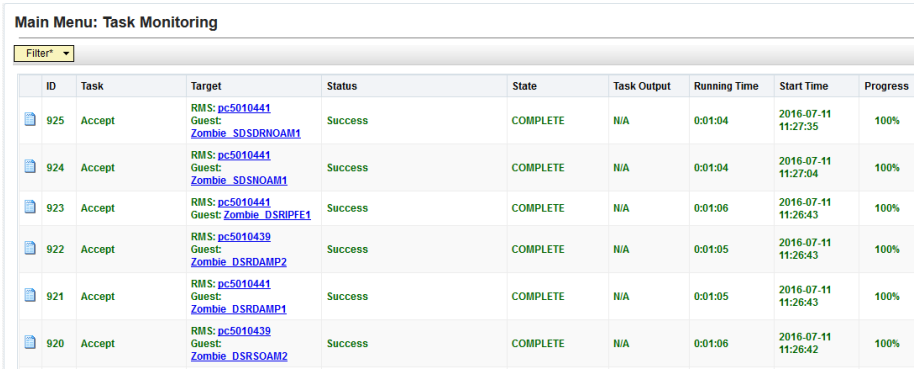
Procedure 2. Recovery Scenario 2

19. ☐	**PMAC**: Execute the config.sh script	Execute **config.sh** against the modified backup config file. ***Note:*** If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again. `$ sudo ./config.sh <config file>` Example output: 

```
[admusr@5010441PMAC RMS]$ sudo ./config.sh rms.cfg
        Validating cfg file...
       Successful validation of cfg file.
       Added Cabinet 101 to Fast Deployment File.
       Added Zombie_TVOE1 to Fast Deployment File.
       Added Zombie_TVOE2 to Fast Deployment File.
       Added xmi(bond0.4) to Fast Deployment File.
       Added imi(bond0.3) to Fast Deployment File.
       Added rep(bond1.10) to Fast Deployment File.
       Added xsi1(bond1.6) to Fast Deployment File.
       Added xsi2(bond1.7) to Fast Deployment File.
       Added xsi3(bond1.8) to Fast Deployment File.
       Added xsi4(bond1.9) to Fast Deployment File.
       Added xsi5(bond1.11) to Fast Deployment File.
       Added xsi6(bond1.12) to Fast Deployment File.
       Added xsi7(bond1.13) to Fast Deployment File.
       Added xsi8(bond1.14) to Fast Deployment File.
       Added xsi9(bond1.15) to Fast Deployment File.
       Added xsi10(bond1.16) to Fast Deployment File.
       Added xsi11(bond1.17) to Fast Deployment File.
       Added xsi12(bond1.18) to Fast Deployment File.
       Added xsi13(bond1.19) to Fast Deployment File.
       Added xsi14(bond1.20) to Fast Deployment File.
       Added xsi15(bond1.21) to Fast Deployment File.
       Added xsi16(bond1.22) to Fast Deployment File.
       Added Zombie_DSRNOAM1 to Fast Deployment File.
       Added Zombie_DSRNOAM2 to Fast Deployment File.
       Added Zombie_DSRDRNOAM1 to Fast Deployment File.
       Added Zombie_DSRDRNOAM2 to Fast Deployment File.
       Added Zombie_SDSNOAM1 to Fast Deployment File.
       Added Zombie_SDSNOAM2 to Fast Deployment File.
       Added Zombie_SDSDRNOAM1 to Fast Deployment File.
       Added Zombie_SDSDRNOAM2 to Fast Deployment File.
       Added Zombie_DSRSOAM1 to Fast Deployment File.
       Added Zombie_DSRSOAM2 to Fast Deployment File.
       Added Zombie_SDSSOAM1 to Fast Deployment File.
       Added Zombie_SDSSOAM2 to Fast Deployment File.
       Added Zombie_DSRDAMP1 to Fast Deployment File.
       Added Zombie_DSRDAMP2 to Fast Deployment File.
       Added Zombie_DSRIPFE1 to Fast Deployment File.
       Added Zombie_DSRIPFE2 to Fast Deployment File.
       Added Zombie_SDSDPSV1 to Fast Deployment File.
       Added Zombie_SDSDPSV2 to Fast Deployment File.
        Validating Fast Deployment File.......
Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml"
Configuration file validation successful.
Validation complete
       Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml
       SUCCESS: OPERATION SUCCESS!!
[admusr@5010441PMAC RMS]$
```

Procedure 2. Recovery Scenario 2

<table>
<tr><td>20.
☐</td><td>PMAC: Execute fast deployment</td><td>With the file generated from the config.sh script, execute the following command to start fast deployment:
<pre>$ screen
$ sudo fdconfig config --file=<fd_config.xml></pre>Note: This is a long duration command. 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.</td></tr>
<tr><td>21.
☐</td><td>PMAC GUI: Monitor the configuration</td><td>1. If not already done, establish a GUI session on the PMAC server.
2. Navigate to Task Monitoring.
 

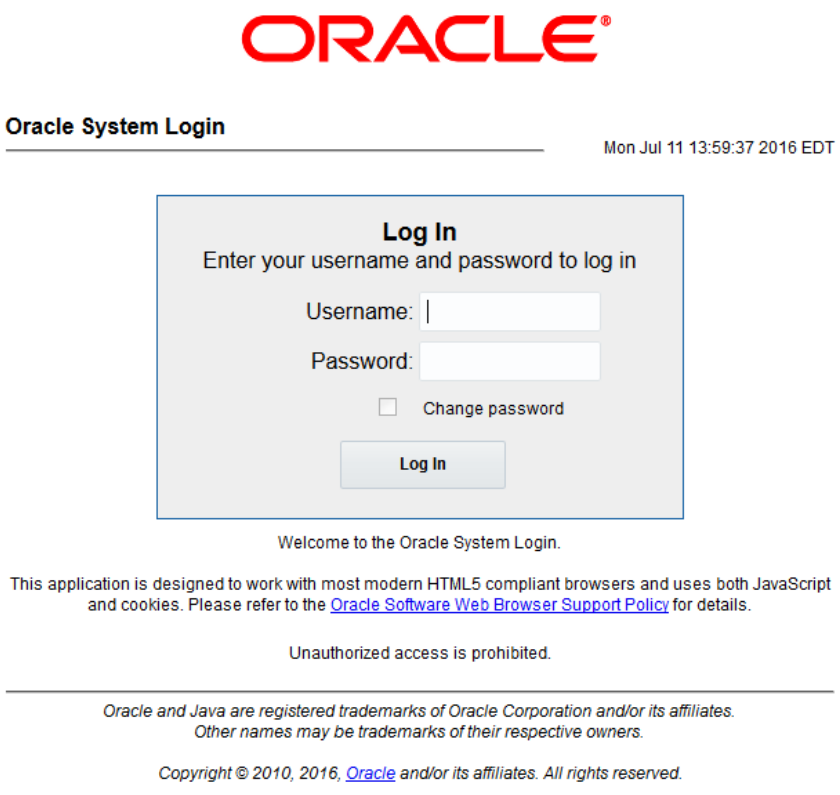
3. Monitor the configuration to completion:
 

<table>
<tr><th></th><th>ID</th><th>Task</th><th>Target</th><th>Status</th><th>State</th><th>Task Output</th><th>Running Time</th><th>Start Time</th><th>Progress</th></tr>
<tr><td></td><td>925</td><td>Accept</td><td>RMS: pc5010441
Guest:
Zombie_SDSDRNOAM1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:04</td><td>2016-07-11
11:27:35</td><td>100%</td></tr>
<tr><td></td><td>924</td><td>Accept</td><td>RMS: pc5010441
Guest:
Zombie_SDSNOAM1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:04</td><td>2016-07-11
11:27:04</td><td>100%</td></tr>
<tr><td></td><td>923</td><td>Accept</td><td>RMS: pc5010441
Guest: Zombie_DSRIPFE1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:06</td><td>2016-07-11
11:26:43</td><td>100%</td></tr>
<tr><td></td><td>922</td><td>Accept</td><td>RMS: pc5010439
Guest:
Zombie_DSRDAMP2</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:05</td><td>2016-07-11
11:26:43</td><td>100%</td></tr>
<tr><td></td><td>921</td><td>Accept</td><td>RMS: pc5010441
Guest:
Zombie_DSRDAMP1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:05</td><td>2016-07-11
11:26:43</td><td>100%</td></tr>
<tr><td></td><td>920</td><td>Accept</td><td>RMS: pc5010439
Guest:
Zombie_DSRSOAM2</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:06</td><td>2016-07-11
11:26:42</td><td>100%</td></tr>
</table>
Note: If a failure occurs with fdconfig, logs can be accessed in /var/TKLC/log/fdconfig/fdconfig.log file.
<pre>[admusr@melbourne-pmac-1 fdconfig]$ sudo fdconfig dumpsteps --file=deploy_melbourne_20170329T202458_701b.fdcdb
Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb"
Here are the steps that were generated
--------------- begin ----------------
Dump of DB steps:
NUM PHS DLY INFRA ID SVRTYPE CMD ELEMENT PRE STATE TO BGTS COMMAND TEXT
----
1 1 0 pmac Fast_Deployment 0 21 0 Complete 300 0 Check PM&C is available
2 1 0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet
3 1 0 pmac Fast_Deployment 0 3 melbourne_RMS3 1 Skipped 900 0 Add Rms
4 2 0 pmac Fast_Deployment 1</pre>4. Restart the fdconfig after a failure has occurred and has been resolved:
<pre>$ sudo fdconfig restart --file=deploy_melbourne_20170329T202458_701b.fdcdb</pre></td></tr>
</table>

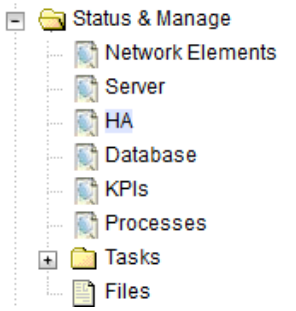
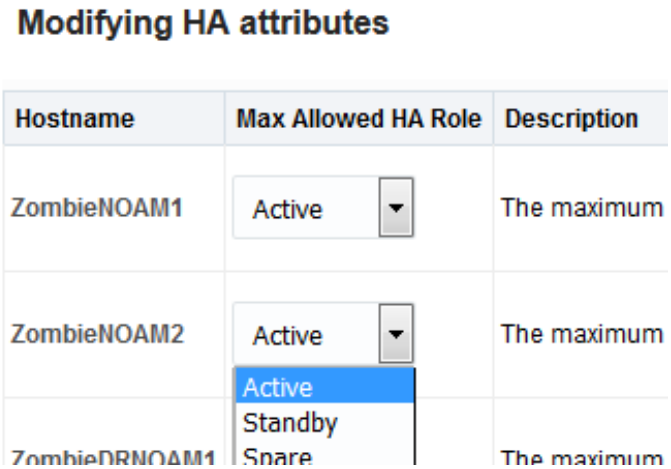
Procedure 2. Recovery Scenario 2

22. ☐	**PMAC**: Repeat for each rack mount server configuration file	Repeat steps 14. -21. for each rack mount server/configuration file, if required.

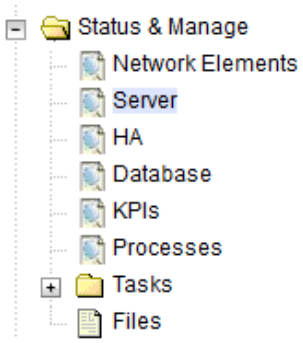
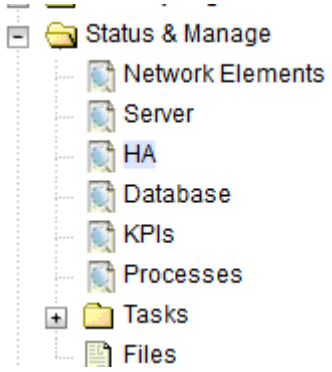
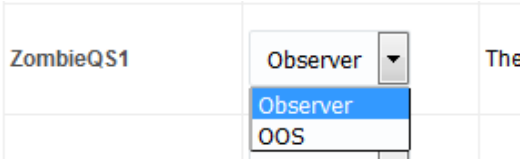
23. ☐	**PMAC**: Back up FDC file	1. Copy the updated fdc file to the fdc backup directory:
		`$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> /usr/TKLC/smac/etc/fdc/`
		2. Change permissions:
		`$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/<fdc_file>`

24. ☐	Perform CPU pinning	Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the **CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only)** procedure from reference [8].
25. ☐	**NOAM GUI**: Login If the failed server is not OAM, then skip to step 47.	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: 

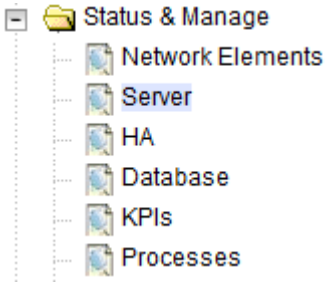
Procedure 2. Recovery Scenario 2

26. ☐	**NOAM VIP GUI**: Recover standby NOAM, if needed	Install the second NOAM server: **DSR**: Execute the **Configure the Second NOAM Server** procedure, steps 1 and 3-6, from reference [8]. **SDS**: Execute the **Configure the Second SDS NOAM Server** procedure, steps 1 and 3-6, from reference [8].
27. ☐	Install NetBackup client (optional)	If NetBackup is used, execute the **Install NetBackup Client (Optional)** procedure from reference [8].
28. ☐	**NOAM VIP GUI**: Set HA on standby NOAM	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Select the standby NOAM server and set it to **Active**.  4. Click **OK**.

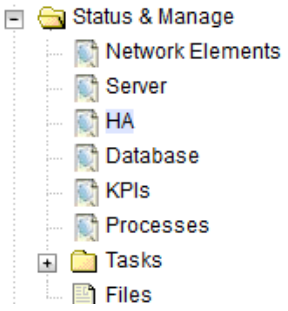
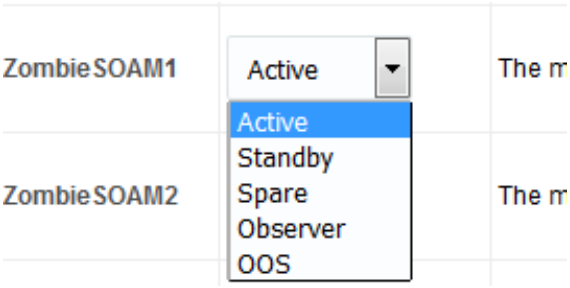
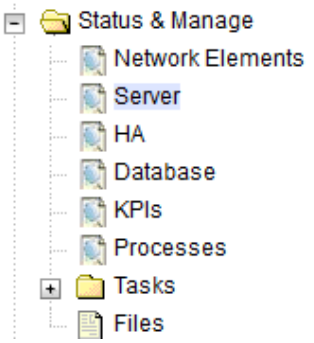
Procedure 2. Recovery Scenario 2

29. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**. 
30. ☐	**NOAM VIP GUI**: Recover query servers. SDS only. If DSR, skip to step 33.	Execute the **Configuring SDS Query Servers** procedure, steps 1 and 4-7, from reference [8].
31. ☐	**SDS NOAM VIP GUI**: Set HA on query server. SDS only. If DSR, skip to step 33.	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Select the query server and select **Observer**.  4. Click **OK**.

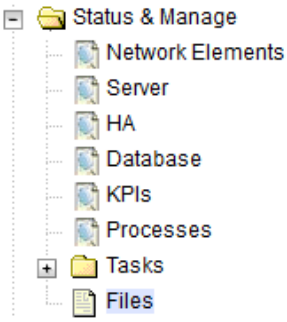
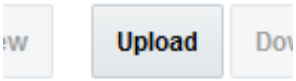
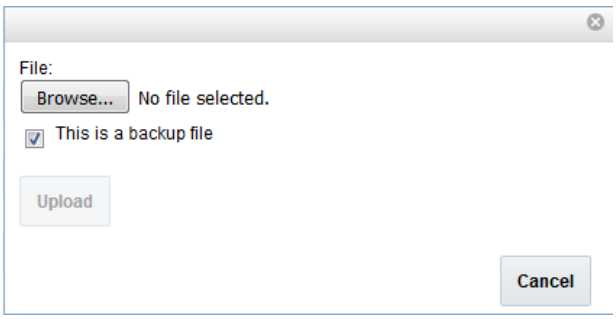
Procedure 2. Recovery Scenario 2

32. ☐	**SDS NOAM VIP GUI**: Restart SDS application. SDS only. If DSR, skip to step 33.	1. Navigate to **Status & Manage > Server**.  2. Select the recovered query server and click **Restart**. 
33. ☐	**NOAM VIP GUI**: Stop replication to the C-level servers of this site.	**For DSR:** Before continuing this procedure, replication to C-level servers **MUST** be inhibited at the SOAM site being recovered. 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. **For SDS,** Inhibit database replication for defective SOAM servers and DP servers associated with this SOAM network element. NOTE: It is expected that each SOAM and subtending DP will have a DB Level of "UNKNOWN" until the SOAMs are restored. 1. Go to the NOAMP GUI. 2. Select [**Main Menu: Status & Manage** → **Database**] screen 3. Filter on the SOAM Network Element name. 4. Record the DP server hostnames (Role: MP). 5. Click “Inhibit Replication” button for each DP server until all DP servers associated with this SOAM Network Element have been inhibited "Inhibiting" SOAM server: Click “Inhibit Replication” button for each defective SOAM servers.

Procedure 2. Recovery Scenario 2

34. ☐	**NOAM VIP GUI**: Recover active SOAM server	Install the SOAM servers. **DSR**: Execute the **Configure the SOAM Servers** procedure, steps 1-3 and 5-9, from reference [8]. ***Note:*** If you are using NetBackup, also execute step 12. **SDS**: Execute the **Configure the SDS DP SOAM Servers** procedure, steps 1-3 and 5-8, from reference [8].
35. ☐	**NOAM VIP GUI**: Set HA on the SOAM server	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Select the SOAM server and set it to **Active**.  4. Click **OK**.
36. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered SOAM server and click **Restart**. 

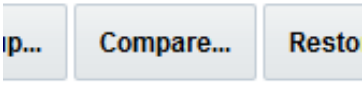
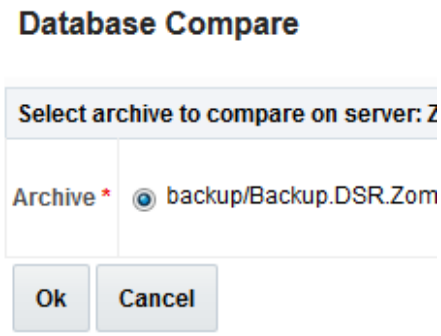
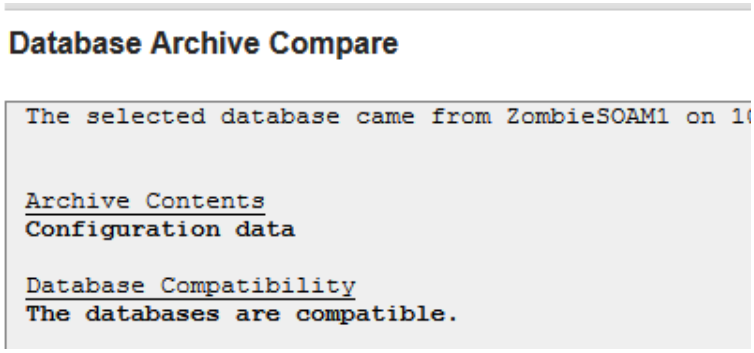
Procedure 2. Recovery Scenario 2

37. ☐	**NOAM VIP GUI**: Upload the backup SOAM database file. DSR only. If SDS, skip to step 42.	1. Navigate to **Status & 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. Mark the **This is a backup file** checkbox. 5. Click **Open**. 6. Click **Upload**.  The file takes a few seconds to upload depending on the size of the backup data and displays on the list of entries when it has completed the upload.

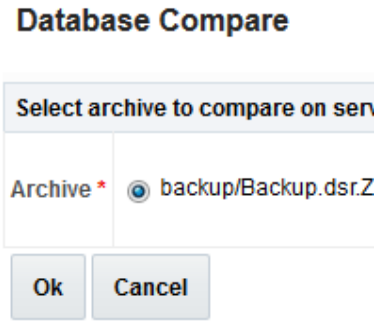
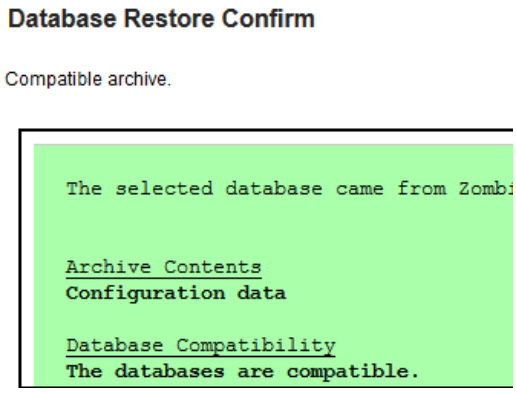
Procedure 2. Recovery Scenario 2

38. ☐	**Recovered SOAM GUI**: Login. DSR only. If SDS, skip to step 42.	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

39. ☐	**Recovered SOAM GUI**: Verify the archive contents and database compatibility. DSR only. If SDS, skip to step 42.	1. Navigate to **Status & Manage > Database**. 2. Select the **Active SOAM** server and click **Compare**.  3. Click the button for the restored database file uploaded as a part of step 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.

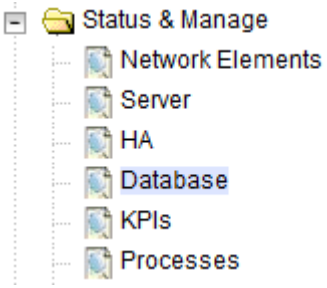
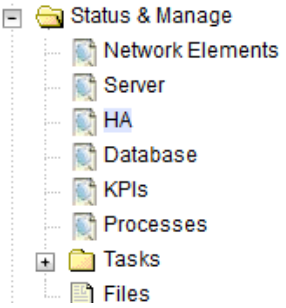
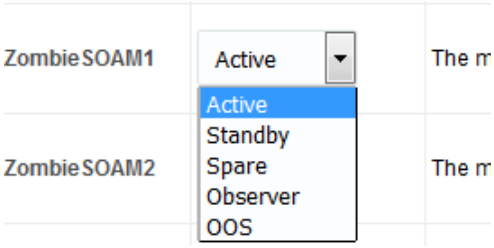
Procedure 2. Recovery Scenario 2

40. ☐	**Recovered SOAM GUI**: Restore the database. DSR only. If SDS, skip to step 42.	1. Select the **Active SOAM** server and click **Restore**. 2. Select the backup provisioning and configuration file.  3. Click **OK**.  4. If the Node Type Compatibility error displays, it is expected. If no other errors display, mark the **Force** checkbox and click **OK** to proceed with the DB restore. ***Notes***: • After the restore has started, the user is logged out of XMI SOAM GUI since the restored topology is old data. • If the spare SOAM is in another network and is unreachable, the database restore cannot be done. **Workaround**: If the spare SOAM is unreachable and ping (from recovered SOAM server to spare SOAM server) hangs (as evidenced by **ps -ef | grep ping** showing the same ping process and its child for more than 10 seconds), then kill the hung ping processes and the restore proceeds.
41. ☐	**Recovered SOAM GUI**: Monitor and confirm database restoral. DSR only. If SDS, skip to step 42.	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. ***Notes***: • Do not pay attention to alarms until all the servers in the system are completely restored. • The Configuration and Maintenance information is in the same state it was when backed up during initial backup.

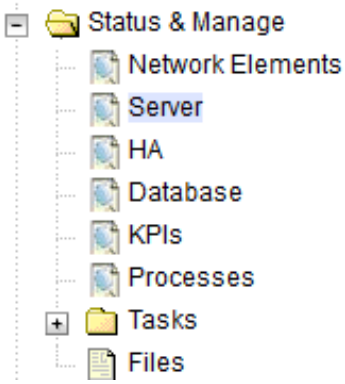
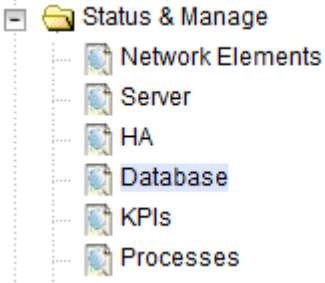
Procedure 2. Recovery Scenario 2

42. ☐	**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: 
43. ☐	**NOAM VIP GUI**: Recover the remaining SOAM servers (standby, spare)	**DSR**: Execute the **Configure the SOAM Servers** procedure, steps 1-3 and 5-9, from reference [8]. ***Note:*** If you are using NetBackup, also execute step 12. **SDS**: Execute the **Configure the SDS DP SOAM Servers** procedure, steps 1-3 and 5-8, from reference [8].

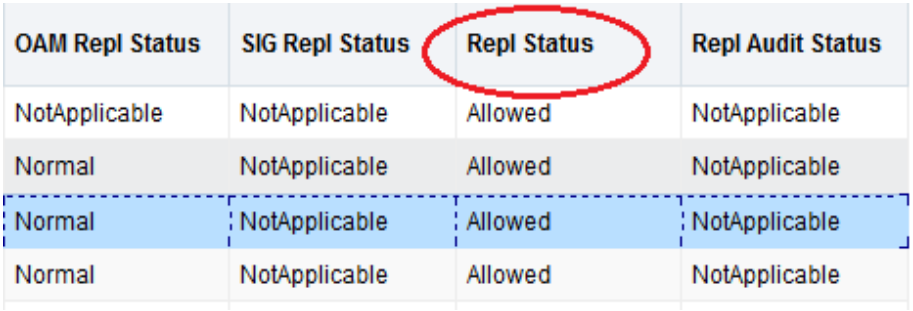
Procedure 2. Recovery Scenario 2

44. ☐	**NOAM VIP GUI**: Start replication on the recovered SOAMs, if replication is inhibited	Un-Inhibit (start) replication to the recovered SOAM servers 5. Navigate to **Status & Manage > Database**.  6. Click **Allow Replication** on the recovered SOAM servers. 7. Verify the replication on all SOAMs servers is allowed. This can be done by checking **Repl status** column of respective server
45. ☐	**NOAM VIP GUI**: Set HA on the recovered standby SOAM server	1. Navigate to **Status & 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**.

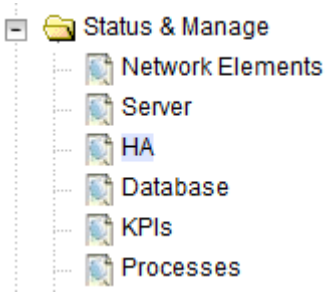
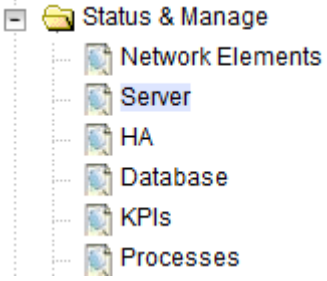
Procedure 2. Recovery Scenario 2

46. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered NOAM server and click **Restart**. 
47. ☐	**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 & 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)** — Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only • Active DR NOAM Server • Standby DR NOAM Server • MP/IPFE Servers (if MPs are configured as active/standby, start with

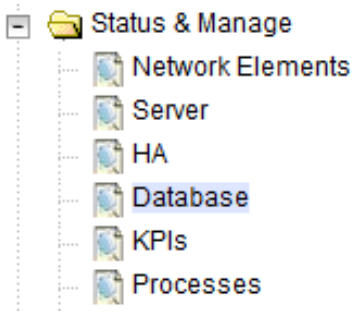
Procedure 2. Recovery Scenario 2

<table>
<tr><td></td><td></td><td>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) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only
3. Verify the replication on all the working servers is allowed. This can be done by examining the Repl Status table.
 
<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>
For SDS:
Allow database replication for SOAM-A and SOAM-B servers and DP servers associated with this SOAM network element.
1. Go to the NOAMP GUI.
2. Select [Main Menu: Status & Manage → Database] screen
3. Filter on the SOAM Network Element name.
4. Record the DP server hostnames (Role: MP).
5. Wait until audit becomes active on SOAM's. Allowing Replication: Click “Allow Replication” button for each newly replaced SOAM-A and SOAM-B servers
Allowing Replication: Click “Allow Replication” button for each DP server until all DP servers associated with this SOAM Network Element have been inhibited</td></tr>
<tr><td>48. ☐</td><td>Activate PCA feature.
DSR only</td><td>If you have PCA installed in the system being recovered, re-activate PCA by executing the PCA Activation on Entire Network procedure on the recovered standby NOAM server from [7].</td></tr>
<tr><td>49. ☐</td><td>NOAM VIP GUI: Recover the C-level server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs</td><td>DSR:
Execute the Configure the MP Servers procedure, steps 1 and 9-13, from reference [8].
Note: Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.
SDS (Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only):
Execute the Configure the SDS DP Servers procedure, steps 1 and 5-8, from reference [8].
Repeat this step for any remaining failed MP servers.</td></tr>
</table>

Procedure 2. Recovery Scenario 2

50. ☐	**NOAM VIP GUI**: Set HA on all C-level servers	1. Navigate to **Status & Manage -> HA**.  2. Click **Edit**. 3. For each recovered C-Level with a Max Allowed HA Role set to **OOS**, set it to **Active**.  4. Click **OK**.
51. ☐	**NOAM VIP GUI**: Restart DSR application on the recovered C-level servers	1. Navigate to **Status & Manage > Server**.  2. Select the recovered C-level servers and click **Restart**. 

Procedure 2. Recovery Scenario 2

<table>
<tr>
<td>52. ☐</td>
<td>NOAM VIP GUI: Start replication on all C-Level servers.
DSR only. If SDS, then skip to next step.</td>
<td>Un-Inhibit (start) replication to the ALL C-level servers.
1. Navigate to Status & Manage > Database.
 

2. If the Repl Status is set to Inhibited, click Allow Replication using this order:
• Active NOAMP Server
• Standby NOAMP Server
• Active SOAM Server
• Standby SOAM Server
• Spare SOAM Server (if applicable) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only)
• Active DR NOAM Server
• Standby DR NOAM Server
• MP/IPFE Servers
• SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only
3. Verify the replication on all servers is allowed. This can be done by checking the Repl Status.
<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>53. ☐</td>
<td>Active NOAM: Perform keyexchange between the active-NOAM and recovered servers</td>
<td>1. Establish an SSH session to the active NOAM and login as admusr.
2. Perform a keyexchange from the active NOAM to each recovered server:

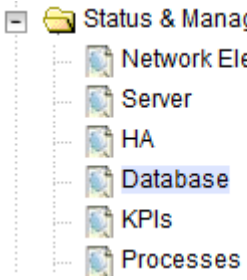
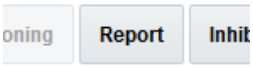
```
$ keyexchange admusr@<Recovered Server Hostname>
```


Note: If an export server is configured, perform this step.</td>
</tr>
</table>

Procedure 2. Recovery Scenario 2

54. ☐	**Active NOAM**: Activate optional features. DSR only. If SDS, then skip to next step.	Establish an SSH session to the active NOAM and login as **admusr**. **Note for PCA Feature Activation:** If you have PCA installed in the system being recovered, re-activate the PCA by executing the **PCA Activation on Stand By NOAM Server** procedure on the recovered standby NOAM server; and the **PCA Activation on Active SOAM Server** procedure on the recovered active SOAM server from [6]. ***Notes***: • If not all SOAM sites are recovered at this point, then repeat the activation for each "new" SOAM site that comes online. • If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature. Refer to section 1.5 Optional Features to activate any features that were previously activated. ***Note:*** While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored: `iload#31000{S/W Fault}`

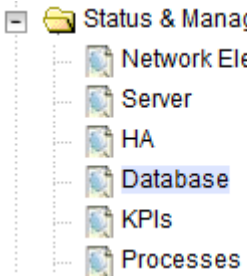
Procedure 2. Recovery Scenario 2

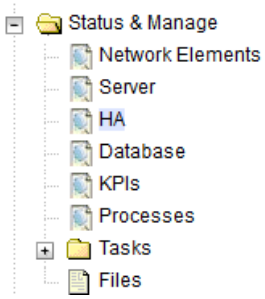
55. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status & Manage > Database**.
		 
		2. Select the active NOAM server and click **Report**.
		 
		The following screen displays:
		Main Menu: Status & Manage -> Database [Report]
		`dsr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

Procedure 2. Recovery Scenario 2

56. ☐	**Active NOAM**: Verify replication between servers	1. Log into the active NOAM as **admusr** using SSH terminal.
		2. Execute this command:
		`$ sudo irepstat –m`
		Example output:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`Oahu-DAMP-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.15%cpu 25B/s  A=me`
		`  CC To  Oahu-DAMP-2  Active  0  0.10  0.14%cpu 25B/s  A=me`
		`Oahu-DAMP-2 -- Stby`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.11%cpu 31B/s  A=C3642.212`
		`  CC From Oahu-DAMP-1  Active  0  0.10 ^0.14 1.16%cpu 31B/s A=C3642.212`
		`Oahu-IPFE-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 24B/s  A=C3642.212`
		`Oahu-IPFE-2 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 28B/s  A=C3642.212`
		`Oahu-NOAM-1 -- Stby`
		`  AA From Oahu-NOAM-2  Active  0  0.25 ^0.03%cpu 23B/s`
		`Oahu-NOAM-2 -- Active`
		`  AA To  Oahu-NOAM-1  Active  0  0.25 1%R 0.04%cpu 61B/s`
		`  AB To  Oahu-SOAM-2  Active  0  0.50 1%R 0.05%cpu 75B/s`
		`Oahu-SOAM-1 -- Stby`
		`  BB From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 27B/s`
		`Oahu-SOAM-2 -- Active`
		`  AB From Oahu-NOAM-2  Active  0  0.50 ^0.03%cpu 24B/s`
		`  BB To  Oahu-SOAM-1  Active  0  0.50 1%R 0.04%cpu 32B/s`
		`  BC To  Oahu-IPFE-1  Active  0  0.50 1%R 0.04%cpu 21B/s`
		`  BC To  Oahu-SS7MP-2 Active  0  0.50 1%R 0.04%cpu 21B/s`
		`irepstat ( 40 lines) (h)elp (m)erged`

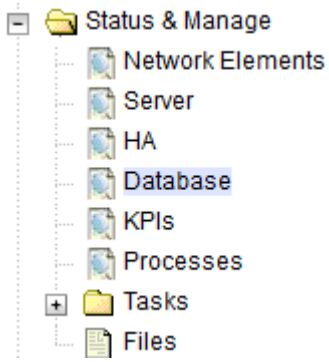
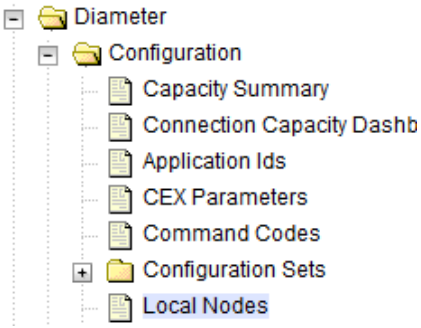
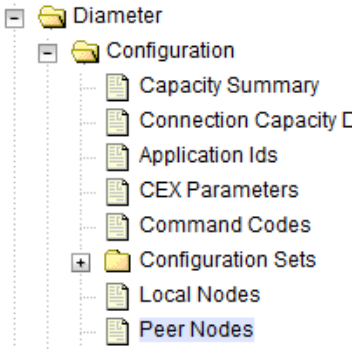
Procedure 2. Recovery Scenario 2

<table>
<tr>
<td>57. ☐</td>
<td>NOAM VIP GUI: Verify the database states</td>
<td>
1. Navigate to Status & Manager > Database.


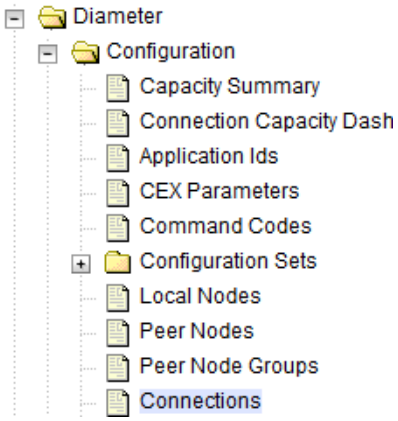
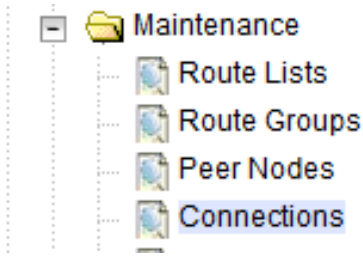
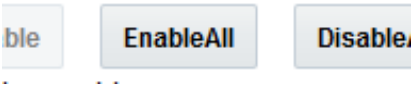
2. Verify the OAM Max HA Role is either Active or Standby for NOAM and SOAM; Application Max HA Role for MPs is Active; and status is Normal:
<table>
<tr><th>Network Element</th><th>Server</th><th>Role</th><th>OAM Max HA Role</th></tr>
<tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM1</td><td>Network OAM&P</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>58. ☐</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>

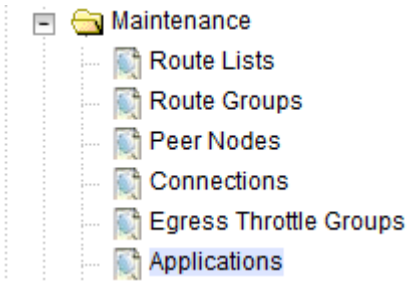
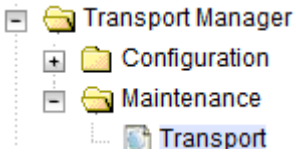
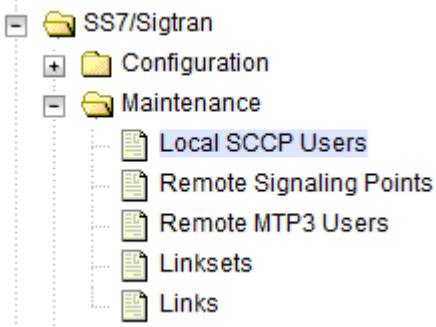
Procedure 2. Recovery Scenario 2

59. ☐	**SOAM GUI**: Enable site provisioning. DSR only. If SDS, skip to step 69.	1. Navigate to **Status & Manage > Database**.  2. Click **Enable Site Provisioning**.  3. A confirmation window displays. Click **OK** to enable provisioning.
60. ☐	**SOAM VIP GUI**: Verify local node information. DSR only. If SDS, skip to step 69.	1. Navigate to **Diameter > Configuration > Local Node**.  2. Verify all the local nodes are shown.
61. ☐	**SOAM VIP GUI**: Verify the peer node information. DSR only. If SDS, then skip to step 69.	1. Navigate to **Diameter > Configuration > Peer Node**.  2. Verify all the peer nodes are shown.

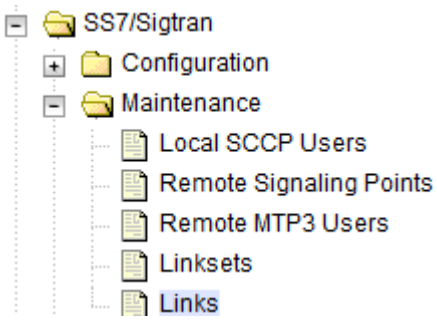
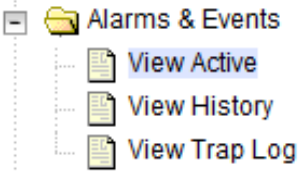
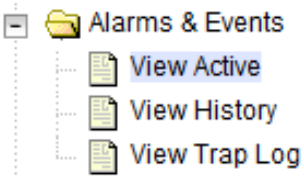
Procedure 2. Recovery Scenario 2

62. ☐	**SOAM VIP GUI**: Verify the connections information. DSR only. If SDS, then skip to step 69.	1. Navigate to **Diameter > Configuration > Connections**.  2. Verify all the connections are shown.
63. ☐	**MP Servers**: Disable SCTP Auth Flag. DSR only. If SDS, then skip to step 69.	For SCTP connections without DTLS enabled, refer to the **Enable/Disable DTLS (SCTP Diameter Connections Only)** section in reference [8]. Execute this procedure on all failed MP servers.
64. ☐	**SOAM VIP GUI**: Enable connections, if needed. DSR only. If SDS, then skip to step 69.	3. Navigate to **Diameter > Maintenance > Connections**.  4. Select each connection and click **Enable**. Alternatively, enable all the connections by clicking **EnableAll**.  5. Verify the Operational State is **Available**. ***Note:*** If a disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution

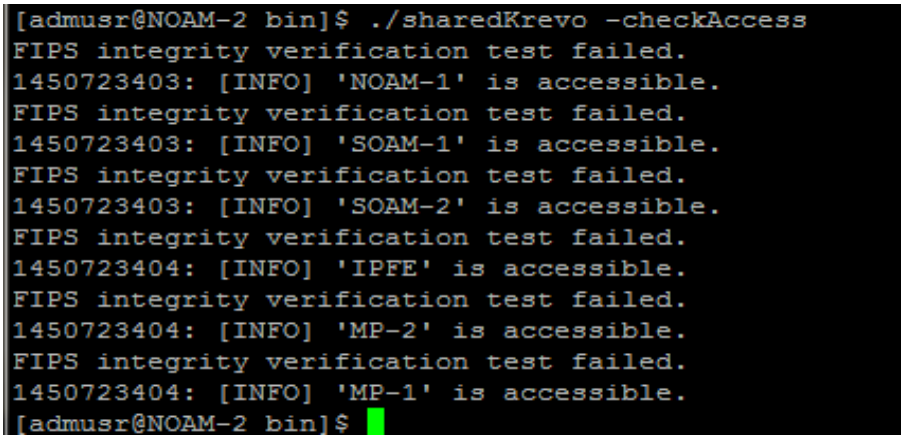
Procedure 2. Recovery Scenario 2

65. ☐	**SOAM VIP GUI**: Enable optional features. DSR only. If SDS, then skip to step 69.	1. Navigate to **Diameter > Maintenance > Applications**.  2. Select the optional feature application configured in step 72. 3. Click **Enable**. 
66. ☐	**SOAM VIP GUI**: Re-enable transports, if needed. DSR only. If SDS, then skip to step 69.	1. Navigate to **Transport Manager > Maintenance > Transport**.  2. Select each transport and click **Enable**.  3. Verify the Operational Status for each transport is **Up**.
67. ☐	**SOAM VIP GUI**: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 69.	1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.  2. Click the **Enable** button corresponding to MAPIWF Application Name.  3. Verify the SSN Status is **Enabled**.

Procedure 2. Recovery Scenario 2

68. ☐	**SOAM VIP GUI**: Re-enable links, if needed. DSR only. If SDS, then skip to step 69.	1. Navigate to **SS7/Sigtran > Maintenance > Links**.  2. Click **Enable** for each link.  3. Verify the Operational Status for each link is **Up**.
69. ☐	**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).
70. ☐	**NOAM VIP GUI**: Examine all alarms	1. Navigate to **Alarms & Events > View Active**.  2. Examine all active alarms and refer to the on-line help on how to address them. If needed, contact My Oracle Support (MOS).

Procedure 2. Recovery Scenario 2

71. ☐	**NOAM VIP**: Verify all servers in topology are accessible (RADIUS only)	If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.
		1. Establish an SSH session to the NOAM VIP and login as **admusr**.
		2. Check if all the servers in the topology are accessible:
		`$ /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo -checkAccess`
		Example output:
		 
		Note: If any server is not accessible, stop and contact My Oracle Support (MOS).

72. ☐	**NOAM VIP**: Copy key file to all the servers in topology (RADIUS only)	If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.
		1. Check if existing key file on active NOAM (the NOAM, which is intact and was not recovered) server is valid:
		`$ cd /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo -validate`
		Example output:

Procedure 2. Recovery Scenario 2

```
[admusr@NOAM-2 bin]$ ./sharedKrevo -validate
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723458: [INFO] Key file for 'NOAM-1' is valid
1450723458: [INFO] Key file for 'NOAM-2' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723459: [INFO] Key file for 'SOAM-1' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723460: [INFO] Key file for 'SOAM-2' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723461: [INFO] Key file for 'IPFE' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723461: [INFO] Key file for 'MP-2' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723462: [INFO] Key file for 'MP-1' is valid
[admusr@NOAM-2 bin]$
```

If output of above command shows the existing key file is not valid, contact My Oracle Support (MOS).

2. Copy the key file to all the servers in the topology:

```
$ ./sharedKrevo -synchronize
```

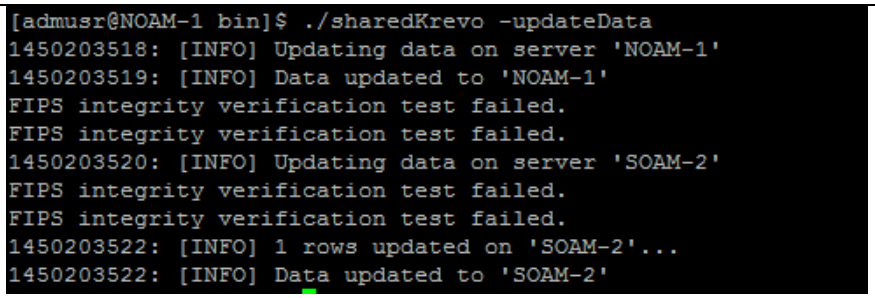
Example output:

```
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722733: [INFO] Synched key to IPFE
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722734: NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722735: [INFO] Synched key to MP-2
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722736: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722738: [INFO] Synched key to MP-1
[admusr@NOAM-2 bin]$
```

```
$ ./sharedKrevo -updateData
```

Example output:

Procedure 2. Recovery Scenario 2

		 ***Note:*** If any errors display, stop and contact My Oracle Support (MOS).
73. ☐	Back up and archive all the databases from the recovered system	Execute Appendix A DSR Database Backup to back up the Configuration databases.
74. ☐	Recover IDIH	If IDIH was affected, refer to section 6 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 **Query Server** (if needed) by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover any failed **SOAM and MP/DP 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/DP servers.

- Recover IDIH if necessary

Procedure 3. Recovery Scenario 3

S T E P #	This procedure performs recovery if ALL NOAM servers are failed but 1 or more SOAM servers are intact. This includes any SOAM server that is in another location (spare SOAM server). Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Gather required materials	Gather the documents and required materials listed in the Required Materials section.
2. ☐	Create a backup directory, if needed	Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.
3. ☐	Replace failed equipment	HW vendor to replace the failed equipment.
4. ☐	**Recover PMAC and PMAC TVOE Host**: Configure BIOS settings and update firmware	1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]: • HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings • Oracle X5-2/Netra X5-2/X6-2/ X7-2: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings • HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings 2. Verify and/or upgrade server firmware by executing the **Upgrade Rack Mount Server Firmware** procedure from reference [8].
5. ☐	**PMAC, TVOE Hosts, and Switch Recovery**: Backups available	This step assumes TVOE and PMAC backups are available. If backups are **NOT** available, **skip this step**. 1. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers. 2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup. 3. Proceed to step 7.
6. ☐	**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 the **Install and Configure TVOE on First RMS (PMAC Host)** procedure from reference [8]. 2. Execute the **Install PMAC** procedure from reference [8]. 3. Execute the **Initialize the PMAC Application** section from reference [8].

Procedure 3. Recovery Scenario 3

7. ☐	Recovery failed Cisco 4948 aggregation switches (HP DL380 only)	Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 GEN 9, **skip this step**. Recover failed Cisco 4948 aggregation switches, if needed: 1. Back up available configuration files. Refer to Appendix C Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only) to recover failed Cisco 4948 aggregation switches. 2. Back up configuration files NOT available. Execute **Configure Cisco 4948E-F Aggregation Switches (HP DL 380 Gen 8 Only)** section from reference [8].
8. ☐	Configure PMAC (no backup)	If PMAC backup was **NOT** restored in step 5, execute this step; otherwise skip this step. Execute the **Configure PMAC Server (NetBackup Only)** and **Add RMS to the PMAC Inventory** sections from reference [8].
9. ☐	Install/Configure additional rack mount servers	1. Execute the **Install TVOE on Additional Rack Mount Servers** procedure from reference [8]. 2. **If backups are available**, restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers. **If backups are NOT available**, execute the **Configure TVOE on Additional Rack Mount Servers** procedure from reference [8].
10. ☐	Configure BIOS settings and update firmware on additional rack mount servers	1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]: • HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings • Oracle X5-2/Netra X5-2/X6-2/ X7-2: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings • HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings 2. Verify and/or upgrade server firmware by executing the **Upgrade Rack Mount Server Firmware** procedure from reference [8].
11. ☐	Determine VM Placement and Socket Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 only)	HP DL380 GEN 8, skip this step. Determine VM placement and pinning by following: 1. From this document, section 3.1, item 14, to determine the VM placement; and 2. In reference [8], Appendix S VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1 Gbps NICs) and CPU Pinning in HP DL380 Gen 9 (Onboard 1 Gbps NICs) for Pinning Information on HP DL380 Gen 9.
12. ☐	Deploy redundant PMAC, if required	Refer to the **Deploy Redundant PMAC (Optional)** procedure to re-deploy and configure any redundant PMACs previously configured.

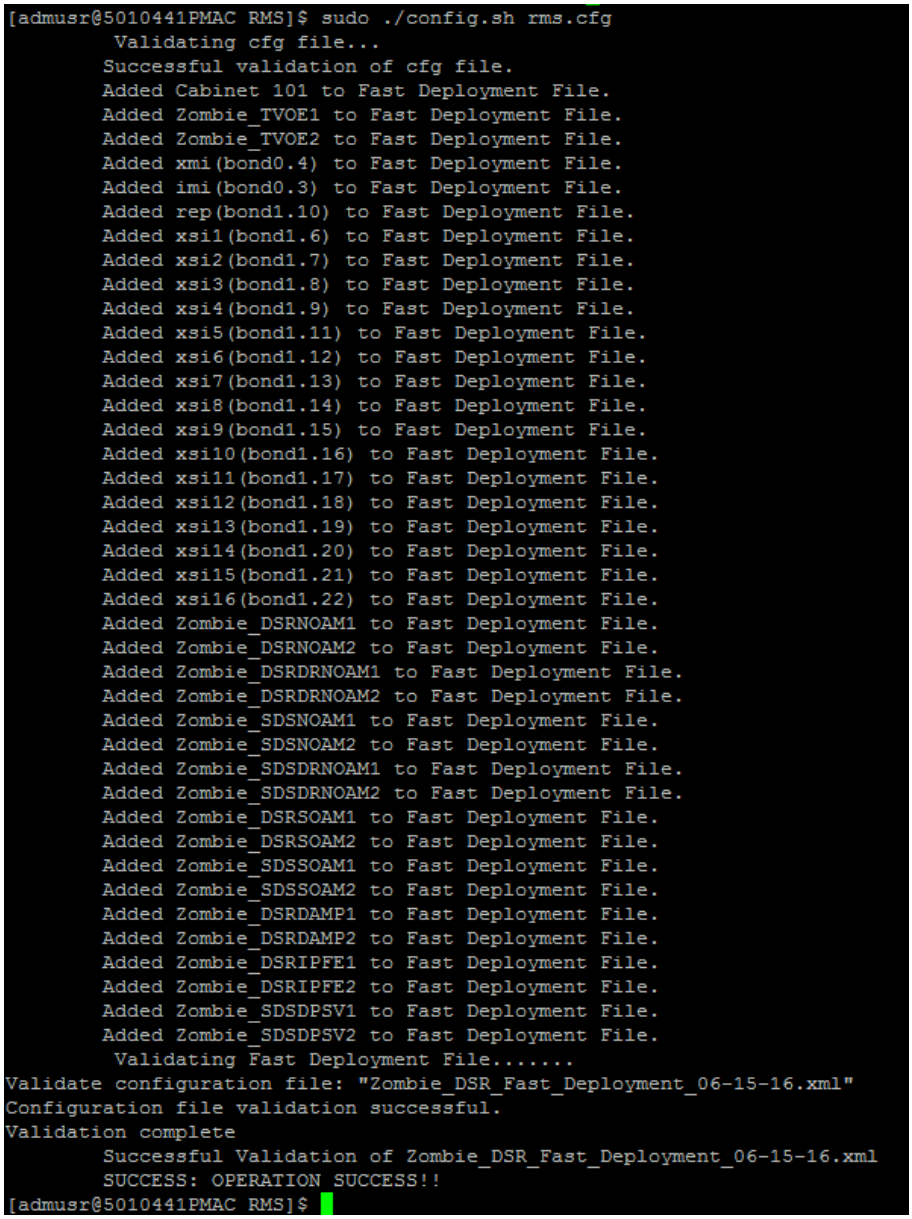
Procedure 3. Recovery Scenario 3

13. ☐	**PMAC**: Determine if the fdconfig file exists from the initial deployment	1. Type: `[admusr@melbourne-pmac-1 ~]$ ll /usr/TKLC/smac/etc/fdc/` 2. Examine the results and verify if the **rms config file <hostname>.cfg** exists. ***Note:*** There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS.
14. ☐	Create fdconfig backup file, if it does not already exist	Execute this step ONLY If the fdconfig backup file does **NOT** exist. 1. Create the needed file(s) by executing the **Virtual Machine/Network Fast Deployment** section from reference [8]. **WARNING** It is very important to ensure the file(s) created only affects the TVOE server(s) and the guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service. 2. Skip to step 23. if this step was executed.
15. ☐	**PMAC**: Load ISOs into PMAC, if not done already	If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the **Virtual Machine/Network Fast Deployment** section from reference [8].
16. ☐	**PMAC**: Edit/Update configuration file	Edit the fdconfig file to include only the required/failed servers. ***Notes***: • Comment out configuration items that are not needed. • Create a separate configuration file for EACH rack mount server being deployed. • The Cabinet ID in the config file needs to match the cabinet already defined in PMAC. The following items are mandatory: • siteName • tpdIso • dsrIso (if DSR VMs are being configured) • sdsIso (if SDS VMs are being configured) • NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured) • XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured) • XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured) • DSRNOAM1XMIIPADDRESS (if DSRNOAM1 is being configured) • DSRNOAM2XMIIPADDRESS (if DSRNOAM2 is being configured) • DSRDRNOAM1XMIIPADDRESS (if DSRDRNOAM1 is being configured) • DSRDRNOAM2XMIIPADDRESS (if DSRDRNOAM2 is being configured)

Procedure 3. Recovery Scenario 3

		• SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured) • SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured) • SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured) • SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured) ***Notes***: • Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8]. • Comment out SDS and DSR profile items if corresponding products are not used. • For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9: Refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8]. • VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName. • VM locations should not be changed from their **RMSx** format. Each RMS should correspond to a separate rack mount server. **WARNING** Ensure the file(s) created only affect the TVOE server(s) and guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.
17. ☐	**PMAC**: Copy the backed up fdc file to the RMS directory	Copy the fdconfig backup file to the RMS directory. `$ sudo cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file> /usr/TKLC/smac/etc/RMS/`

Procedure 3. Recovery Scenario 3

18. ☐	**PMAC**: Execute the config.sh script	Execute **config.sh** against the modified backup config file. ***Note:*** If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again. `$ sudo ./config.sh <config file>` Example output: 

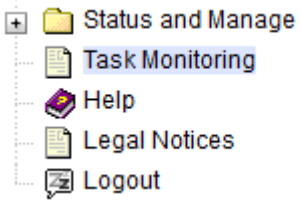
```
[admusr@5010441PMAC RMS]$ sudo ./config.sh rms.cfg
         Validating cfg file...
        Successful validation of cfg file.
        Added Cabinet 101 to Fast Deployment File.
        Added Zombie_TVOE1 to Fast Deployment File.
        Added Zombie_TVOE2 to Fast Deployment File.
        Added xmi(bond0.4) to Fast Deployment File.
        Added imi(bond0.3) to Fast Deployment File.
        Added rep(bond1.10) to Fast Deployment File.
        Added xsi1(bond1.6) to Fast Deployment File.
        Added xsi2(bond1.7) to Fast Deployment File.
        Added xsi3(bond1.8) to Fast Deployment File.
        Added xsi4(bond1.9) to Fast Deployment File.
        Added xsi5(bond1.11) to Fast Deployment File.
        Added xsi6(bond1.12) to Fast Deployment File.
        Added xsi7(bond1.13) to Fast Deployment File.
        Added xsi8(bond1.14) to Fast Deployment File.
        Added xsi9(bond1.15) to Fast Deployment File.
        Added xsi10(bond1.16) to Fast Deployment File.
        Added xsi11(bond1.17) to Fast Deployment File.
        Added xsi12(bond1.18) to Fast Deployment File.
        Added xsi13(bond1.19) to Fast Deployment File.
        Added xsi14(bond1.20) to Fast Deployment File.
        Added xsi15(bond1.21) to Fast Deployment File.
        Added xsi16(bond1.22) to Fast Deployment File.
        Added Zombie_DSRNOAM1 to Fast Deployment File.
        Added Zombie_DSRNOAM2 to Fast Deployment File.
        Added Zombie_DSRDRNOAM1 to Fast Deployment File.
        Added Zombie_DSRDRNOAM2 to Fast Deployment File.
        Added Zombie_SDSNOAM1 to Fast Deployment File.
        Added Zombie_SDSNOAM2 to Fast Deployment File.
        Added Zombie_SDSDRNOAM1 to Fast Deployment File.
        Added Zombie_SDSDRNOAM2 to Fast Deployment File.
        Added Zombie_DSRSOAM1 to Fast Deployment File.
        Added Zombie_DSRSOAM2 to Fast Deployment File.
        Added Zombie_SDSSOAM1 to Fast Deployment File.
        Added Zombie_SDSSOAM2 to Fast Deployment File.
        Added Zombie_DSRDAMP1 to Fast Deployment File.
        Added Zombie_DSRDAMP2 to Fast Deployment File.
        Added Zombie_DSRIPFE1 to Fast Deployment File.
        Added Zombie_DSRIPFE2 to Fast Deployment File.
        Added Zombie_SDSDPSV1 to Fast Deployment File.
        Added Zombie_SDSDPSV2 to Fast Deployment File.
         Validating Fast Deployment File.......
Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml"
Configuration file validation successful.
Validation complete
        Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml
        SUCCESS: OPERATION SUCCESS!!
[admusr@5010441PMAC RMS]$
```

Procedure 3. Recovery Scenario 3

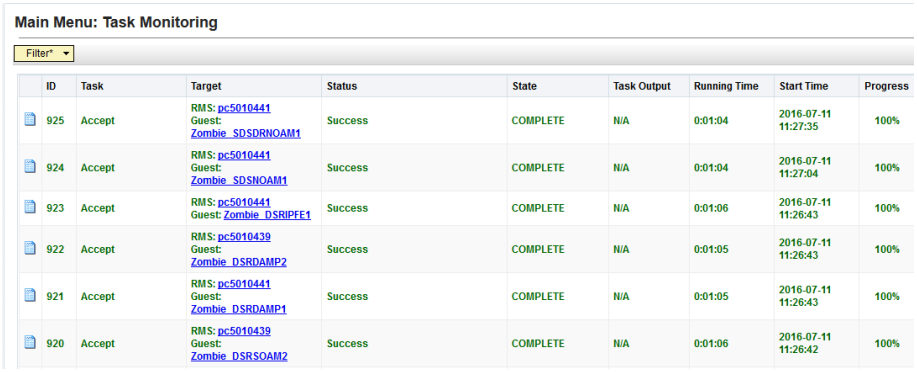
<table>
<tr>
<td>19. ☐</td>
<td>PMAC: Execute fast deployment</td>
<td>With the file generated from the config.sh script, execute the following command to start fast deployment:

<pre>$ screen
$ sudo fdconfig config --file=<fd_config.xml></pre>

Note: This is a long duration command. 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.</td>
</tr>
<tr>
<td>20. ☐</td>
<td>PMAC GUI: Monitor the configuration</td>
<td>1. If not already done, establish a GUI session on the PMAC server.
2. Navigate to Task Monitoring.



3. Monitor the configuration to completion:



Note: If a failure occurs with fdconfig, logs can be accessed in /var/TKLC/log/fdconfig/fdconfig.log file.

<pre>[admusr@melbourne-pmac-1 fdconfig]$ sudo fdconfig dumpsteps --file=deploy_melbourne_20170329T202458_701b.fdcdb
Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb"
Here are the steps that were generated
--------------- begin ----------------
Dump of DB steps:
NUM PHS DLY INFRA ID SVRTYPE CMD ELEMENT PRE STATE TO BGTS COMMAND TEXT

-
1 1 0 pmac Fast_Deployment 0 21 0 Complete 300 0 Check PM&C is available
2 1 0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet
3 1 0 pmac Fast_Deployment 0 3 melbourne_RMS3 1 Skipped 900 0 Add Rms
4 2 0 pmac Fast_Deployment 1</pre>
4. Restart the fdconfig after a failure has occurred and has been resolved:

<pre>$ sudo fdconfig restart --file=deploy_melbourne_20170329T202458_701b.fdcdb</pre></td>
</tr>
</table>

Procedure 3. Recovery Scenario 3

21. ☐	**PMAC**: Repeat for each rack mount server configuration file	Repeat steps 13. -20. for each rack mount server/configuration file, if required.

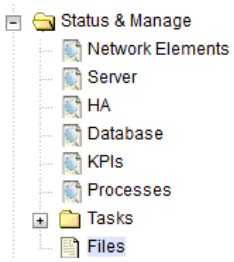
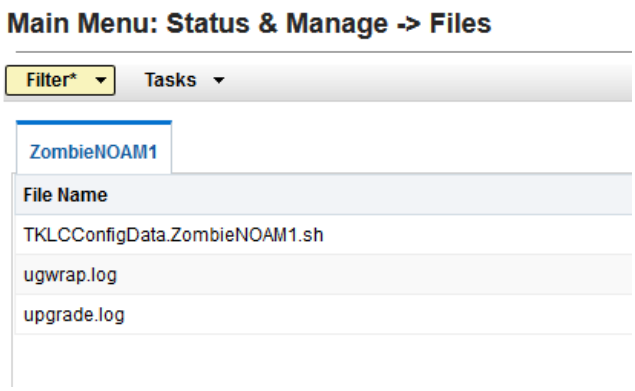
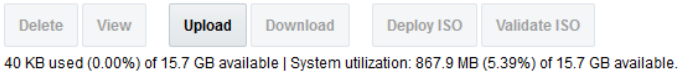
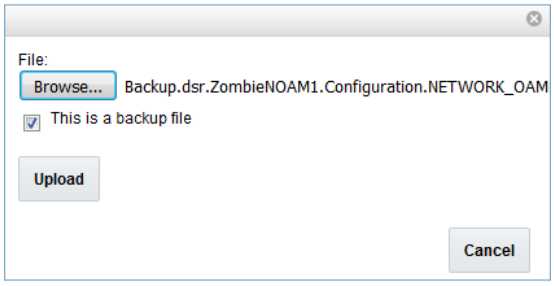
22. ☐	**PMAC**: Back up FDC file	1. Copy the updated fdc file to the fdc backup directory:
		`$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> /usr/TKLC/smac/etc/fdc/`
		2. Change permissions:
		`$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/<fdc_file>`

23. ☐	Perform CPU pinning	Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the **CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only)** procedure from reference [8].
24. ☐	Obtain latest database backup and network configuration data	1. Obtain the most recent database backup file from external backup sources (for example, file servers) or tape backup sources. 2. Obtain most recent **RADIUS shared secret encryption key** from the **DpiKf.bin.encr** file on external backup sources (only when the RADIUS key revocation MOP has been executed on the system). 3. 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.
25. ☐	Execute DSR installation procedure for the first NOAM	Verify the networking data for network elements. ***Notes*** • Use the backup copy of network configuration data and site surveys from step 2. • SDS disaster recovery actions can and should be worked simultaneously to allow faster recovery of the complete solution (that is, stale DB on DP servers do not receive updates until SDS-SOAM servers are recovered). The following steps accommodate both DSR and SDS disaster recovery steps. ***Important***: While creating the first NOAMs in this step, it is important that the server hostname is the same as one of the NOAM hostnames used prior to the disaster. **DSR**: 1. Configure the first NOAM server by executing the **Configure First NOAM NE and Server** procedure from reference [8]. 2. Configure the NOAM server group by executing the **Configure the NOAM Server Group** procedure from reference [8]. **SDS**: 3. Configure the first SDS NOAM server by executing **Configure First SDS NOAM NE and Server** procedure from reference [8]. 4. Configure the SDS NOAM server group by executing the **Configure the SDS NOAM Server Group** procedure from reference [8]. 5. Skip to step 31.

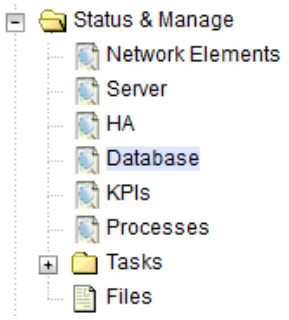
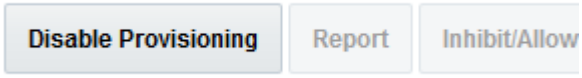
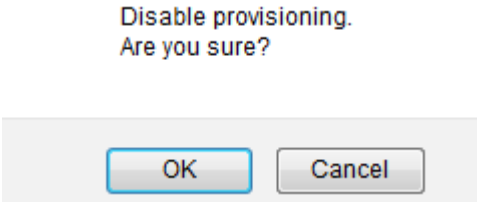
Procedure 3. Recovery Scenario 3

26. ☐	**NOAM GUI**: Login DSR only. If SDS, skip to step 31. If the failed server is not OAM, then skip to step 37.	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: 

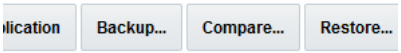
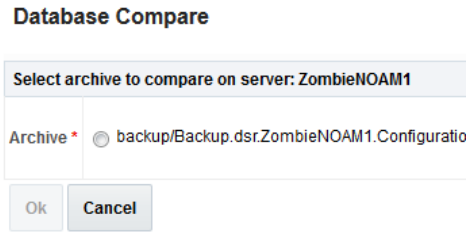
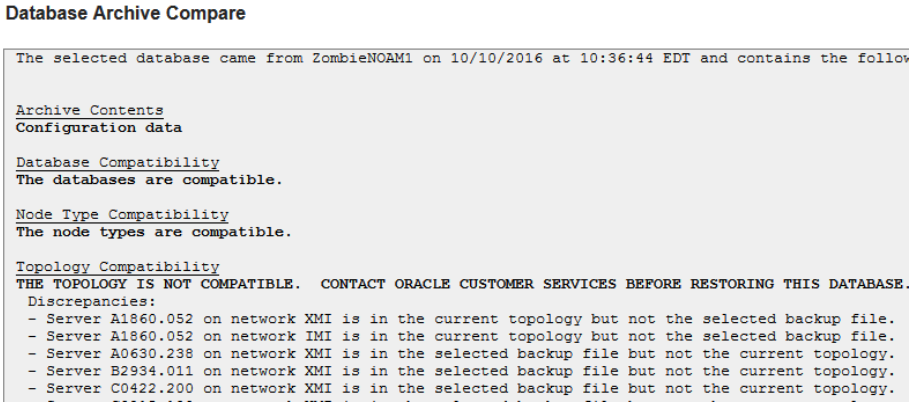
Procedure 3. Recovery Scenario 3

27. ☐	**NOAM GUI**: Upload the backup database file. DSR only. If SDS, skip to step 31.	1. Navigate to **Status & Manage > Files**.  2. Select the active NOAM server.  3. Click **Upload** and select the **NO Provisioning and Configuration** file backed up after initial installation and provisioning.  4. Click **Browse** and locate the backup file. ***Note:*** If there is no backup file, refer to Appendix L Backup Directory to create the backup directory. 5. Click **Open**. 6. Mark the **This is a backup file** checkbox. 7. Click **Upload**.  The file takes a few seconds to upload depending on the size of the backup data. The file is visible on the list of entries after the upload is complete.

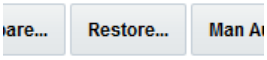
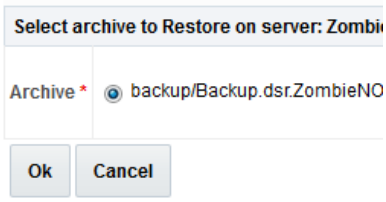
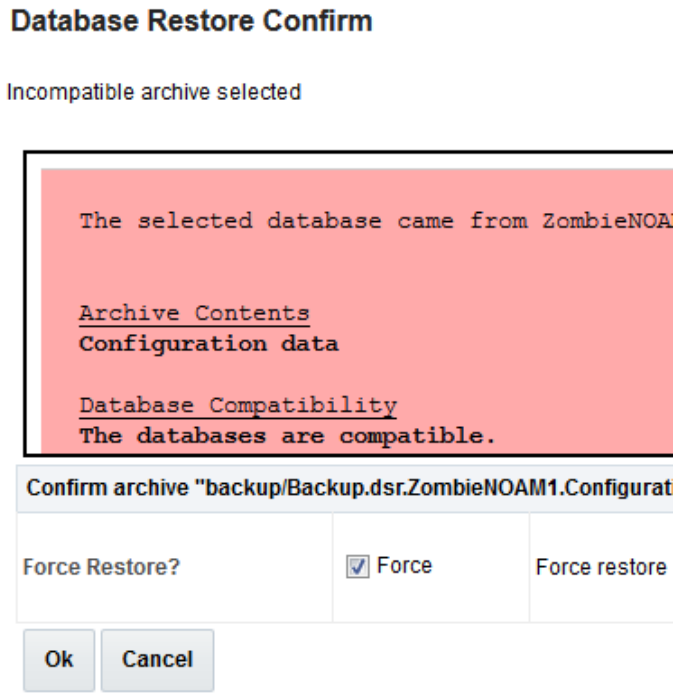
Procedure 3. Recovery Scenario 3

28. ☐	**NOAM GUI**: Disable provisioning. DSR only. If SDS, skip to step 31.	1. Navigate to **Status & Manage > Database**.  2. Click **Disable Provisioning**.  3. Click **OK** to disable Provisioning. 

Procedure 3. Recovery Scenario 3

29. ☐	**NOAM GUI**: Verify the archive contents and database compatibility. DSR only. If SDS, skip to step 31.	1. Select the active NOAM server and click **Compare**.  2. Click the button for the restored database file uploaded as a part of step 27. 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 3. Recovery Scenario 3

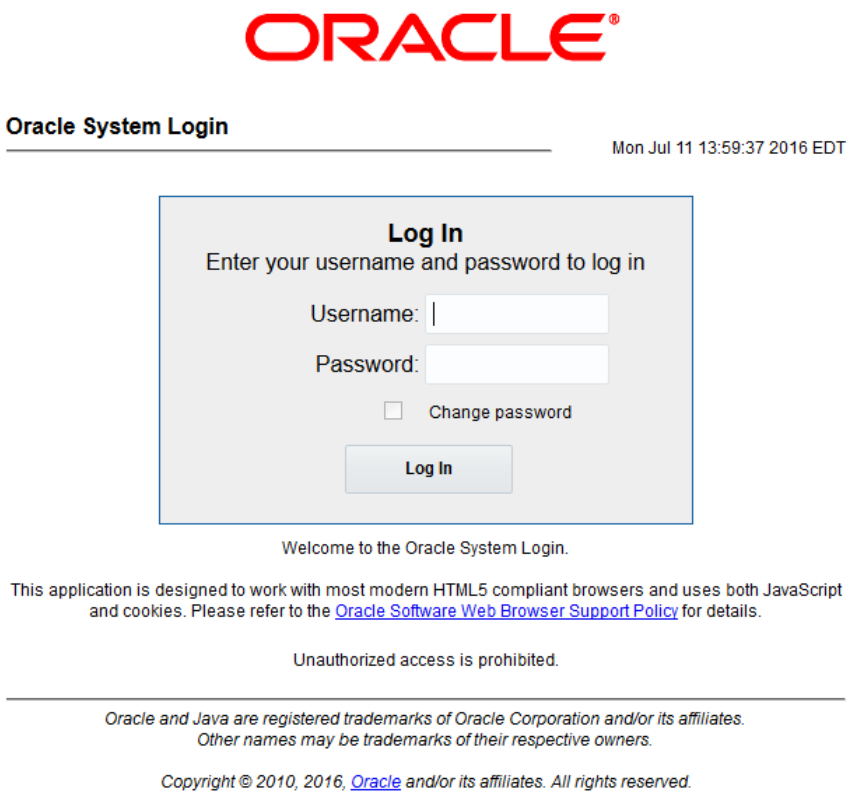
30. ☐	**Active NOAM**: Restore the database. DSR only. If SDS, skip to step 31.	1. From **Status & Manage > Database**. 2. Select the active NOAM server and click **Restore**.  3. Select the proper backup provisioning and configuration file.  4. Click **OK**. 5. If you get errors related to the warnings highlighted in the previous step, then it is expected. If no other errors display, then 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 the XMI NO GUI since the restored topology is old data. 6. Go to step 37.

Procedure 3. Recovery Scenario 3

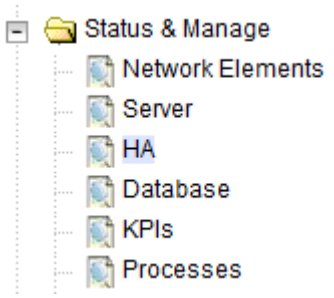
31. ☐	**SDS NOAM**: Transfer SDS configuration and provisioning backup database files.
	SDS only. If DSR, skip to step 37.
		Using the IP of the recovered SDS NOAM, transfer the uncompressed backup database files to the **/var/TKLC/db/filemgmt** directory.
		Linux:
		1. From the command line of a Linux machine, copy the configuration backup file to the SDS NOAM guest:
		`# scp <path_to_configuration_db_file> admusr@<SDS_NOAM_IP>:/var/TKLC/db/filemgmt`
		2. From the command line of a Linux machine, copy the provisioning backup file to the SDS NOAM guest:
		`# scp < path_to_provisioning_db _file> admusr@<SDS_NOAM_IP>:/var/TKLC/db/filemgmt`
		where **<path_to_db_file>** is the path to the backup database file on the local system and **<SDS_NOAM_IP>** is the recovered SDS NOAM IP address.
		Windows:
		Use WinSCP to copy the backup database files into the **/var/TKLC/db/filemgmt** directory. Refer to the **Using WinSCP** procedure in reference [9] to copy the backup image to the customer system.

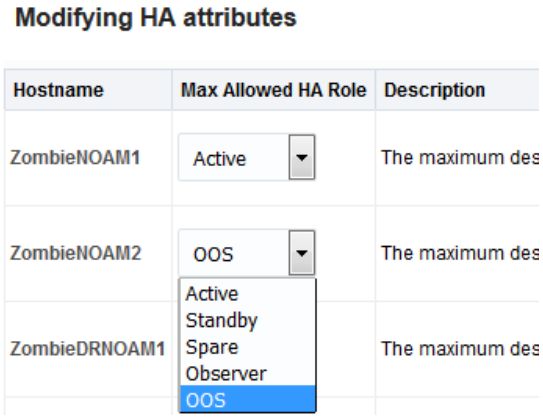
32. ☐	**SDS NOAM**: Login. SDS only. If DSR, skip to step 37.	Establish an SSH session to the SDS active NOAM XMI IP address and login as **admusr**.
33. ☐	**SDS NOAM**: Stop running applications. SDS only. If DSR, skip to step 37.	Issue the following command to stop running applications. Leave database running: `$ sudo prod.stop --ignore-cap` ***Note:*** This step may take several minutes to complete.
34. ☐	**SDS NOAM**: Restore configuration database. SDS only. If DSR, skip to step 37.	Restore the configuration DB by executing the following command: `$ sudo idb.restore -n -t /var/TKLC/db/filemgmt -v <full path to configuration archive file name>`
35. ☐	**SDS NOAM**: Restore provisioning database. SDS only. If DSR, skip to step 37.	Refer to Appendix I Restore Provisioning Database to restore the provisioning database.
36. ☐	**SDS NOAM**: Start running applications. SDS only. If DSR, skip to step 37.	Start the SDS application by executing the following command: `$ sudo prod.start`

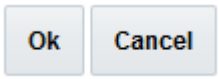
Procedure 3. Recovery Scenario 3

37. ☐	**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: 
38. ☐	**NOAM VIP GUI**: Monitor and confirm database restore	1. Wait for **5-10 minutes** for the system to stabilize with the new topology: 2. Monitor the Info tab for **Success**. This indicates the restore is complete and the system is stabilized. Ignore these alarms for NOAM and MP servers until all the servers are configured: • Alarms with Type Column as **REPL**, **COLL, HA** (with mate NOAM), **DB** (about Provisioning Manually Disabled). ***Notes***: • Do not pay attention to alarms until all the servers in the system are completely restored. • The Configuration and Maintenance information is in the same state it was when backed up during initial backup.

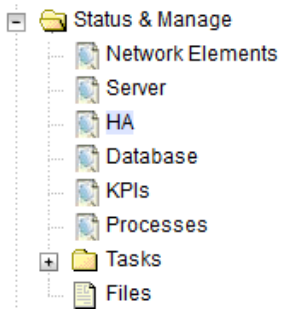
Procedure 3. Recovery Scenario 3

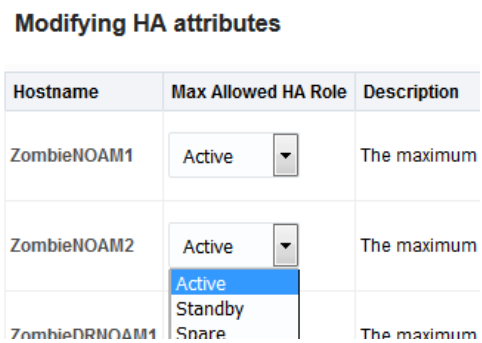
<table>
<tr>
<td>39. ☐</td>
<td>Active NOAM:
Set failed servers to OOS</td>
<td>1. Navigate to Status & Manage > HA.
 

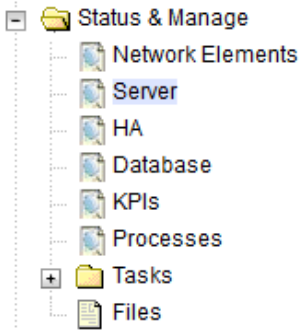
2. Click Edit.
3. Set the Max Allowed HA Role option to OOS for the failed servers.
 

4. Click OK.
 
</td>
</tr>
<tr>
<td>40. ☐</td>
<td>NOAM VIP GUI:
Recover standby NOAM</td>
<td>Install the second NOAM server:
DSR:
Execute the Configure the Second NOAM Server procedure, steps 1, 3-6, from reference [8].
SDS:
Execute the Configure the Second SDS NOAM Server procedure, steps 1, 3-6, from reference [8].</td>
</tr>
<tr>
<td>41. ☐</td>
<td>Install NetBackup client (optional)</td>
<td>If NetBackup is used, execute the Install NetBackup Client (Optional) procedure from reference [8].</td>
</tr>
</table>

Procedure 3. Recovery Scenario 3

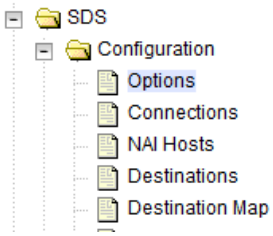
<table>
<tr>
<td>42. ☐</td>
<td>NOAM VIP GUI:
Set HA on standby NOAM</td>
<td>1. Navigate to Status & Manage > HA.
 

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

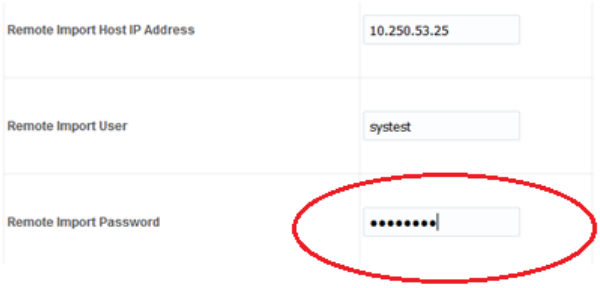
4. Click OK.</td>
</tr>
<tr>
<td>43. ☐</td>
<td>NOAM VIP GUI:
Restart DSR application</td>
<td>1. Navigate to Status & Manage > Server.
 

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

Procedure 3. Recovery Scenario 3

<table>
<tr>
<td>44. ☐</td>
<td>Active NOAM: Correct the recognized authority table</td>
<td>1. Establish an SSH session to the active NOAM and login as admusr.
2. Execute this command:
<pre>$ sudo top.setPrimary
- Using my cluster: A1789
- New Primary Timestamp: 11/09/15 20:21:43.418
- Updating A1789.022: <DSR_NOAM_B_hostname>
- Updating A1789.144: <DSR_NOAM_A_hostname></pre></td>
</tr>
<tr>
<td>45. ☐</td>
<td>NOAM VIP GUI: Perform Keyexchange with remote import server.
SDS only. If DSR, skip to step 47.</td>
<td>1. Navigate to SDS > Configuration > Options.
 

2. Unmark the Remote Import Enabled checkbox.
 

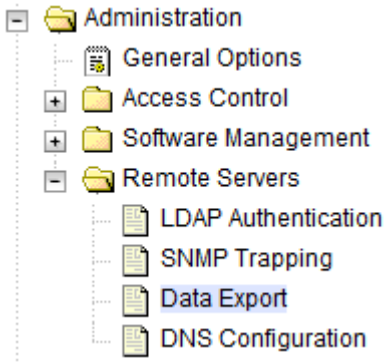
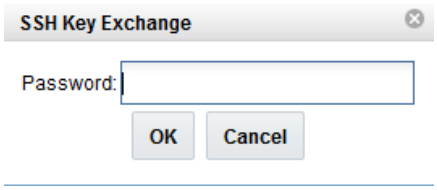
3. Click Apply.
Note: Navigate to SDS > Configuration > Options again to clear the banner.
4. Enter the Remote Import Password.
 

5. Click Apply.
 

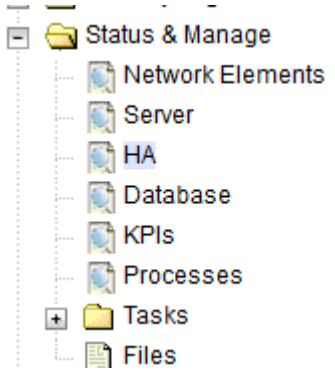
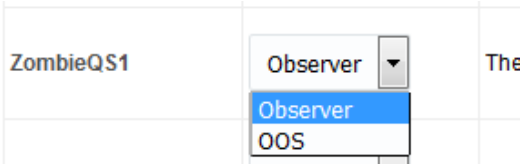
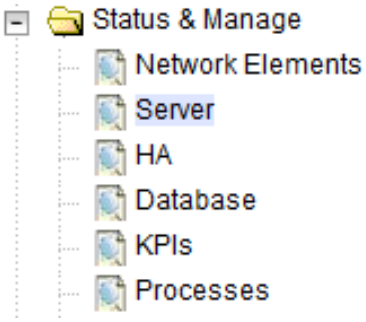
Note: Navigate to SDS > Configuration > Options again to clear the banner.
6. Mark the Remote Import Enabled checkbox.
 

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

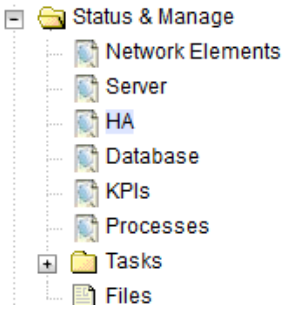
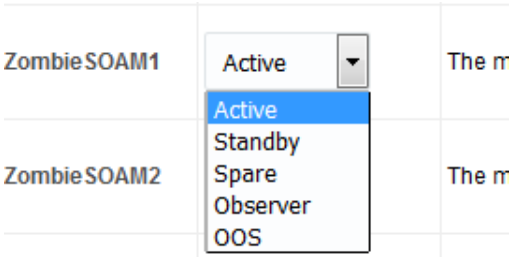
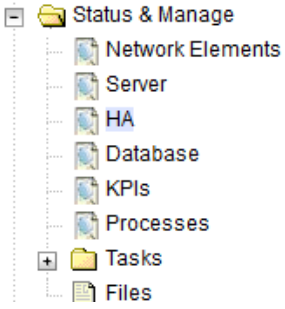
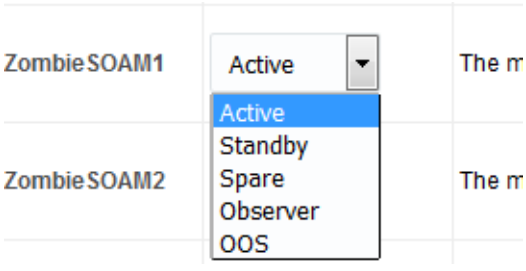
Procedure 3. Recovery Scenario 3

46. ☐	**NOAM VIP GUI**: Repeat for remote export server. SDS only. If DSR, skip to step 47.	Repeat step 45. for the remote export server.
47. ☐	**NOAM VIP GUI**: Perform Keyexchange with export server	1. Navigate to **Administration > Remote Servers > Data Export**.  2. Click **SSH Key Exchange**.  3. Type the **Password** and click **OK**. 
48. ☐	**NOAM VIP GUI**: Recover query servers. SDS only. If DSR, skip to step 51.	Execute the **Configuring SDS Query Servers** procedure, steps 1, 4-7, from reference [8].

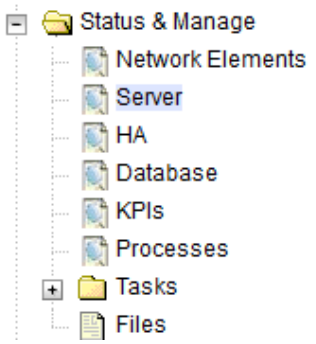
Procedure 3. Recovery Scenario 3

49. ☐	**SDS NOAM VIP GUI**: Set HA on query server. SDS only. If DSR, skip to step 51.	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Select the query server and select **Observer**.  4. Click **OK**.
50. ☐	**SDS NOAM VIP GUI**: Restart SDS application. SDS only. If DSR, skip to step 51.	1. Navigate to **Status & Manage > Server**.  2. Select the recovered query server and click **Restart**. 
51. ☐	**NOAM VIP GUI**: Recover the remaining SOAM servers (standby, spare)	**DSR**: Execute the **Configure the SOAM Servers** procedure, steps 1-3 and 5-9, from reference [8]. ***Note:*** If you are using NetBackup, also execute step 12. **SDS**: Execute the **Configure the SDS DP SOAM Servers** procedure, steps 1-3 and 5-8, from reference [8].

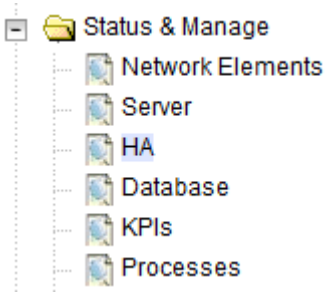
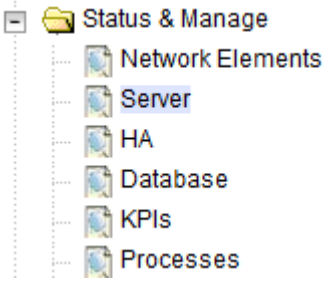
Procedure 3. Recovery Scenario 3

52. ☐	**NOAM VIP GUI**: Set HA on SOAM server	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Select the SOAM server and set it to **Active**.  4. Click **OK**.
53. ☐	**NOAM VIP GUI**: Set HA on the SOAM server	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Select the SOAM server and set it to **Active**.  4. Click **OK**.

Procedure 3. Recovery Scenario 3

54. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered SOAM server and click **Restart**. 
55. ☐	Activate PCA feature. DSR only. If SDS, skip this step.	If you have PCA installed in the system being recovered, re-activate PCA by executing the **PCA Activation on Active NOAM Network** procedure on the recovered active NOAM server and the **PCA Activation on Stand By SOAM Network** procedure on the recovered standby SOAM from reference [7].
56. ☐	**NOAM VIP GUI**: Recover the C-level servers (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs	**DSR**: Execute the **Configure the MP Servers** procedure, steps 1 and 9-13, from reference [8]. ***Note:*** Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. **SDS**: Execute the **Configure the SDS DP Servers** procedure, steps 1 and 5-8, from reference [8], Repeat this step for any remaining failed MP servers.

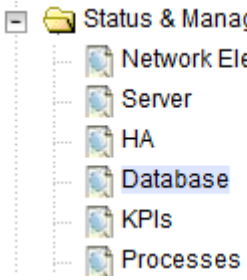
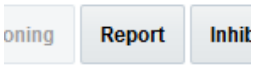
Procedure 3. Recovery Scenario 3

57. ☐	**NOAM VIP GUI**: Set HA on all C-level servers	1. Navigate to **Status & 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**.
58. ☐	**NOAM VIP GUI**: Restart DSR application on recovered C-level servers	1. Navigate to **Status & Manage > Server**.  2. Select the recovered C-level servers and click **Restart**. 
59. ☐	**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

60. ☐	**Active NOAM**: Activate optional features. DSR only. If SDS, then skip to next step.	Establish an SSH session to the active NOAM and login as **admusr**. **Note for PCA Feature Activation:** If you have PCA installed in the system being recovered, re-activate the PCA by executing the **PCA Activation on Active NOAM Server** procedure on recovered active NOAM server and the **PCA Activation on Standby SOAM Server** procedure on the recovered standby SOAM server from [6]. ***Notes***: • If not all SOAM sites are recovered at this point, then repeat the activation for each "new" SOAM site that comes online. • If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature. Refer to section 1.5 Optional Features to activate any features that were previously activated. ***Note:*** While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored: `iload#31000{S/W Fault}`

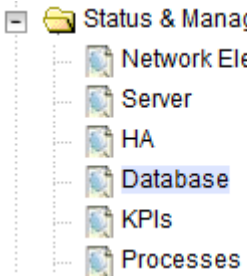
Procedure 3. Recovery Scenario 3

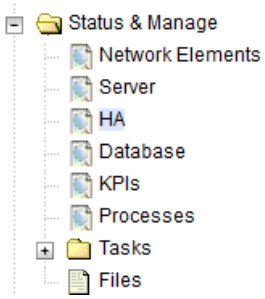
61. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status & Manage > Database**.
		 
		2. Select the active NOAM server and click **Report**.
		 
		The following screen displays:
		Main Menu: Status & Manage -> Database [Report]
		`dsr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

Procedure 3. Recovery Scenario 3

62. ☐	**Active NOAM**: Verify replication between servers	1. Log into the active NOAM as **admusr** using SSH terminal.
		2. Execute this command:
		`$ sudo irepstat –m`
		Example output:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`Oahu-DAMP-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.15%cpu 25B/s  A=me`
		`  CC To  Oahu-DAMP-2  Active  0  0.10  0.14%cpu 25B/s  A=me`
		`Oahu-DAMP-2 -- Stby`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.11%cpu 31B/s  A=C3642.212`
		`  CC From Oahu-DAMP-1  Active  0  0.10 ^0.14 1.16%cpu 31B/s A=C3642.212`
		`Oahu-IPFE-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 24B/s  A=C3642.212`
		`Oahu-IPFE-2 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 28B/s  A=C3642.212`
		`Oahu-NOAM-1 -- Stby`
		`  AA From Oahu-NOAM-2  Active  0  0.25 ^0.03%cpu 23B/s`
		`Oahu-NOAM-2 -- Active`
		`  AA To  Oahu-NOAM-1  Active  0  0.25 1%R 0.04%cpu 61B/s`
		`  AB To  Oahu-SOAM-2  Active  0  0.50 1%R 0.05%cpu 75B/s`
		`Oahu-SOAM-1 -- Stby`
		`  BB From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 27B/s`
		`Oahu-SOAM-2 -- Active`
		`  AB From Oahu-NOAM-2  Active  0  0.50 ^0.03%cpu 24B/s`
		`  BB To  Oahu-SOAM-1  Active  0  0.50 1%R 0.04%cpu 32B/s`
		`  BC To  Oahu-IPFE-1  Active  0  0.50 1%R 0.04%cpu 21B/s`
		`  BC To  Oahu-SS7MP-2 Active  0  0.50 1%R 0.04%cpu 21B/s`
		`irepstat ( 40 lines) (h)elp (m)erged`

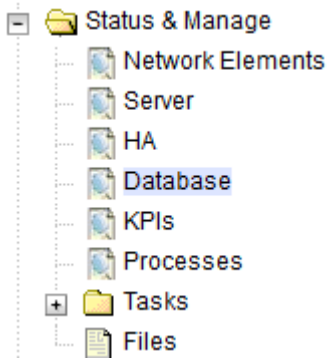
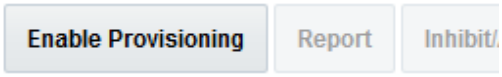
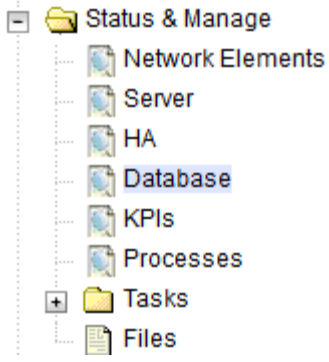
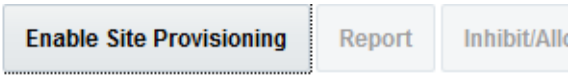
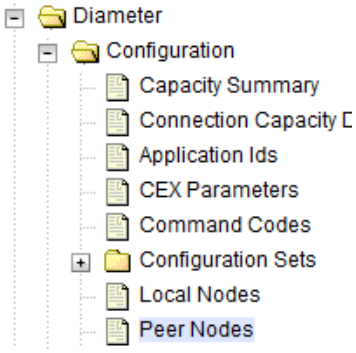
Procedure 3. Recovery Scenario 3

<table>
<tr>
<td>63. ☐</td>
<td>NOAM VIP GUI: Verify the database states</td>
<td>
1. Navigate to Status & Manager > Database.


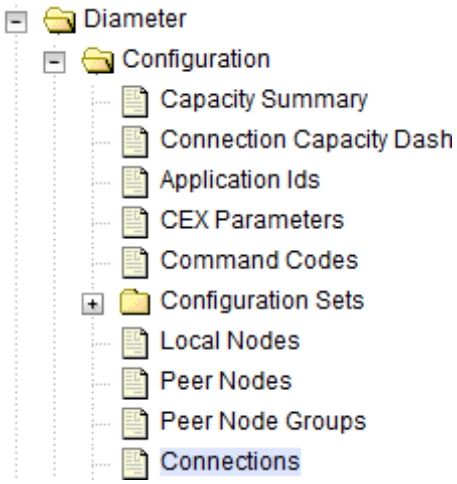
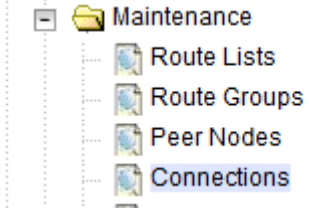
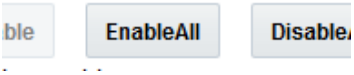
2. Verify the OAM Max HA Role is either Active or Standby for NOAM and SOAM; Application Max HA Role for MPs is Active; and status is Normal:
<table>
<tr><th>Network Element</th><th>Server</th><th>Role</th><th>OAM Max HA Role</th></tr>
<tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM1</td><td>Network OAM&P</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>64. ☐</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>

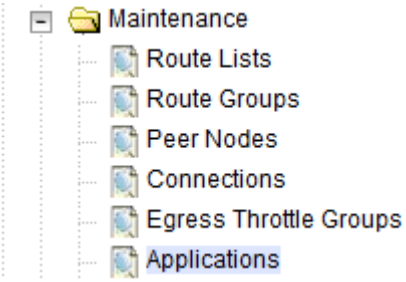
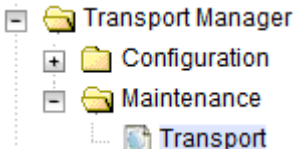
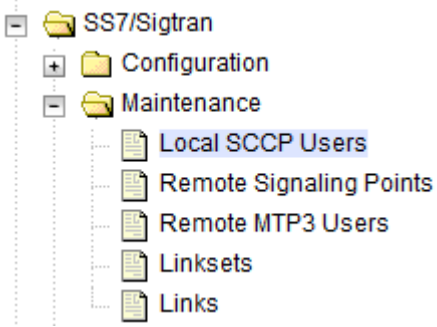
Procedure 3. Recovery Scenario 3

65. ☐	**NOAM GUI**: Enable provisioning	1. Navigate to **Status & Manage > Database**.  2. Click **Enable Provisioning**.  3. Click **OK**.
66. ☐	**SOAM GUI**: Enable site provisioning. DSR only. If SDS, then skip to step 75.	1. Navigate to **Status & Manage > Database**.  2. Click **Enable Site Provisioning**.  3. Click **OK**.
67. ☐	**SOAM VIP GUI**: Verify the peer node information. DSR only. If SDS, then skip to step 75.	1. Navigate to **Diameter > Configuration > Peer Node**.  2. Verify all the peer nodes are shown.

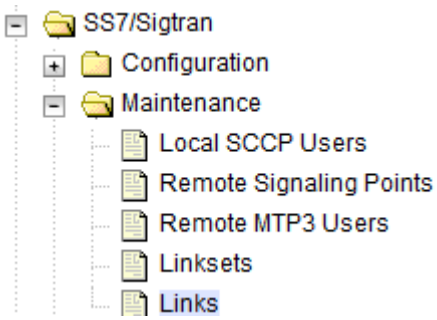
Procedure 3. Recovery Scenario 3

68. ☐	**SOAM VIP GUI**: Verify the connections information. DSR only. If SDS, then skip to step 75.	1. Navigate to **Diameter > Configuration > Connections**.  2. Verify all the connections are shown.
69. ☐	**MP Servers**: Disable SCTP Auth Flag (DSR only). DSR only. If SDS, then skip to step 75.	For SCTP connections without DTLS enabled, refer to the **Enable/Disable DTLS (SCTP Diameter Connections Only)** section in reference [8]. Execute this procedure on all failed MP servers.
70. ☐	**SOAM VIP GUI**: Enable connections, if needed. DSR only. If SDS, then skip to step 75.	1. Navigate to **Diameter > Maintenance > Connections**.  2. Select each connection and click **Enable**. Alternatively, enable all the connections by clicking **EnableAll**.  3. Verify the Operational State is **Available**. ***Note:*** If a disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution

Procedure 3. Recovery Scenario 3

71. ☐	**SOAM VIP GUI**: Enable optional features. DSR only. If SDS, then skip to step 75.	1. Navigate to **Diameter > Maintenance > Applications**.  2. Select the optional feature application configured in step 60. 3. Click **Enable**. 
72. ☐	**SOAM VIP GUI**: Re-enable transports, if needed. DSR only. If SDS, then skip to step 75.	1. Navigate to **Transport Manager > Maintenance > Transport**.  2. Select each transport and click **Enable**.  3. Verify the Operational Status for each transport is **Up**.
73. ☐	**SOAM VIP GUI**: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 75.	1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.  2. Click the **Enable** button corresponding to MAPIWF Application Name.  3. Verify the SSN Status is **Enabled**.

Procedure 3. Recovery Scenario 3

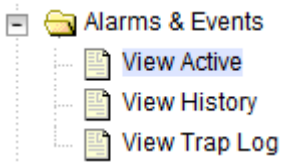
74. ☐	**SOAM VIP GUI**: Re-enable links, if needed. DSR only. If SDS, then skip to step 75.	1. Navigate to **SS7/Sigtran > Maintenance > Links**.  2. Click **Enable** for each link.  3. Verify the Operational Status for each link is **Up**.

75. ☐	**NOAM VIP**: Verify all servers in topology are accessible (RADIUS only)	If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.
		1. Establish an SSH session to the NOAM VIP and login as **admusr**.
		2. Check if all the servers in the topology are accessible:
		`$ /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo -checkAccess`
		Example output:
		`1450112012: [INFO] 'SOAM-2' is accessible.`
		`FIPS integrity verification test failed.`
		`The authenticity of host 'ipfe (10.240.146.16)' can't be established.`
		`RSA key fingerprint is ea:7f:0d:eb:56:4d:de:b1:5b:04:a3:fe:72:4e:c3:52.`
		`Are you sure you want to continue connecting (yes/no)? yes`
		`Warning: Permanently added 'ipfe,10.240.146.16' (RSA) to the list of known hosts.`
		`1450112015: [INFO] 'IPFE' is accessible.`
		`FIPS integrity verification test failed.`
		`The authenticity of host 'mp-2 (10.240.146.24)' can't be established.`
		`RSA key fingerprint is 73:ec:ac:d7:af:d2:78:dd:8e:bf:8e:79:a8:26:a7:b6.`
		`Are you sure you want to continue connecting (yes/no)? yes`
		`Warning: Permanently added 'mp-2,10.240.146.24' (RSA) to the list of known hosts.`
		`1450112017: [INFO] 'MP-2' is accessible.`
		`FIPS integrity verification test failed.`
		`The authenticity of host 'mp-1 (10.240.146.14)' can't be established.`
		`RSA key fingerprint is c5:66:85:6c:1d:c8:9f:78:92:2c:ca:8b:83:9b:ef:99.`
		`Are you sure you want to continue connecting (yes/no)? yes`
		`Warning: Permanently added 'mp-1,10.240.146.14' (RSA) to the list of known hosts.`
		`1450112020: [INFO] 'MP-1' is accessible.`
		Note: If any server is not accessible, stop and contact My Oracle Support (MOS).

Procedure 3. Recovery Scenario 3

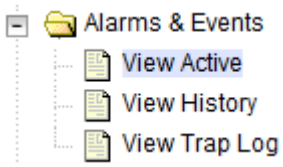
76. ☐	**SOAM VIP**: Copy key file to all the servers in topology (RADIUS only)	If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.
		1. Establish an SSH session to any active SOAM that remained intact and operational (Log into an active SOAM server that was not recovered or did not need recovery).
		2. Login as **admusr**.
		3. Check if the existing key file on active SOAM server is valid:
		`$ cd /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo –validate`
		Note: If output of above command shows that existing key file is not valid, contact My Oracle Support (MOS).
		4. Establish an SSH session to the active NOAM, login as **admusr**.
		5. Copy the key file to active NOAM:
		`$ cd /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo –copyKey –destServer <Active NOAM server name>`

Procedure 3. Recovery Scenario 3

<table>
<tr>
<td>77. ☐</td>
<td>NOAM VIP: Copy key file to all the servers in topology (RADIUS only)</td>
<td>
1. Establish an SSH session to any of the active NOAM. Login as admusr.
2. Copy the key file to all the servers in the topology:
<pre>$ cd /usr/TKLC/dpi/bin/
$ ./sharedKrevo –synchronize</pre>
Example output:
<pre>[admusr@NOAM-1 bin]$ ./sharedKrevo -synchronize
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450203505: [INFO] Key file on Active NOAM and NOAM-2 are same.
1450203505: [INFO] NO NEED to sync key file to NOAM-2.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450203506: [INFO] Key file on Active NOAM and SOAM-1 are same.
1450203506: [INFO] NO NEED to sync key file to SOAM-1.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450203506: [INFO] Key file on Active NOAM and SOAM-2 are same.
1450203506: [INFO] NO NEED to sync key file to SOAM-2.</pre>
<pre>$ ./sharedKrevo –updateData</pre>
Example output:
<pre>[admusr@NOAM-1 bin]$ ./sharedKrevo -updateData
1450203518: [INFO] Updating data on server 'NOAM-1'
1450203519: [INFO] Data updated to 'NOAM-1'
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450203520: [INFO] Updating data on server 'SOAM-2'
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450203522: [INFO] 1 rows updated on 'SOAM-2'...
1450203522: [INFO] Data updated to 'SOAM-2'</pre>
</td>
</tr>
<tr>
<td>78. ☐</td>
<td>SOAM VIP GUI: Examine all alarms</td>
<td>
1. Navigate to Alarms & Events > View Active.


2. Examine all active alarms and refer to the on-line help on how to address them.
If needed, contact My Oracle Support (MOS).
</td>
</tr>
</table>

Procedure 3. Recovery Scenario 3

79. ☐	**NOAM 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).
80. ☐	Back up and archive all the databases from the recovered system	Execute the **DSR Database Backup** procedure to back up the configuration databases.
81. ☐	Recover IDIH, if configured	If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.
82. ☐	SNMP workaround	Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases: 1. If SNMP is not configured in DSR/SDS. 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:

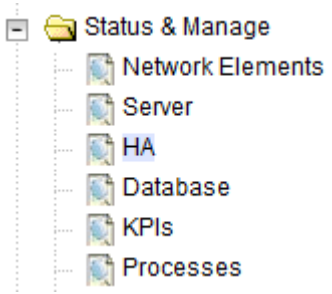
- Recover standby NOAM server by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover Query Server (if needed) by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
- Recover Standby SOAM server by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
- Recover MP/DP C-level servers by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.

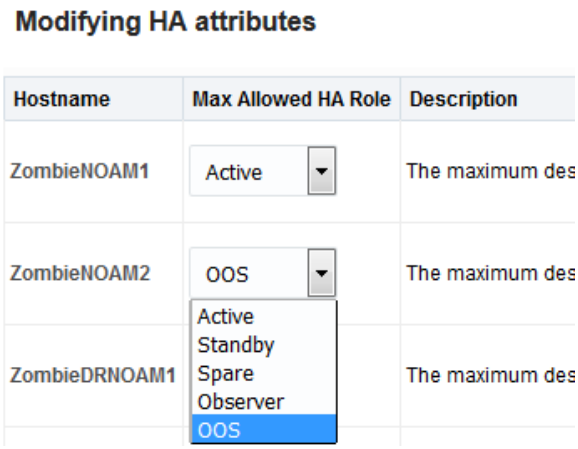
- Recover IDIH if necessary

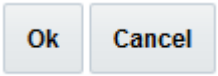
Procedure 4. Recovery Scenario 4

S T E P #	This procedure performs recovery if at least one 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 Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist. Refer to Appendix K 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.
3. ☐	Replace failed equipment	Work with the hardware vendor to replace the failed equipment.
4. ☐	**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

<table>
<tr>
<td>5. ☐</td>
<td>Active NOAM: Set failed servers to OOS</td>
<td>
1. Navigate to Status & Manage > HA.


2. Click Edit.
3. Set the Max Allowed HA Role option to OOS for the failed servers.


4. Click OK.


</td>
</tr>
<tr>
<td>6. ☐</td>
<td>Recover PMAC and PMAC TVOE Host: Configure BIOS settings and update firmware</td>
<td>
1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:

HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings
Oracle X5-2/Netra X5-2/X6-2/X7-2: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings
HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings

2. Verify and/or upgrade server firmware by executing the Upgrade Rack Mount Server Firmware procedure from reference [8].
</td>
</tr>
</table>

Procedure 4. Recovery Scenario 4

7. ☐	**Recover PMAC, TVOE Hosts, and Switch**: Backups available	If the PMAC is located on the failed rack mount server, execute this step; otherwise skip to step 10. This step assumes TVOE and PMAC backups are available. If backups are **NOT** available, **skip this step**. 1. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers. 2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup. 3. Proceed to step 9.
8. ☐	**Recover PMAC, TVOE Hosts, and Switch**: Backups NOT available	If the PMAC is located on the failed rack mount server, execute this step; otherwise skip to step 10. This step assumes TVOE and PMAC backups are **NOT** available. If the TVOE and PMAC have already been restored, **skip this step**. Execute these procedures from reference [8]: • **Install and Configure TVOE on First RMS (PMAC Host)** • **Install PMAC** • **Initialize the PMAC Application**
9. ☐	Configure PMAC (no backup)	If PMAC backup was **NOT** restored in step 7. , execute this step; otherwise, skip this step. Execute these procedures from reference [8]: • **Configure PMAC Server (NetBackup Only)** • **Add RMS to the PMAC Inventory**
10. ☐	Install/Configure additional rack mount servers	***Note:*** If TVOE backups are available, refer Appendix G Restore TVOE Configuration from Backup Media; otherwise, execute this step. If TVOE backups were **NOT** performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step. 1. Execute these procedures from reference [8]: • **Install TVOE on Additional Rack Mount Servers** • **Configure TVOE on Additional Rack Mount Servers** 2. Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]: • **HP DL380 Gen8**: Configure HP Gen 8 Server BIOS Settings • **Oracle X5-2/Netra X5-2/X6-2/X7-2**: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings • **HP DL380 Gen9**: Configure HP Gen9 Server BIOS Settings 3. Verify and/or upgrade server firmware by executing the **Upgrade Rack Mount Server Firmware** procedure from reference [8].

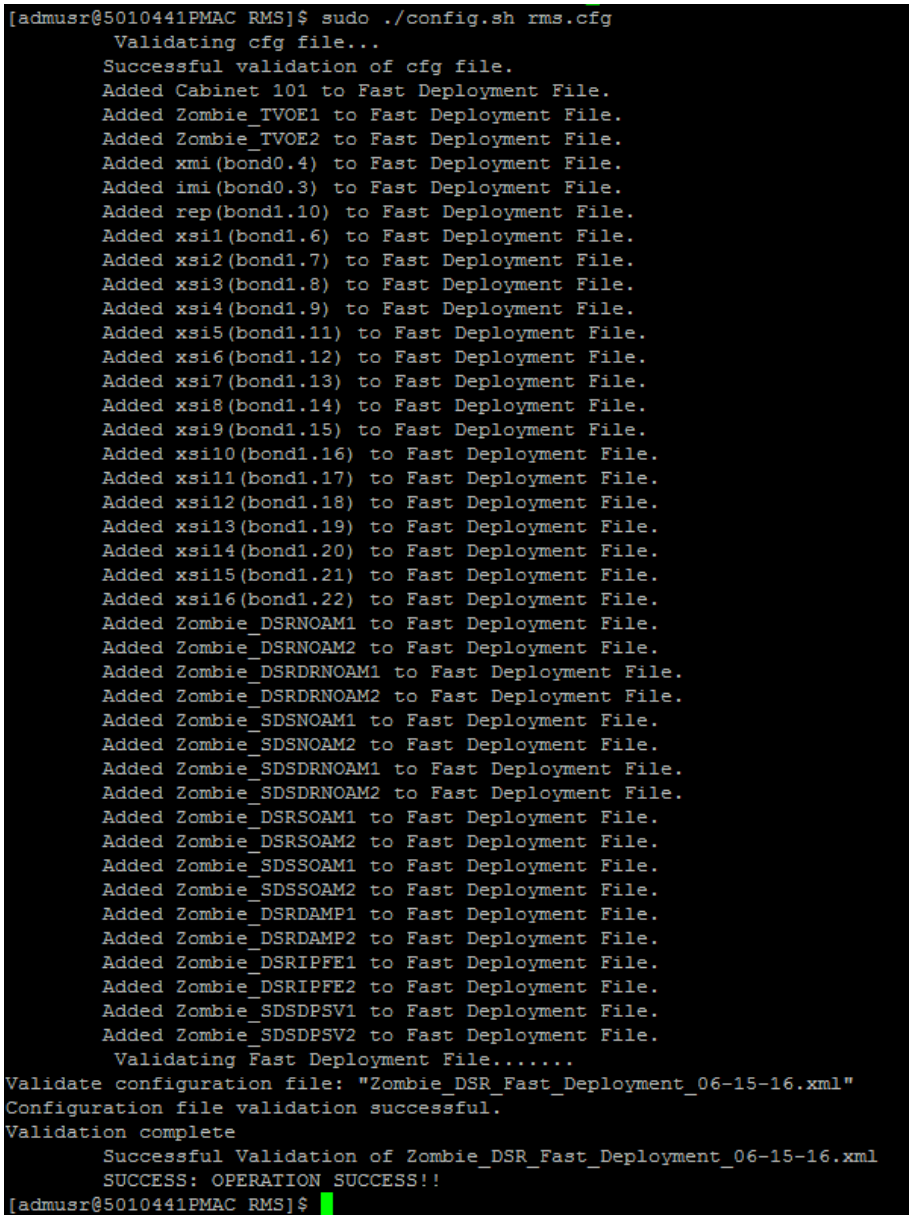
Procedure 4. Recovery Scenario 4

11. ☐	Determine VM placement and socket pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 only)	HP DL380 GEN 8, **skip this step**. Determine VM placement and pinning by following section 3.1, item 14.
12. ☐	Deploy redundant PMAC, if required	Refer to the **Deploy Redundant PMAC (Optional)** procedure to re-deploy and configure any redundant PMACs previously configured.
13. ☐	**PMAC**: Determine if the fdconfig file exists from the initial deployment	1. Type: `[admusr@melbourne-pmac-1 ~]$ ll /usr/TKLC/smac/etc/fdc/` 2. Examine the results and verify if the **rms config file <hostname>.cfg** exists. ***Note:*** There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS. 3. Skip to step 15.
14. ☐	Create fdconfig backup file, if it does not already exist	Execute this step ONLY If the fdconfig backup file does **NOT** exist. Create the needed file(s) by executing the **Virtual Machine/Network Fast Deployment** section from reference [8]. **WARNING** It is very important to ensure the file(s) created only affects the TVOE server(s) and the guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.
15. ☐	**PMAC**: Load ISOs into PMAC, if not done already	If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the **Virtual Machine/Network Fast Deployment** section from reference [8].
16. ☐	**PMAC**: Edit/Update configuration file	Edit the fdconfig file to include only the required/failed servers. ***Notes***: • Comment out configuration items that are not needed. • Create a separate configuration file for EACH rack mount server being deployed. • The Cabinet ID in the config file needs to match the cabinet already defined in PMAC. The following items are mandatory: • siteName • tpdIso • dsrIso (if DSR VMs are being configured) • sdsIso (if SDS VMs are being configured) • NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured)

Procedure 4. Recovery Scenario 4

		• XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured) • XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured) • DSRNOAM1XMIIPADDRESS (if DSRNOAM1 is being configured) • DSRNOAM2XMIIPADDRESS (if DSRNOAM2 is being configured) • DSRDRNOAM1XMIIPADDRESS (if DSRDRNOAM1 is being configured) • DSRDRNOAM2XMIIPADDRESS (if DSRDRNOAM2 is being configured) • SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured) • SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured) • SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured) • SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured) ***Notes***: • Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8]. • Comment out SDS and DSR profile items if corresponding products are not used. • For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9, refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8]. • VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName. • VM locations should not be changed from their **RMSx** format. Each RMS should correspond to a separate rack mount server. **WARNING** Ensure the file(s) created only affect the TVOE server(s) and guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.
17. ☐	**PMAC**: Copy the backed up fdc file to the RMS directory	Copy the fdconfig backup file to the RMS directory. `$ sudo cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file> /usr/TKLC/smac/etc/RMS/`

Procedure 4. Recovery Scenario 4

18. ☐	**PMAC**: Execute the config.sh script	Execute **config.sh** against the modified backup config file. ***Note:*** If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again. `$ sudo ./config.sh <config file>` Example output: 

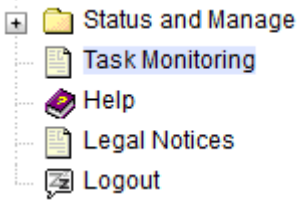
```
[admusr@5010441PMAC RMS]$ sudo ./config.sh rms.cfg
        Validating cfg file...
       Successful validation of cfg file.
       Added Cabinet 101 to Fast Deployment File.
       Added Zombie_TVOE1 to Fast Deployment File.
       Added Zombie_TVOE2 to Fast Deployment File.
       Added xmi(bond0.4) to Fast Deployment File.
       Added imi(bond0.3) to Fast Deployment File.
       Added rep(bond1.10) to Fast Deployment File.
       Added xsi1(bond1.6) to Fast Deployment File.
       Added xsi2(bond1.7) to Fast Deployment File.
       Added xsi3(bond1.8) to Fast Deployment File.
       Added xsi4(bond1.9) to Fast Deployment File.
       Added xsi5(bond1.11) to Fast Deployment File.
       Added xsi6(bond1.12) to Fast Deployment File.
       Added xsi7(bond1.13) to Fast Deployment File.
       Added xsi8(bond1.14) to Fast Deployment File.
       Added xsi9(bond1.15) to Fast Deployment File.
       Added xsi10(bond1.16) to Fast Deployment File.
       Added xsi11(bond1.17) to Fast Deployment File.
       Added xsi12(bond1.18) to Fast Deployment File.
       Added xsi13(bond1.19) to Fast Deployment File.
       Added xsi14(bond1.20) to Fast Deployment File.
       Added xsi15(bond1.21) to Fast Deployment File.
       Added xsi16(bond1.22) to Fast Deployment File.
       Added Zombie_DSRNOAM1 to Fast Deployment File.
       Added Zombie_DSRNOAM2 to Fast Deployment File.
       Added Zombie_DSRDRNOAM1 to Fast Deployment File.
       Added Zombie_DSRDRNOAM2 to Fast Deployment File.
       Added Zombie_SDSNOAM1 to Fast Deployment File.
       Added Zombie_SDSNOAM2 to Fast Deployment File.
       Added Zombie_SDSDRNOAM1 to Fast Deployment File.
       Added Zombie_SDSDRNOAM2 to Fast Deployment File.
       Added Zombie_DSRSOAM1 to Fast Deployment File.
       Added Zombie_DSRSOAM2 to Fast Deployment File.
       Added Zombie_SDSSOAM1 to Fast Deployment File.
       Added Zombie_SDSSOAM2 to Fast Deployment File.
       Added Zombie_DSRDAMP1 to Fast Deployment File.
       Added Zombie_DSRDAMP2 to Fast Deployment File.
       Added Zombie_DSRIPFE1 to Fast Deployment File.
       Added Zombie_DSRIPFE2 to Fast Deployment File.
       Added Zombie_SDSDPSV1 to Fast Deployment File.
       Added Zombie_SDSDPSV2 to Fast Deployment File.
        Validating Fast Deployment File.......
Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml"
Configuration file validation successful.
Validation complete
       Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml
       SUCCESS: OPERATION SUCCESS!!
[admusr@5010441PMAC RMS]$
```

Procedure 4. Recovery Scenario 4

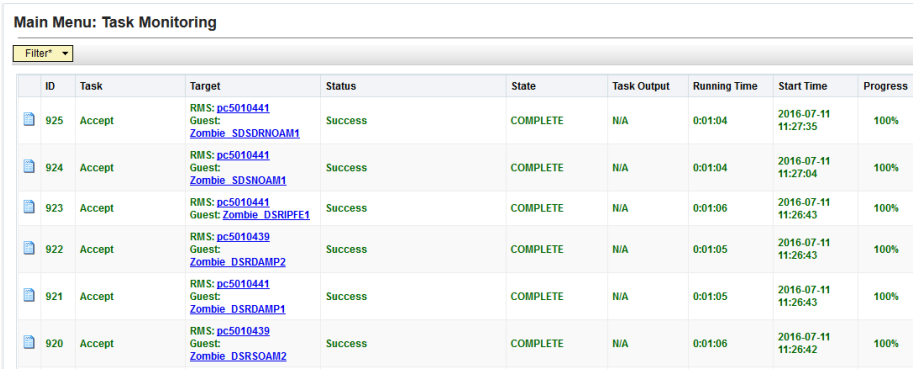
<table>
<tr>
<td>19. ☐</td>
<td>PMAC: Execute fast deployment</td>
<td>With the file generated from the config.sh script, execute the following command to start fast deployment:

<pre>$ screen
$ sudo fdconfig config --file=<fd_config.xml></pre>

Note: This is a long duration command. 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.</td>
</tr>
<tr>
<td>20. ☐</td>
<td>PMAC GUI: Monitor the configuration</td>
<td>1. If not already done, establish a GUI session on the PMAC server.
2. Navigate to Task Monitoring.



3. Monitor the configuration to completion:



Note: If a failure occurs with fdconfig, logs can be accessed in /var/TKLC/log/fdconfig/fdconfig.log file.

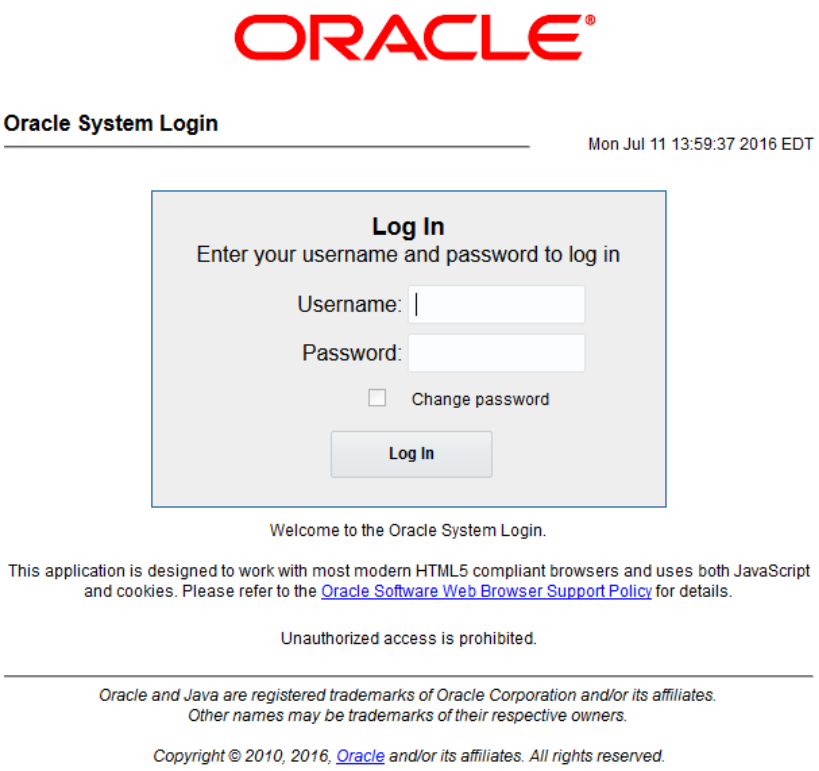
<pre>[admusr@melbourne-pmac-1 fdconfig]$ sudo fdconfig dumpsteps --file=deploy_melbourne_20170329T202458_701b.fdcdb
Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb"
Here are the steps that were generated
--------------- begin ----------------
Dump of DB steps:
NUM PHS DLY INFRA ID SVRTYPE CMD ELEMENT PRE STATE TO BGTS COMMAND TEXT
----
1 1 0 pmac Fast_Deployment 0 21 0 Complete 300 0 Check PM&C is available
2 1 0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet
3 1 0 pmac Fast_Deployment 0 3 melbourne_RMS3 1 Skipped 900 0 Add Rms
4 2 0 pmac Fast_Deployment 1</pre>
4. Restart the fdconfig after a failure has occurred and has been resolved:

<pre>$ sudo fdconfig restart --file=deploy_melbourne_20170329T202458_701b.fdcdb</pre></td>
</tr>
</table>

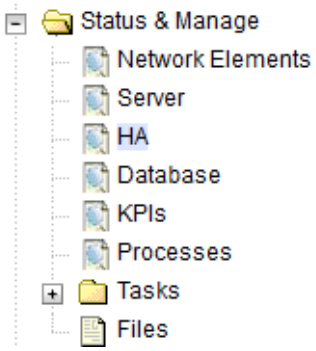
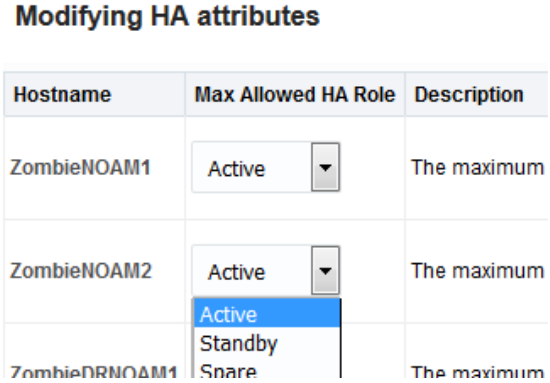
Procedure 4. Recovery Scenario 4

21. ☐	**PMAC**: Repeat for each rack mount server configuration file	Repeat steps 13. -20. for each rack mount server/configuration file, if required.

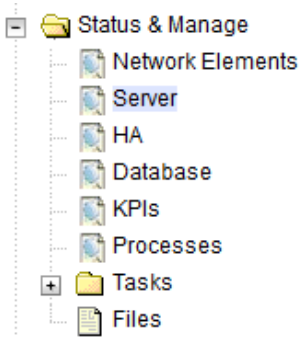
22. ☐	**PMAC**: Back up FDC file	1. Copy the updated fdc file to the fdc backup directory:
		`$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> /usr/TKLC/smac/etc/fdc/`
		2. Change permissions:
		`$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/<fdc_file>`

23. ☐	Perform CPU pinning	Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the **CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only)** procedure from reference [8].
24. ☐	**NOAM GUI**: Login If the failed server is not OAM, then skip to step 47.	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

25. ☐	**NOAM VIP GUI**: Recover standby NOAM, if needed	Install the second NOAM server: **DSR**: Execute the **Configure the Second NOAM Server** procedure, steps 1 and 3-6, from reference [8]. **SDS**: Execute the **Configure the Second SDS NOAM Server** procedure, steps 1 and 3-6, from reference [8].
26. ☐	Install NetBackup client (optional)	If NetBackup is used, execute the **Install NetBackup Client (Optional)** procedure from reference [8].
27. ☐	**NOAM VIP GUI**: Set HA on standby NOAM	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Select the standby NOAM server and set it to **Active**.  4. Click **OK**.

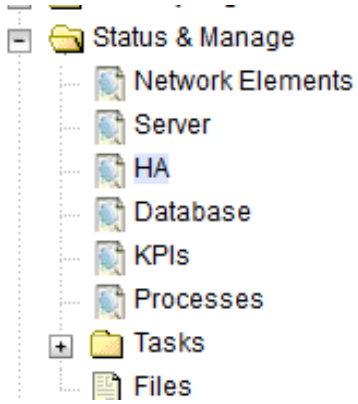
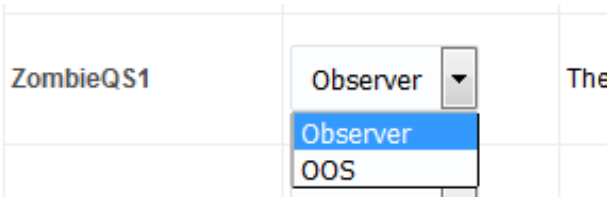
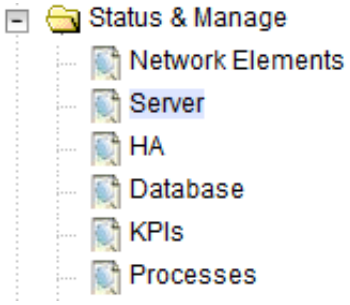
Procedure 4. Recovery Scenario 4

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

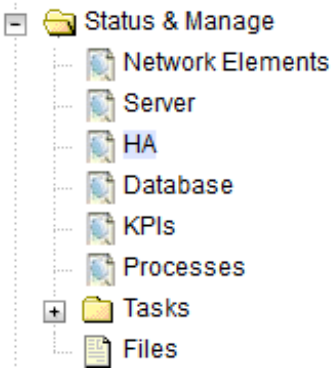
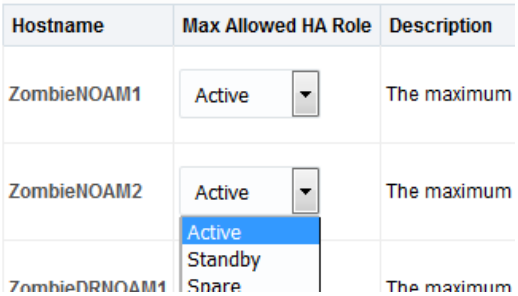
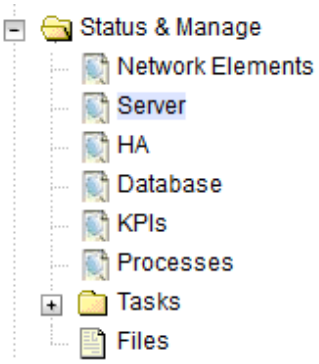
29. ☐	**Active NOAM**: Correct the recognized authority table	1. Establish an SSH session to the active NOAM and login as **admusr**.
		2. Execute this command:
		`$ sudo top.setPrimary`
		`- Using my cluster: A1789`
		`- New Primary Timestamp: 11/09/15 20:21:43.418`
		`- Updating A1789.022: <DSR_NOAM_B_hostname>`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

30. ☐	**NOAM VIP GUI**: Recover query servers. SDS only. If DSR, skip to step 33.	Execute the **Configuring SDS Query Servers** procedure, steps 1 and 4-7, from reference [8].

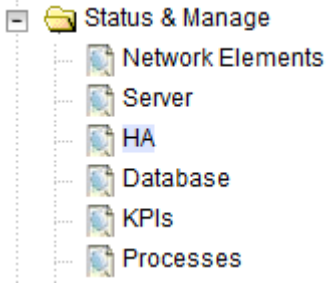
Procedure 4. Recovery Scenario 4

31. ☐	**SDS NOAM VIP GUI**: Set HA on query server. SDS only. If DSR, skip to step 33.	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Select the query server and select **Observer**.  4. Click **OK**.
32. ☐	**SDS NOAM VIP GUI**: Restart SDS application. SDS only. If DSR, skip to step 33.	1. Navigate to **Status & Manage > Server**.  2. Select the recovered query server and click **Restart**. 
33. ☐	**NOAM VIP GUI:** Recover the SOAM servers (**Standby, Spare —** Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only)	**DSR:** Execute the **Configure the SOAM Servers** procedure, steps 1-3 and 5-9, from reference [8]. ***Note:*** If you are using NetBackup, also execute step 12. **SDS:** Execute the **Configure the SDS DP SOAM Servers** procedure, steps 1-3 and 5-8, from reference [8].

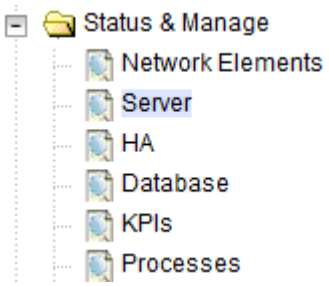
Procedure 4. Recovery Scenario 4

34. ☐	**NOAM VIP GUI**: Set HA on standby NOAM	1. Navigate to **Status & Manage > HA**.  2. Click **Edit**. 3. Select the standby NOAM server and set it to **Active**. **Modifying HA attributes**  4. Click **OK**.
35. ☐	**NOAM VIP GUI**: Restart DSR application	1. Navigate to **Status & Manage > Server**.  2. Select the recovered standby NOAM server and click **Restart**. 
36. ☐	Activate PCA feature. DSR only. If SDS, skip this step.	If you have PCA installed in the system being recovered, re-activate PCA by executing the **PCA Activation on Active NOAM Network** procedure on the recovered standby NOAM server and the **PCA Activation on Stand By SOAM Network** procedure on the recovered standby SOAM from reference [7].

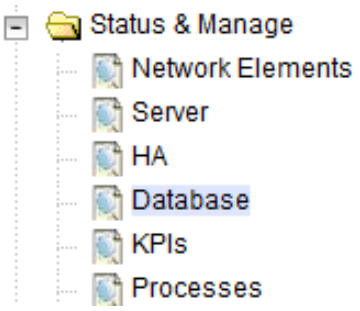
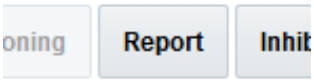
Procedure 4. Recovery Scenario 4

37. ☐	**NOAM VIP GUI**: Recover the C-level servers (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs	**DSR**: Execute the **Configure the MP Servers** procedure, steps 1 and 9-13, from reference [8]. ***Note:*** Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. **SDS** — Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only: Execute the **Configure the SDS DP Servers** procedure, steps 1 and 5-8, from reference [8], Repeat this step for any remaining failed MP servers.
38. ☐	**NOAM VIP GUI**: Set HA on all C-level servers	1. Navigate to **Status & 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 4. Recovery Scenario 4

39. ☐	**NOAM VIP GUI**: Restart DSR application on recovered C-level servers	1. Navigate to **Status & Manage > Server**.  2. Select the recovered C-level servers and click **Restart**. 
40. ☐	**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.
41. ☐	**Active NOAM**: Activate optional features. DSR only. If SDS, then skip step 43.	Establish an SSH session to the active NOAM and login as **admusr**. **Note for PCA Feature Activation:** If you have PCA installed in the system being recovered, re-activate the PCA by executing the **PCA Activation on Active NOAM Server** procedure on recovered active NOAM server and the **PCA Activation on Standby SOAM Server** procedure on the recovered standby SOAM server from [6]. ***Notes***: • If not all SOAM sites are recovered at this point, then repeat the activation for each "new" SOAM site that comes online. • If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature. Refer to section 1.5 Optional Features to activate any features that were previously activated. ***Note:*** While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored: `iload#31000{S/W Fault}`
42. ☐	**MP Servers**: Disable SCTP Auth Flag (DSR only). DSR only. If SDS, then skip step 43.	For SCTP connections without DTLS enabled, refer to the **Enable/Disable DTLS (SCTP Diameter Connections Only)** section in reference [8]. Execute this procedure on all failed MP servers.

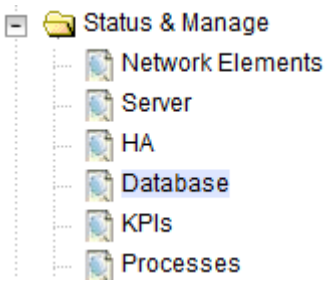
Procedure 4. Recovery Scenario 4

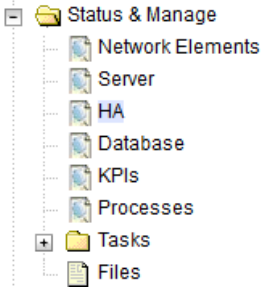
43. ☐	**NOAM VIP GUI**: Fetch and store the database report for the newly restored data and save it	1. Navigate to **Status & Manage > Database**.
		 
		2. Select the active NOAM server and click **Report**.
		 
		The following screen displays:
		Main Menu: Status & Manage -> Database [Report]
		`dsr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

Procedure 4. Recovery Scenario 4

44. ☐	**Active NOAM**: Verify replication between servers	1. Log into the active NOAM as **admusr** using SSH terminal.
		2. Execute this command:
		`$ sudo irepstat –m`
		Example output:
		`-- Policy 0 ActStb [DbReplication] ----------`
		`Oahu-DAMP-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.15%cpu 25B/s  A=me`
		`  CC To  Oahu-DAMP-2  Active  0  0.10  0.14%cpu 25B/s  A=me`
		`Oahu-DAMP-2 -- Stby`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.11%cpu 31B/s  A=C3642.212`
		`  CC From Oahu-DAMP-1  Active  0  0.10 ^0.14 1.16%cpu 31B/s A=C3642.212`
		`Oahu-IPFE-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 24B/s  A=C3642.212`
		`Oahu-IPFE-2 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 28B/s  A=C3642.212`
		`Oahu-NOAM-1 -- Stby`
		`  AA From Oahu-NOAM-2  Active  0  0.25 ^0.03%cpu 23B/s`
		`Oahu-NOAM-2 -- Active`
		`  AA To  Oahu-NOAM-1  Active  0  0.25 1%R 0.04%cpu 61B/s`
		`  AB To  Oahu-SOAM-2  Active  0  0.50 1%R 0.05%cpu 75B/s`
		`Oahu-SOAM-1 -- Stby`
		`  BB From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 27B/s`
		`Oahu-SOAM-2 -- Active`
		`  AB From Oahu-NOAM-2  Active  0  0.50 ^0.03%cpu 24B/s`
		`  BB To  Oahu-SOAM-1  Active  0  0.50 1%R 0.04%cpu 32B/s`
		`  BC To  Oahu-IPFE-1  Active  0  0.50 1%R 0.04%cpu 21B/s`
		`  BC To  Oahu-SS7MP-2 Active  0  0.50 1%R 0.04%cpu 21B/s`
		`irepstat ( 40 lines) (h)elp (m)erged`

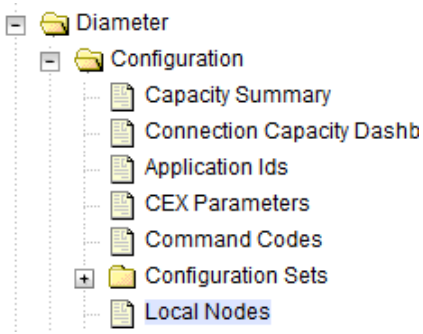
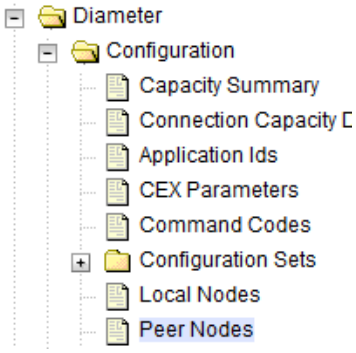
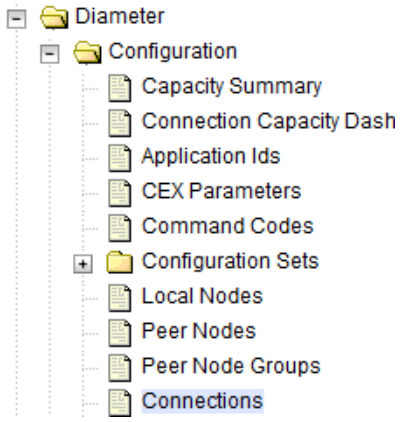
Procedure 4. Recovery Scenario 4

<table>
<tr>
<td>45. ☐</td>
<td>NOAM VIP GUI:
Verify the database states</td>
<td>
1. Navigate to Status & Manager > Database.


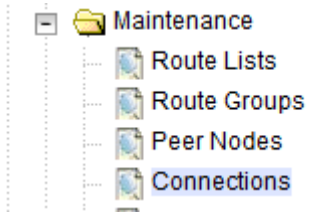
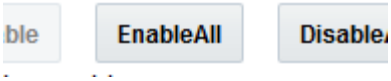
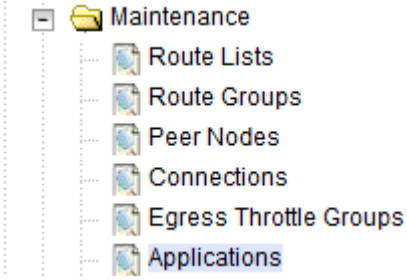
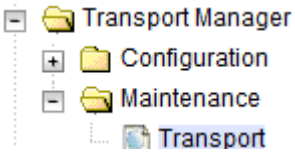
2. Verify the OAM Max HA Role as shown.
<table>
<tr><th>Role</th><th>Server Type</th><th>Expected HA Role(s)</th></tr>
<tr><td>Network OAM&P</td><td>NO</td><td>Active/Standby</td></tr>
<tr><td>SYSTEM OAM</td><td>SOAM</td><td>Active/Standby/Spare</td></tr>
<tr><td>MP</td><td>DA MP(s)
IPFE(s)
SS7MP(s)</td><td>Active</td></tr>
<tr><td>MP</td><td>SBR(s)</td><td>Active/Standby/Spare</td></tr>
</table>
3. Verify the Status and OAM Repl Status is Normal and Repl Status=Allowed.
</td>
</tr>
<tr>
<td>46. ☐</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>

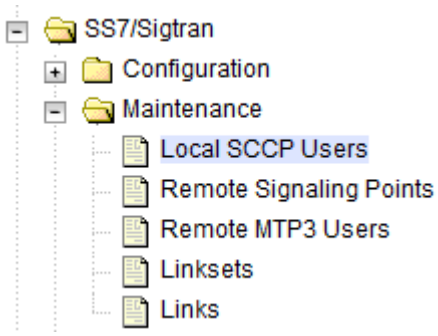
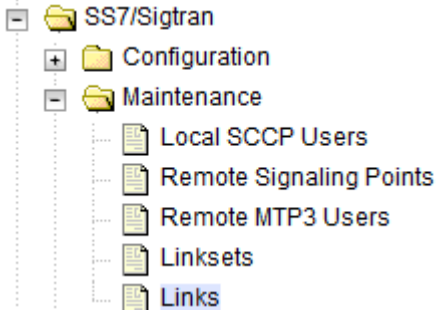
Procedure 4. Recovery Scenario 4

47. ☐	**SOAM VIP GUI**: Verify the local node information. DSR only. If SDS, then skip to step 56.	1. Navigate to **Diameter > Configuration > Local Node**.  2. Verify all the local nodes are shown.
48. ☐	**SOAM VIP GUI**: Verify the peer node information. DSR only. If SDS, then skip to step 56.	1. Navigate to **Diameter > Configuration > Peer Node**.  2. Verify all the peer nodes are shown.
49. ☐	**SOAM VIP GUI**: Verify the connections information. DSR only. If SDS, then skip to step 56.	3. Navigate to **Diameter > Configuration > Connections**.  4. Verify all the connections are shown.

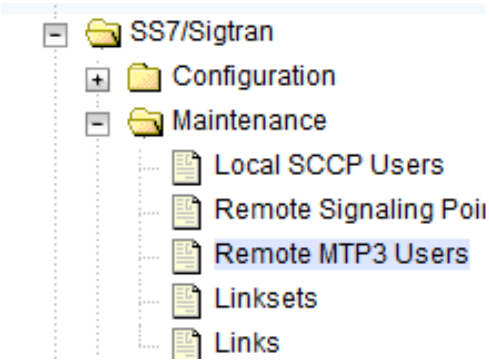
Procedure 4. Recovery Scenario 4

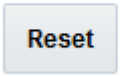
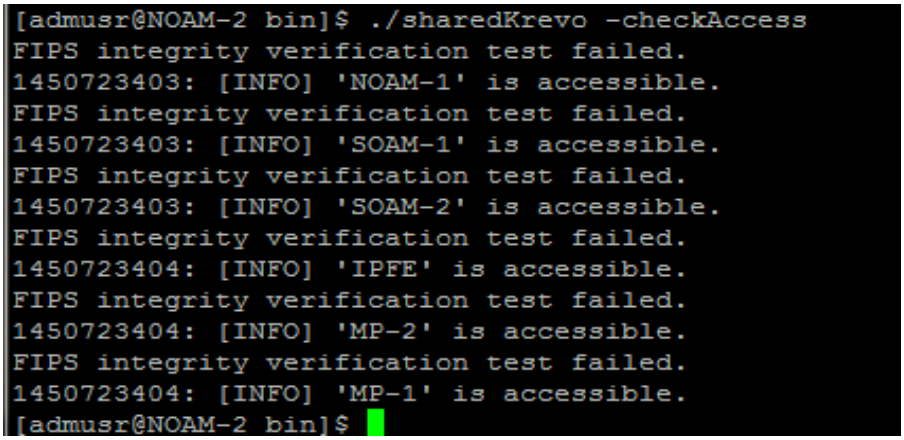
50. ☐	**SOAM VIP GUI**: Enable connections, if needed. DSR only. If SDS, then skip to step 56.	1. Navigate to **Diameter > Maintenance > Connections**.  2. Select each connection and click **Enable**. Alternatively, enable all the connections by clicking **EnableAll**.  3. Verify the Operational State 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
51. ☐	**SOAM VIP GUI**: Enable optional features. DSR only. If SDS, then skip to step 56.	1. Navigate to **Diameter > Maintenance > Applications**.  2. Select the optional feature application configured in step 72. 3. Click **Enable**. 
52. ☐	**SOAM VIP GUI**: Re-enable transports, if needed. DSR only. If SDS, then skip to step 56.	1. Navigate to **Transport Manager > Maintenance > Transport**.  2. Select each transport and click **Enable**.  3. Verify the Operational Status for each transport is **Up**.

Procedure 4. Recovery Scenario 4

53. ☐	**SOAM VIP GUI**: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 56.	1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.  2. Click the **Enable** button corresponding to MAPIWF Application Name. 3. Verify the SSN Status is **Enabled**.
54. ☐	**SOAM VIP GUI**: Re-enable links, if needed. DSR only. If SDS, then skip to step 56.	1. Navigate to **SS7/Sigtran > Maintenance > Links**.  2. Click **Enable** for each link.  3. Verify the Operational Status for each link is **Up**.

Procedure 4. Recovery Scenario 4

<table>
<tr>
<td>55. ☐</td>
<td>SOAM VIP GUI: Reset remote MTP3 users, if needed.
DSR only. If SDS, then skip to step 56.</td>
<td>1. Navigate to SS7/Sigtran > Maintenance > Remote MTP3 Users.
 

2. Click Reset for each record, if needed.
 
</td>
</tr>
<tr>
<td>56. ☐</td>
<td>NOAM VIP: Verify all servers in topology are accessible (RADIUS only)</td>
<td>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.
1. Establish an SSH session to the NOAM VIP and login as admusr.
2. Check if all the servers in the topology are accessible:
<pre>$ /usr/TKLC/dpi/bin/
$ ./sharedKrevo -checkAccess</pre>
Example output:
 

Note: If any server is not accessible, stop and contact My Oracle Support (MOS).</td>
</tr>
<tr>
<td>57. ☐</td>
<td>NOAM VIP: Copy key file to all the servers in topology (RADIUS only)</td>
<td>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.
1. Check if existing key file on active NOAM (the NOAM, which is intact and was not recovered) server is valid:</td>
</tr>
</table>

Procedure 4. Recovery Scenario 4

```
$ cd /usr/TKLC/dpi/bin/
$ ./sharedKrevo –validate
```

Example output:

```
[admusr@NOAM-2 bin]$ ./sharedKrevo -validate
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723458: [INFO] Key file for 'NOAM-1' is valid
1450723458: [INFO] Key file for 'NOAM-2' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723459: [INFO] Key file for 'SOAM-1' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723460: [INFO] Key file for 'SOAM-2' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723461: [INFO] Key file for 'IPFE' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723461: [INFO] Key file for 'MP-2' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723462: [INFO] Key file for 'MP-1' is valid
[admusr@NOAM-2 bin]$
```

If output of above command shows the existing key file is not valid, contact My Oracle Support (MOS).

2. Copy the key file to all the servers in the Topology:

```
$ ./sharedKrevo –synchronize
```

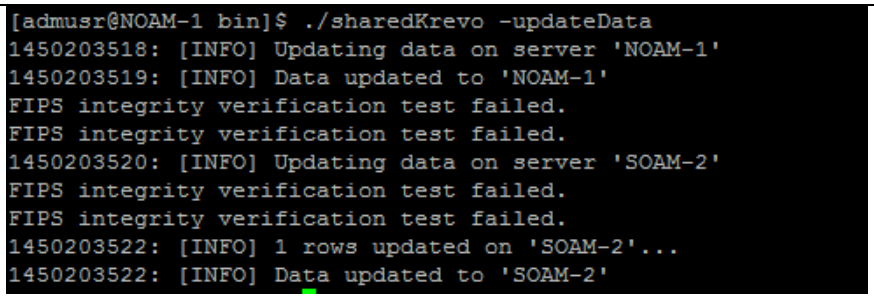
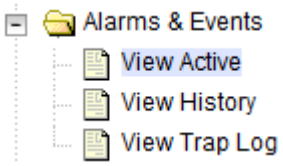
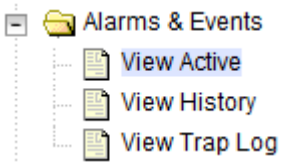
Example output:

```
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722733: [INFO] Synched key to IPFE
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722734: NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722735: [INFO] Synched key to MP-2
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722736: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722738: [INFO] Synched key to MP-1
[admusr@NOAM-2 bin]$
```

```
$ ./sharedKrevo –updateData
```

Example output:

Procedure 4. Recovery Scenario 4

		 ***Note:*** If any errors display, stop and contact My Oracle Support (MOS).
58. ☐	**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).
59. ☐	**NOAM 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. ☐	Restart oampAgent, if needed	***Note:*** If **10012: The responder for a monitored table failed to respond to a table change** alarm displays, the oampAgent needs to be restarted.
		1. Establish an SSH session to each server that has the alarm.
		2. Login admusr
		3. Execute the following commands:
		`$ sudo pm.set off oampAgent`
		`$ sudo pm.set on oampAgent`

61. ☐	Back up and archive all the databases from the recovered system	Execute the **DSR Database Backup** procedure to back up the configuration databases.
62. ☐	Recover IDIH	If IDIH was affected, refer to section 6 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
- Recover IDIH if necessary

Procedure 5. Recovery Scenario 5

S T E P #	This procedure performs recovery if both NOAM servers have failed but a DR NOAM is available. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Workarounds	Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist. Refer to Appendix K 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.
3. ☐	Switch DR NOAM to primary	Refer to [13] DSR/SDS NOAM Failover User's Guide.

Procedure 5. Recovery Scenario 5

4. ☐	Recover failed SOAMs	If ALL SOAM servers have failed, execute Procedure 2.
		If ALL NOAM servers have failed, execute:
		1. Procedure 4, steps 4. through 14.
		2. Perform keyexchange between the newly active NOAM and the recovered NOAM PMAC.
		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's PMAC server using the keyexchange utility, using the management IP address for the PMAC server.
		When asked for the password, enter the password for the **admusr** user of the PMAC server.
		`$ keyexchange admusr@<Recovered_Servers_PMAC_IP Address>`
		Note: If keyexchange fails, edit **/home/admusr/.ssh/known_hosts** and remove blank lines. Retry the keyexchange commands.
		3. Use the PMAC GUI to determine the control network IP address of the recovered VMs.
		4. Navigate to **Software Inventory**.
		5. Perform a keyexchange between the recovered PMAC and the recovered guests:
		From a terminal window connection on the recovered PMAC as the **admusr** user, exchange SSH keys for **admusr** between the PMAC and the recovered VM guests using the keyexchange utility, using the control network IP addresses for the VM guests.
		When asked for the password, enter the password for the **admusr** user of the VM guest.
		`$ keyexchange admusr@<Recovered_VM_control_IP Address>`
		Note: If keyexchange fails, edit **/home/admusr/.ssh/known_hosts** and remove blank lines. Retry the keyexchange commands.
		6. Procedure 4, steps 15. through 19. for each NOAM.

5. ☐	Perform keyexchange between active NOAM and recovered NOAMs	Perform a keyexchange between the newly active NOAM and the recovered NOAM servers: 8. 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. 9. When prompted for the password, enter the password for the **admusr** user of the recovered NOAM servers. `$ keyexchange admusr@<Recovered_NOAM Hostname>`

Procedure 5. Recovery Scenario 5

6. ☐	**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.
7. ☐	**Recovered NOAM Servers**: Activate optional features	Map-Diameter Interworking (MAP-IWF) and/or Policy and Charging Application (PCA) Only Activate the features Map-Diameter Interworking (MAP-IWF) and Policy and Charging Application (PCA) as follows: **For PCA:** Establish SSH sessions to the all the recovered NOAM servers and login as **admusr**. Refer [7] and execute **PCA Activation on Standby NOAM Server** on all recovered NOAM servers to re-activate PCA. **For MAP-IWF:** Establish SSH session to the recovered active NOAM, login as **admusr**. Refer to [5] to activate Map-Diameter Interworking (MAP-IWF). ***Note:*** While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored: `iload#31000{S/W Fault}` ***Note:*** If any of the MPs are failed and recovered, then restart these MP servers after activation of the feature.

8. ☐	**NOAM VIP**: Copy key file to all the servers in topology (RADIUS only)	If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.
		1. Check if existing key file on active NOAM (the NOAM, which is intact and was not recovered) server is valid:
		`$ cd /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo –validate`
		Note: If output of above command shows that existing key file is not valid, contact My Oracle Support (MOS).
		2. Copy the key file from active DR NOAM to recovered NOAMs.
		`$ ./sharedKrevo –copyKey –destServer <First NOAM server>`
		`$ ./sharedKrevo –copyKey –destServer <Second NOAM server>`

Procedure 5. Recovery Scenario 5

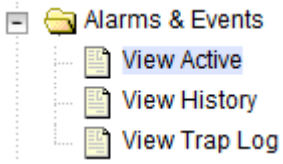
9. ☐	**Primary NOAM**: Modify DSR OAM process	1. Establish an SSH session to the primary NOAM, login as **admusr**.
		2. Retrieve the cluster ID of the recovered NOAM:
		`$ sudo iqt -fClusterID TopologyMapping where "NodeID='<DR_NOAM_Host_Name>'"`
		`Server_ID NodeID ClusterID`
		`1 Oahu-DSR-NOAM-2 A1055`
		3. Execute this command to start the DSR OAM process on the recovered NOAM:
		`$ echo "<clusterID>|DSROAM_Proc|Yes" | iload -ha -xun -fcluster –fresource -foptional HaClusterResourceCfg`

10. ☐	Switch DR NOAM back to secondary	Once the system has been recovered, refer to [13] DSR/SDS NOAM Failover User's Guide.

Procedure 5. Recovery Scenario 5

11. ☐	**NOAM VIP**: Verify all servers in topology are accessible (RADIUS only).
	DSR only. If SDS, then skip to the next step.
		If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.
		1. Establish an SSH session to the NOAM VIP and login as **admusr**.
		2. Check if all the servers in the topology are accessible:
		`$ /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo –checkAccess`
		Note: If any server is not accessible, stop and contact My Oracle Support (MOS).
		3. Copy the key file to all the servers in the topology:
		`$ ./sharedKrevo –synchronize`
		Example output:
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`1450722733: [INFO] Synched key to IPFE`
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`1450722734: NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2.`
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`1450722735: [INFO] Synched key to MP-2`
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`1450722736: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1.`
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`1450722738: [INFO] Synched key to MP-1`
		`[admusr@NOAM-2 bin]$`
		`$ ./sharedKrevo –updateData`
		Example output:
		`[admusr@NOAM-1 bin]$ ./sharedKrevo -updateData`
		`1450203518: [INFO] Updating data on server 'NOAM-1'`
		`1450203519: [INFO] Data updated to 'NOAM-1'`
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`1450203520: [INFO] Updating data on server 'SOAM-2'`
		`FIPS integrity verification test failed.`
		`FIPS integrity verification test failed.`
		`1450203522: [INFO] 1 rows updated on 'SOAM-2'...`
		`1450203522: [INFO] Data updated to 'SOAM-2'`
		Note: If any errors display, stop and contact My Oracle Support (MOS).

Procedure 5. Recovery Scenario 5

12. ☐	**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.)
13. ☐	Recover IDIH	If IDIH was affected, refer to section 6 IDIH Disaster Recovery 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

Notes:

- During recovery, the corrupted database is replaced by the server runtime backup. Any configuration done after taking the backup is not available post recovery.
- Corrupt databases on the SOAM will replicate to all SOAMs in its Network Element (Active, Standby, and Spare). It may be necessary to perform this recovery procedure on ALL SOAMs.

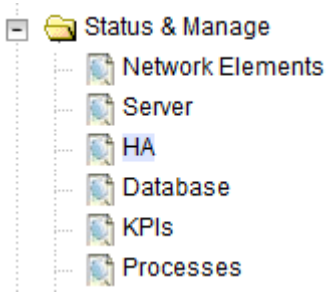
Procedure 6. Recovery Scenario 6 (Case 1)

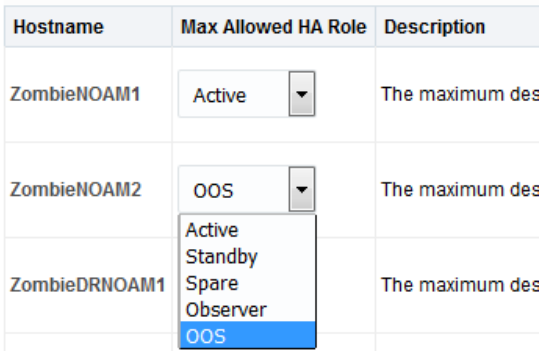
S T E P #	This procedure performs recovery if at least one NOAM server is available, but all SOAM servers in a site have failed. This includes any SOAM server that is in another location. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Workarounds	Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.

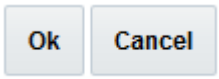
Procedure 6. Recovery Scenario 6 (Case 1)

2. ☐	**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: 

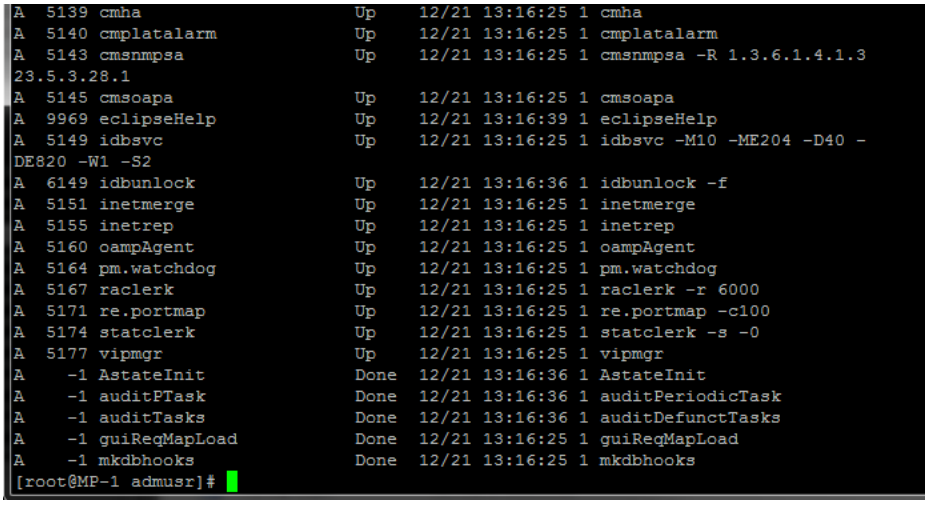
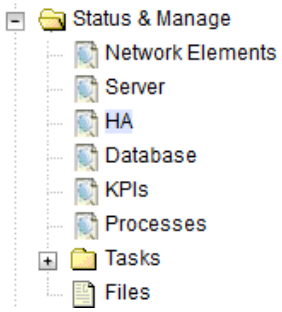
Procedure 6. Recovery Scenario 6 (Case 1)

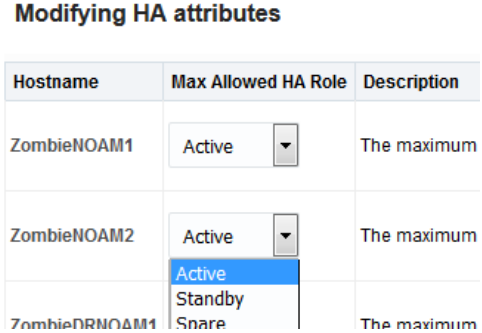
<table>
<tr><td>3. ☐</td><td>NOAM VIP GUI: Set failed servers to OOS</td><td>1. Navigate to Status & Manage > HA.
 

2. Select Edit.
Modifying HA attributes
 

3. Set the Max Allowed HA Role option to OOS for the failed servers.
4. Click OK.
 
</td></tr>
<tr><td>4. ☐</td><td>Server in Question: Login</td><td>Establish an SSH session to the server in question. Login as admusr.</td></tr>
<tr><td>5. ☐</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>6. ☐</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>7. ☐</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>

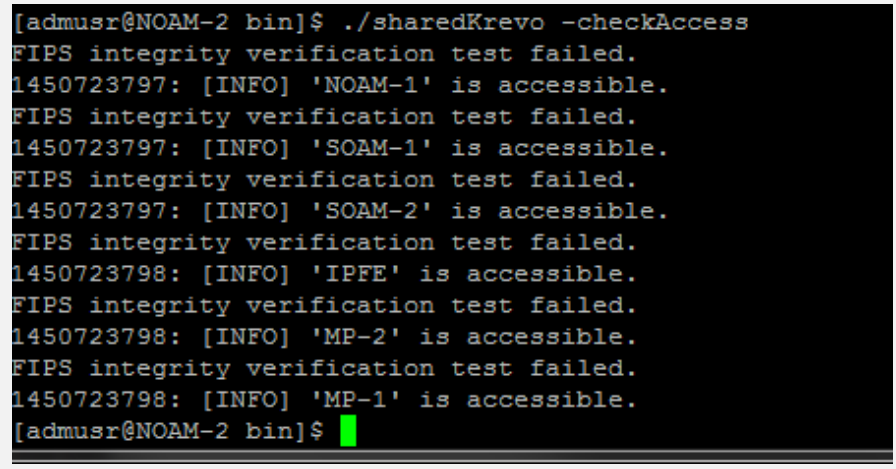
Procedure 6. Recovery Scenario 6 (Case 1)

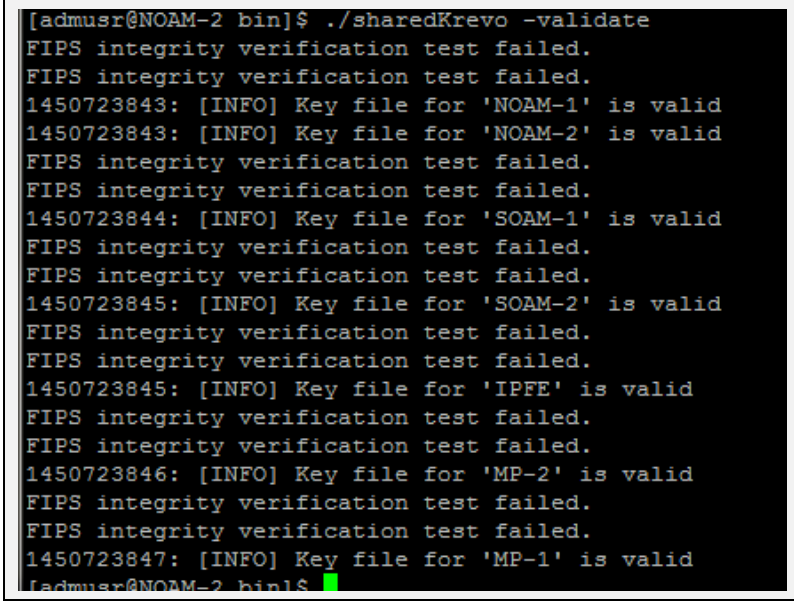
<table>
<tr>
<td>8. ☐</td>
<td>Server in Question: Verify the server</td>
<td>Verify if the processes are up and running.
<code>$ sudo pm.getprocs</code>
Example output:
 
</td>
</tr>
<tr>
<td>9. ☐</td>
<td>NOAM VIP GUI: Set failed servers to active</td>
<td>1. Navigate to Status & Manage > HA.
 

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

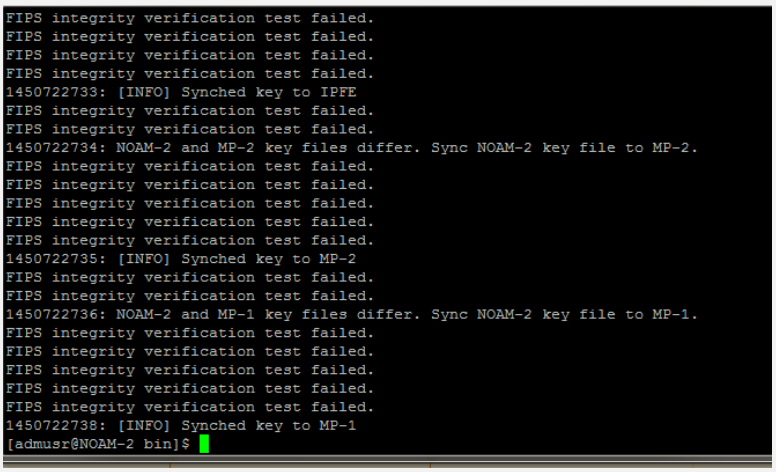
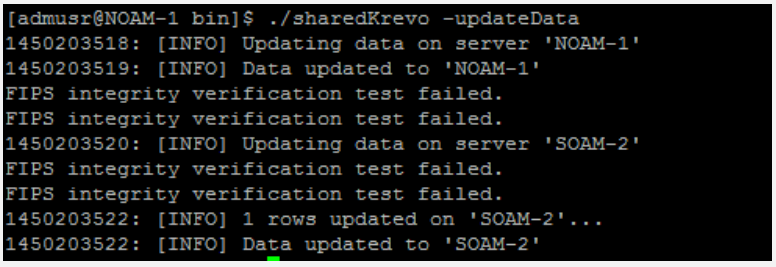
4. Click OK.</td>
</tr>
</table>

Procedure 6. Recovery Scenario 6 (Case 1)

10. ☐	**NOAM VIP**: Verify all servers in topology are accessible (RADIUS only)	If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.
		1. Establish an SSH session to the NOAM VIP and login as **admusr**.
		2. Check if all the servers in the Topology are accessible:
		`$ cd /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo -checkAccess`
		 

11. ☐	**NOAM VIP**: Copy key file to all the servers in topology (RADIUS only)	If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator. 1. Check if existing key file on active NOAM (The NOAM which is intact and was not recovered) server is valid: `$ ./sharedKrevo -validate`  If output of above command shows the existing key file is not valid, contact My Oracle Support (MOS).

Procedure 6. Recovery Scenario 6 (Case 1)

		2. Copy the key file to all the servers in the Topology:
		`$ ./sharedKrevo –synchronize`
		 
		`$ ./sharedKrevo –updateData`
		 
		Note: If any errors are present, stop and contact My Oracle Support (MOS).

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

4.6.2 Recovery Scenario 6: Case 2

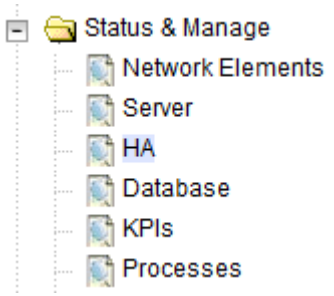
For a partial outage with:

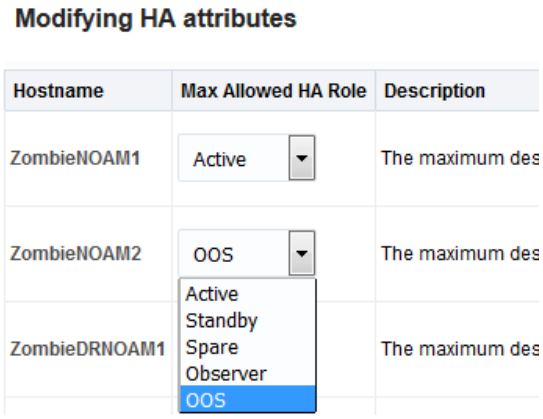
- Server having a corrupted database
- Replication channel is not inhibited; or
- Server has the same release as that of its active parent

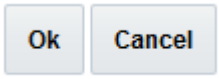
Procedure 7. Recovery Scenario 6 (Case 2)

S T E P #	This procedure performs recovery if at least one 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 Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.
2. ☐	**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)

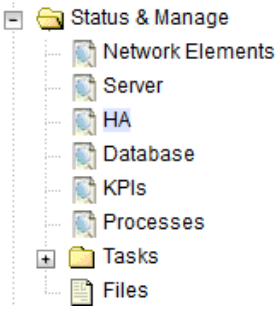
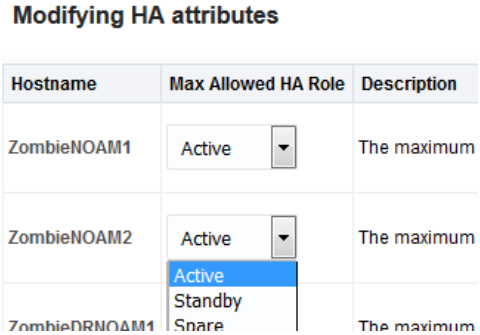
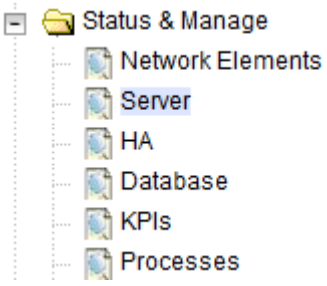
<table>
<tr>
<td>3. ☐</td>
<td>NOAM VIP GUI: Set failed servers to OOS</td>
<td>1. Navigate to Status & Manage > HA.
 

2. Click Edit.
 

3. Set the Max Allowed HA Role option to OOS for the failed servers.
4. Click OK.
 
</td>
</tr>
<tr>
<td>4. ☐</td>
<td>Server in Question: Login</td>
<td>Establish an SSH session to the server in question. Login as admusr.</td>
</tr>
<tr>
<td>5. ☐</td>
<td>Server in Question: Stop httpd service</td>
<td>Stop the httpd service.
<code>$ sudo bash -l</code>
Stop the HTTPD service before the database is down and start the HTTPD service after the database has started.
<code>$ service httpd stop</code></td>
</tr>
<tr>
<td>6. ☐</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>7. ☐</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)

8. ☐	**Server in Question**: Start httpd service	1. Start the httpd service.
		`$ service httpd start`
		2. Exit out of root.
		`$ exit`

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

Procedure 7. Recovery Scenario 6 (Case 2)

11. ☐	**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`

12. ☐	**NOAM VIP**: Verify all servers in topology are accessible (RADIUS Only).
	DSR only. If SDS, skip to step 14.
		If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.
		1. Establish an SSH session to the NOAM VIP and login as **admusr**.
		2. Check if all the servers in the Topology are accessible:
		`$ cd /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo -checkAccess`

Procedure 7. Recovery Scenario 6 (Case 2)

<table>
<tr>
<td>13. ☐</td>
<td>NOAM VIP: Copy key file to all the servers in topology (RADIUS Only)</td>
<td>
If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.
1. Check if existing key file on active NOAM (the NOAM which is intact and was not recovered) server is valid:
<pre>$ cd /usr/TKLC/dpi/bin/
$ ./sharedKrevo –validate</pre>
If output shows the existing key file is not valid, contact My Oracle Support (MOS).
2. Copy the key file to all the servers in the topology:
<pre>$ ./sharedKrevo –synchronize</pre>
<pre>FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722733: [INFO] Synched key to IPFE
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722734: NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722735: [INFO] Synched key to MP-2
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722736: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722738: [INFO] Synched key to MP-1
[admusr@NOAM-2 bin]$</pre>
<pre>$ ./sharedKrevo –updateData</pre>
<pre>[admusr@NOAM-1 bin]$ ./sharedKrevo -updateData
1450203518: [INFO] Updating data on server 'NOAM-1'
1450203519: [INFO] Data updated to 'NOAM-1'
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450203520: [INFO] Updating data on server 'SOAM-2'
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450203522: [INFO] 1 rows updated on 'SOAM-2'...
1450203522: [INFO] Data updated to 'SOAM-2'</pre>
Note: If any errors are present, stop and contact My Oracle Support (MOS).
</td>
</tr>
<tr>
<td>14. ☐</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>

5. Resolve User Credential Issues after Database Restore

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

5.1 Restore a Deleted User

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

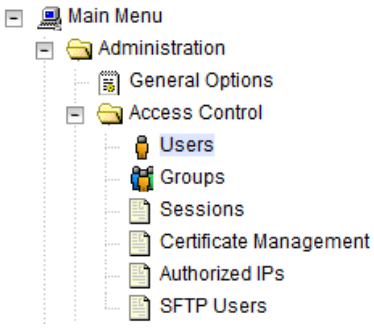
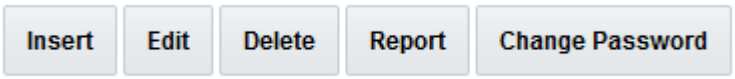
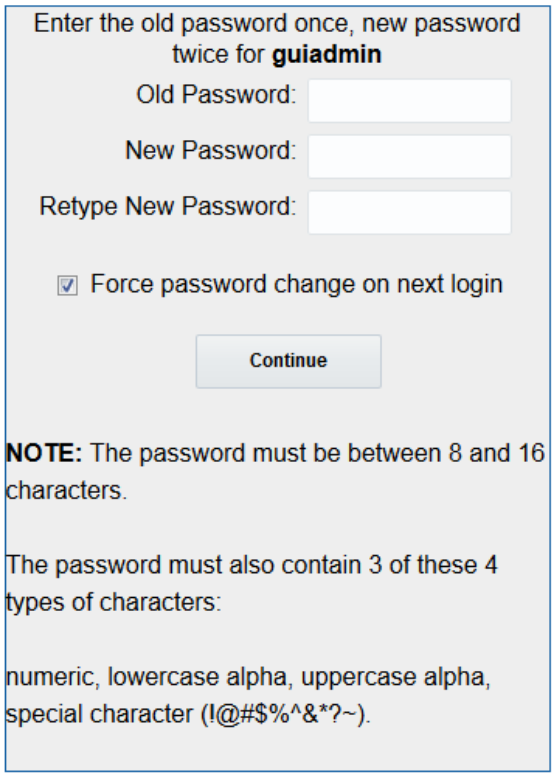
These users were removed before creation of the backup and archive file. They are reintroduced by system restoration of that file.

5.2 Keep a Restored User

Procedure 8. Keep Restored User

S T E P #		
	Perform this procedure to keep users restored by system restoration. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Before Restoration**: Notify affected users before restoration	Contact each user affected before the restoration and notify them that you will reset their password during this maintenance operation.
2. ☐	**After Restoration**: Log into the NOAM VIP	1. Establish a GUI session on the NOAM server by using the VIP 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

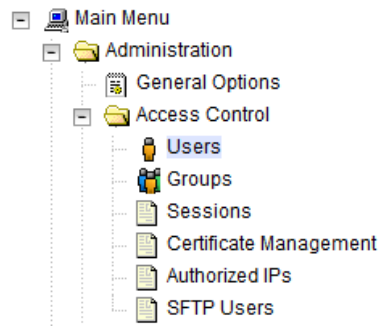
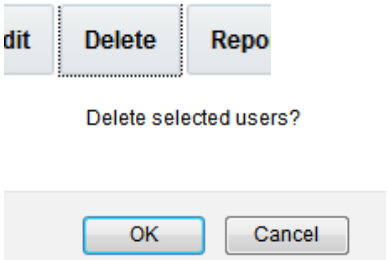
3. ☐	**After Restoration**: Reset user passwords	1. Navigate to **Administration > Access Control > Users**.  2. Select the user. 3. Click **Change Password**.  4. Type a new password.  5. Click **Continue**.

5.3 Remove a Restored User

Procedure 9. Remove the Restored User

S T E P #	Perform this procedure to remove users restored by system restoration Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**After Restoration**: Log into the NOAM VIP	1. Establish a GUI session on the NOAM server by using the VIP 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:

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

5.5 Restore an Archive that Does Not Contain a Current User

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

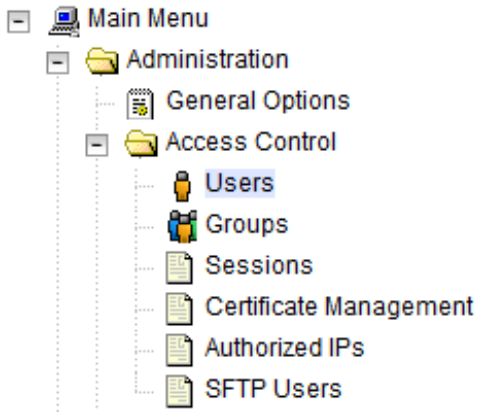
```
- User 'testuser' exists in current database but not in the selected backup
file.
```

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

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

S T E P #		
	Perform this procedure to remove users restored by system restoration. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Before Restoration**: Notify affected users before restoration	Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.
2. ☐	**Before Restoration**: Log into the NOAM VIP	1. Establish a GUI session on the NOAM server by using the VIP 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: 

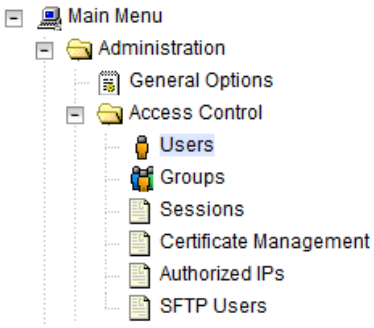
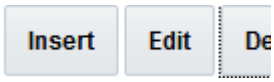
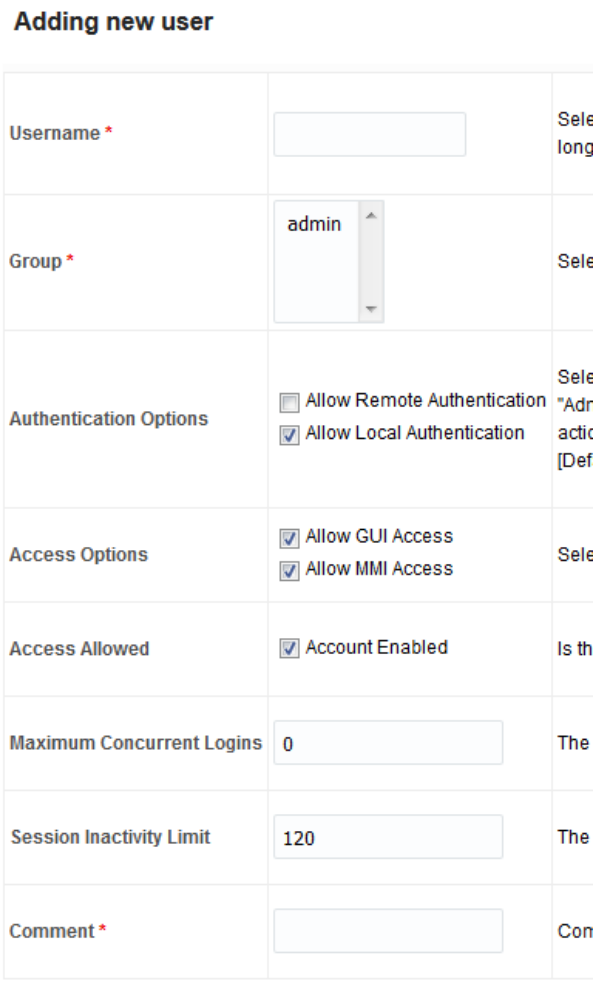
Procedure 10. Restore an Archive That Does Not Contain a Current User

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**.

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

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

6. IDIH Disaster Recovery

The fdconfig xml file you use for disaster recovery is different from the one used for fresh installation. The one for disaster recovery has the **hostname-upgrade_xx-xx-xx.xml** file format. It took out the Oracle server installation part since it is not needed for disaster recovery. If the disaster recovery procedure is being executed on the rack mount server containing the Oracle database, use the fdconfig installation xml file.

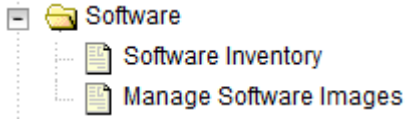
Note: The fdconfig xml file for disaster recovery is exactly the same as the one for upgrade and this file should have been created during the latest upgrade or fresh installation. In case the file is not found, make a copy of the fdconfig.xml file for fresh installation with **-upgrade** between the hostname and the version number. Edit the newly created **hostname-upgrade_xx-xx-xx.xml** file and take out the following section within the dotted line:

```
 </infrastructure>
  </infrastructures>
<servers>
.....................................................................
    <tvoeguest id="ORA">
        <infrastructure>localPMAC</infrastructure>
            </postdeploy>
        </scripts>
    </tvoeguest
.....................................................................
    <tvoeguest id="MED">
        <infrastructure>localPMAC</infrastructure>
             <!--Specify which Rack Mount Server TVOE Host the Mediation
server will be placed -->
        <tvoehost>mgmtsrvrtvoe2</tvoehost>
        <name>MED</name>
```

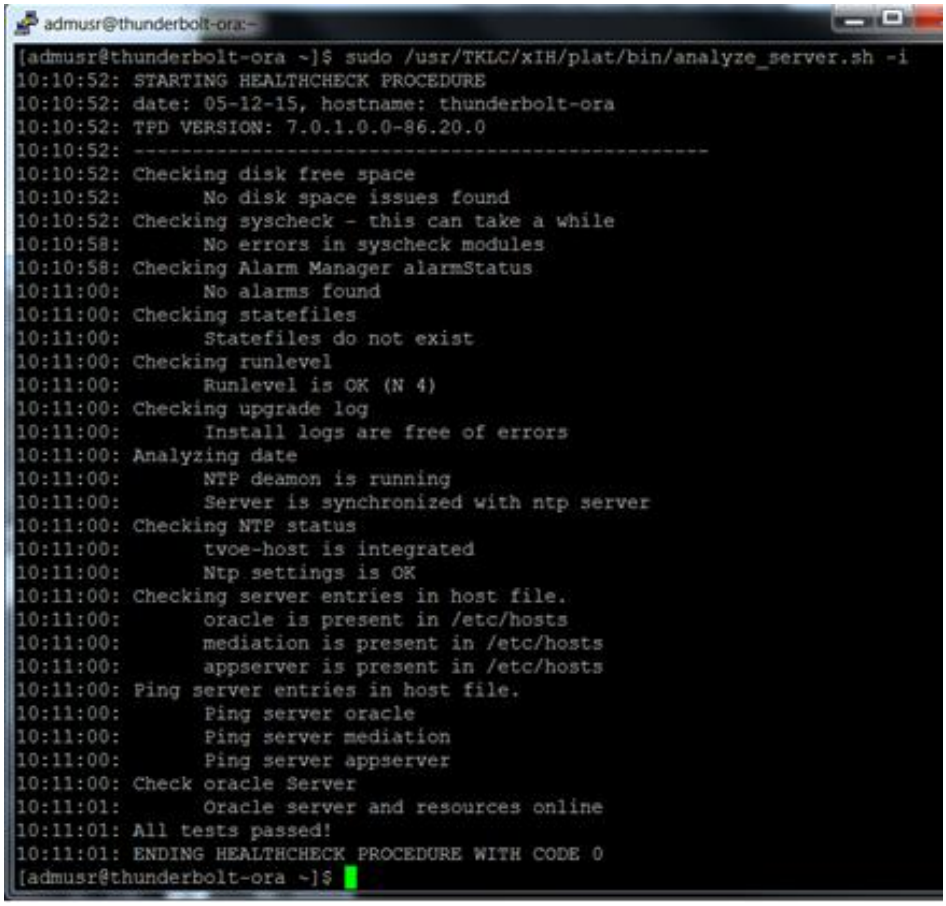
Disaster Recovery Scenarios

Disaster Recovery Scenario	fdconfig file to use
Server containing Oracle database server	Install fdconfig xml
Server containing Application Server	Upgrade/Disaster Recovery xml
Server containing Mediation Server	Upgrade/Disaster Recovery xml

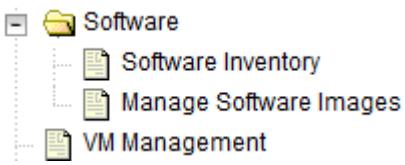
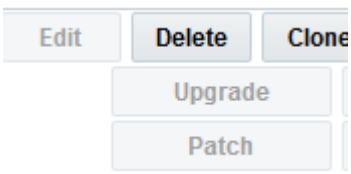
Procedure 11. IDIH Disaster Recovery Preparation

S T E P #		
	This procedure performs disaster recovery preparation steps for the IDIH. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, 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. ☐	**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. 3. Verify these values match the name in the <software> </software> section in the **hostname-upgrade_xx-xx-xx.xml** file. ***Note:*** If the necessary software images are not available, follow the instructions from the **Load Application and TPD ISO onto PMAC Server** procedure and steps 1-4 of **IDIH Configuration** from [8] to acquire and transfer the images.

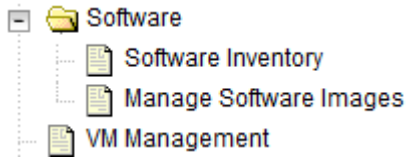
Procedure 11. IDIH Disaster Recovery Preparation

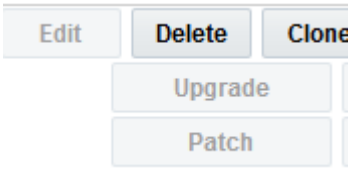
3. ☐	**Oracle Guest**: Login	Establish an SSH session to the Oracle guest, login as **admusr**.
4. ☐	**Oracle Guest**: Perform database health check	Perform a database health check: `$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i` Example output: 

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

S T E P #		
	This procedure performs disaster recovery for the IDIH by re-installing the mediation and application servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, 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)

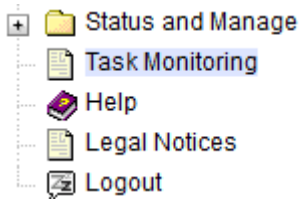
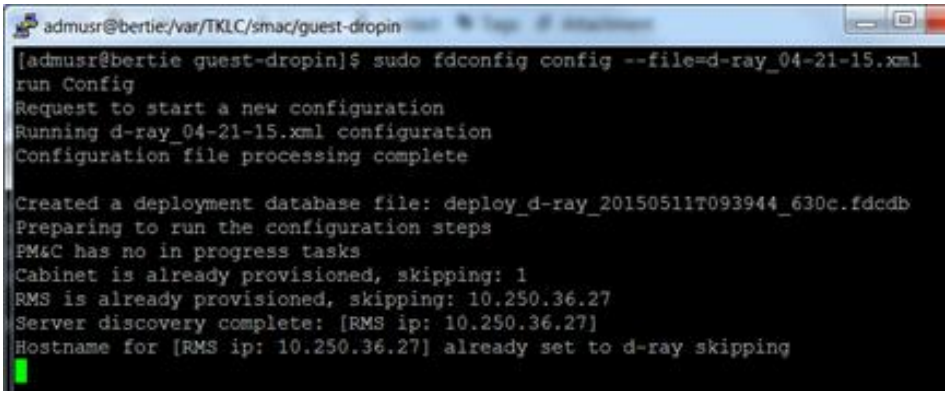
<table>
<tr>
<td>3. ☐</td>
<td>Remove existing mediation server</td>
<td>1. Navigate to Main Menu > VM Management.
 

2. Select the Mediation guest.
3. Click Delete.
 
</td>
</tr>
<tr>
<td>4. ☐</td>
<td>PMAC: Establish SSH session and login</td>
<td>Establish an SSH session to the PMAC, login as admusr.</td>
</tr>
<tr>
<td>5. ☐</td>
<td>PMAC: Re-install the mediation and application servers</td>
<td>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: ***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.</td>
</tr>
</table>

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

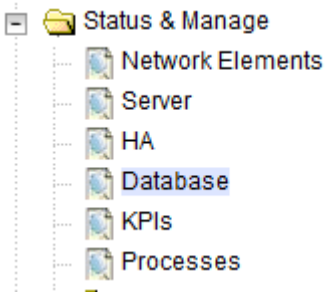
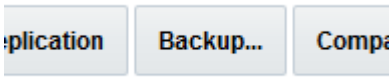
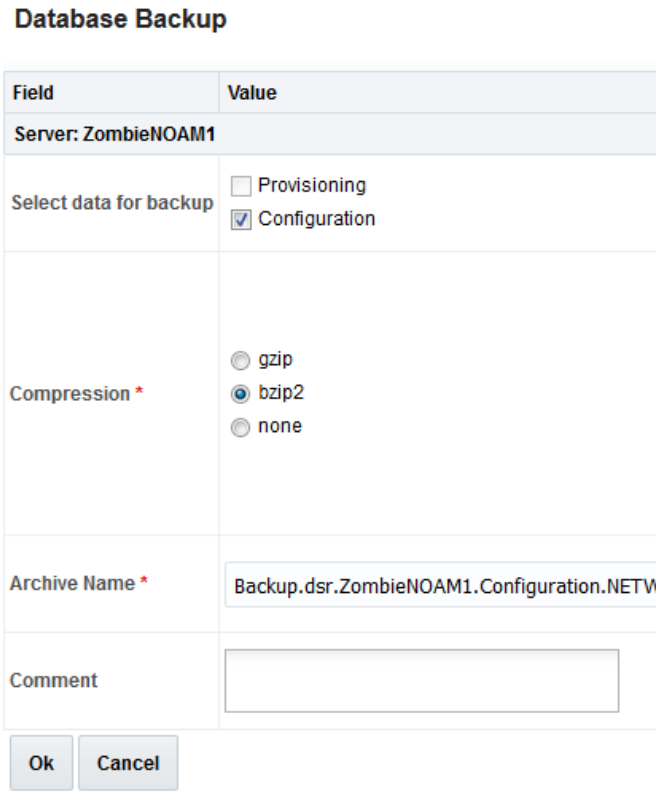
6. ☐	**PMAC GUI**: Monitor the configuration	1. If not already done, establish a GUI session on the PMAC server. 2. Navigate to **Task Monitoring**.  3. Monitor the IDIH configuration to completion. Alternatively, you can monitor the fdconfig status through the command line after executing the fdconfig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

Appendix A. DSR Database Backup

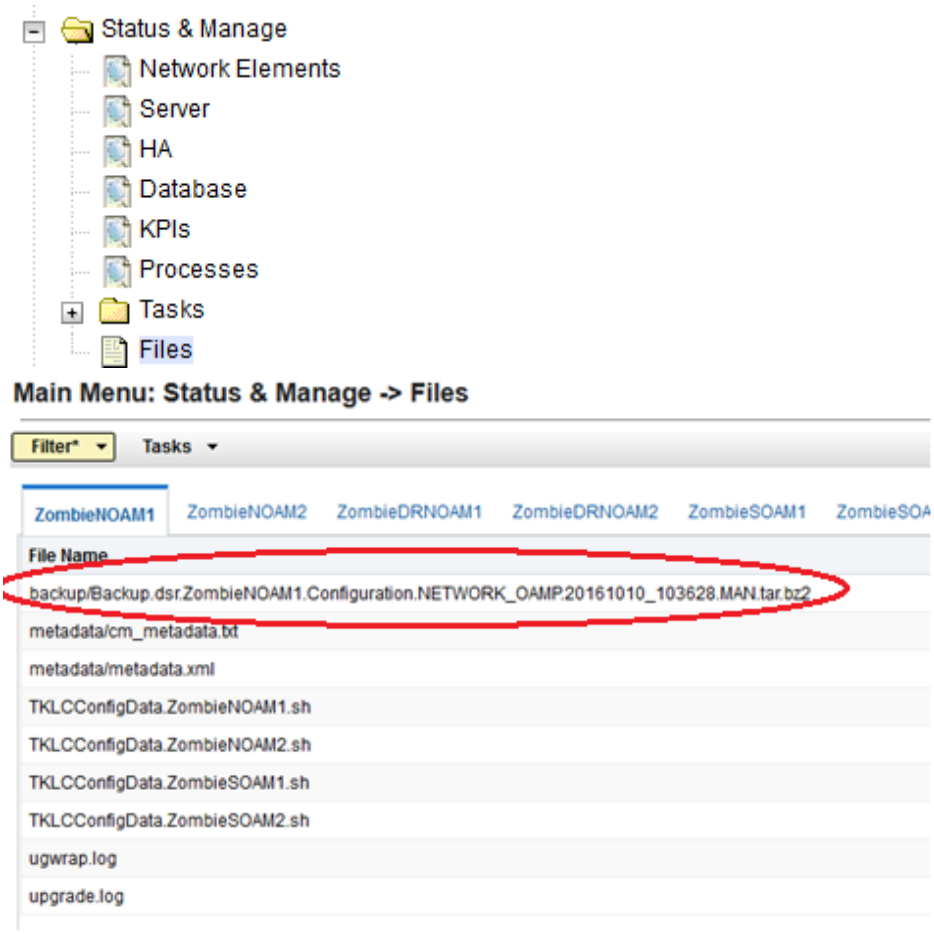
Procedure 13. DSR Database Backup

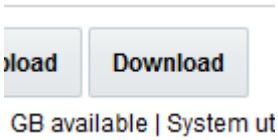
S T E P #		
	This procedure backs up the provision and configuration information from an NOAM or SOAM server after the disaster recovery is complete. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended 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 & 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

<table>
<tr><td>3.
☐</td><td>NOAM/SOAM VIP: Verify the backup file existence</td><td>1. Navigate to Status & Manage > Files.
 

2. Select the active NOAM or SOAM tab.
3. The files on this server display. Verify the existence of the backup file.</td></tr>
<tr><td>4.
☐</td><td>NOAM/SOAM VIP: Download the file to a local machine</td><td>1. From the previous step, select the backup file.
2. Click Download.
 

3. Click OK to confirm the download.</td></tr>
<tr><td>5.
☐</td><td>Upload the image to secure location</td><td>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.</td></tr>
<tr><td>6.
☐</td><td>Backup active SOAM</td><td>Repeat steps 2 through 5 to back up the active SOAM.</td></tr>
</table>

Procedure 13. DSR Database Backup

7. ☐	Take Secured backup of key file (RADIUS only)	If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.
		1. Log into ssh shell of active NOAM server using user **admusr**.
		2. Take secure backup of updated key file **RADIUS shared secret encryption key** for disaster scenarios.
		3. Encrypt the key file before backing up to secure customer setup:
		`$ ./sharedKrevo -encr`
		4. Copy the encrypted key file to secure customer setup:
		`$ sudo scp /var/TKLC/db/filemgmt/DpiKf.bin.encr user@<customer IP>:<path of customer setup>`
		Note: The operator must strictly control access to the backed up key file. If the operator needs to encrypt this key file further using operator specified encryption techniques, the operator is recommended to do so; however, the operator is responsible to decrypt this file using operator-specific decryption techniques and copy the resulting **DpiKf.bin.encr** file securely to the file management folder if the key file needs to be restored for disaster recovery. Once the key file is backed up to the operator-provided server and path, it is the responsibility of the operator to ensure access to the backed up key file is extremely selective and restricted.

Appendix B. Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only)

Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F) (HP DL380 Gen 9 Only)

S T E P #		
	This procedure recovers a failed aggregation (4948E/4948E-F) switch. ***Prerequisites***: • A copy of the networking xml configuration files • A copy of HP miscellaneous firmware DVD or ISO • IP address and hostname of the failed switch • Rack mount position of the failed switch 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	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 <4948_switch_IP>`
		3. Refer to the Replace a failed 4948/4948E/4948E-F switch (c-Class System) (netConfig) procedure in reference [2] to replace a failed aggregation switch.
		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 the switch appropriate init file and use it for respective switch:
		Older platform init files may not work on platform 7.2 systems. Copy the switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy **switch1A_4948_4948E_init.xml**.
		4. The templates can be found using the following method:
		From the PMAC CLI:
		`df | grep –I DSR`
		Sample output:
		`/var/TKLC/smac/image/repository/DSR- 8.4.0.0.0_84.9.0-x86_64.iso`
		`1118514 1118514 0 100% /usr/TKLC/smac/html/TPD/DSR-8.4.0.0.0_84.9.0-x86_64`
		`/var/TKLC/smac/image/repository/DSR- 8.4.0.0.0_84.9.0-x86_64.iso`
		`1118372 1118372 0 100% /usr/TKLC/smac/html/TPD/DSR-8.4.0.0.0_84.9.0-x86_64`
		`/var/TKLC/smac/image/repository/DSR- 8.4.0.0.0_84.9.0-x86_64.iso`

Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F) (HP DL380 Gen 9 Only)

```
1117976 1117976   0 100% /usr/TKLC/smac/html/TPD/DSR-
8.4.0.0.0_84.9.0-x86_64
```

5. Determine the applicable directory of the DSR release being recovered.

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

Example:

```
cd /usr/TKLC/smac/html/TPD/DSR- 8.4.0.0.0_84.9.0-x86_64
/upgrade/overlay/
```

6. 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
```

7. Unzip the DSR_NetConfig_Templates.zip file and retrieve the required switch init file.

Example:

```
$ unzip DSR_NetConfig_Templates.zip
```

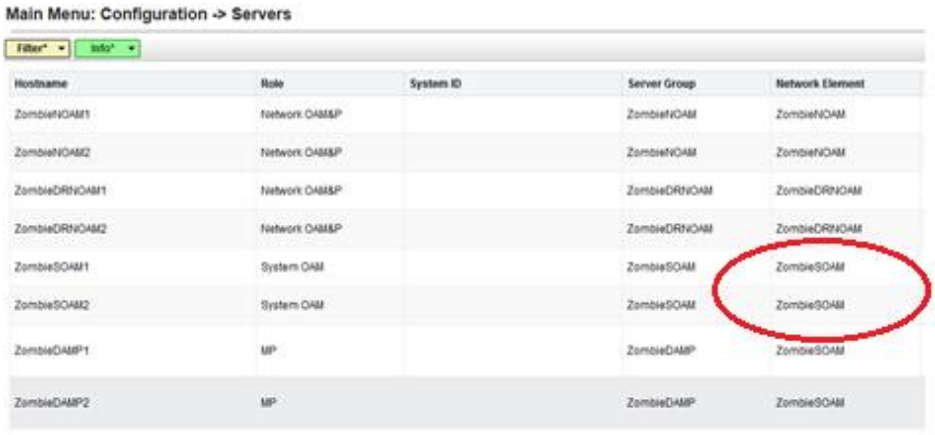
8. Edit the desired file with site specific details. The existing file from original deployment /usr/TKLC/smac/etc/switch/xml can be used as a reference.
9. Copy the new init file to the /usr/TKLC/smac/etc/switch/xml dir.

Example:

```
$ cp <switch_xml_file> /usr/TKLC/smac/etc/switch/xml/
```

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

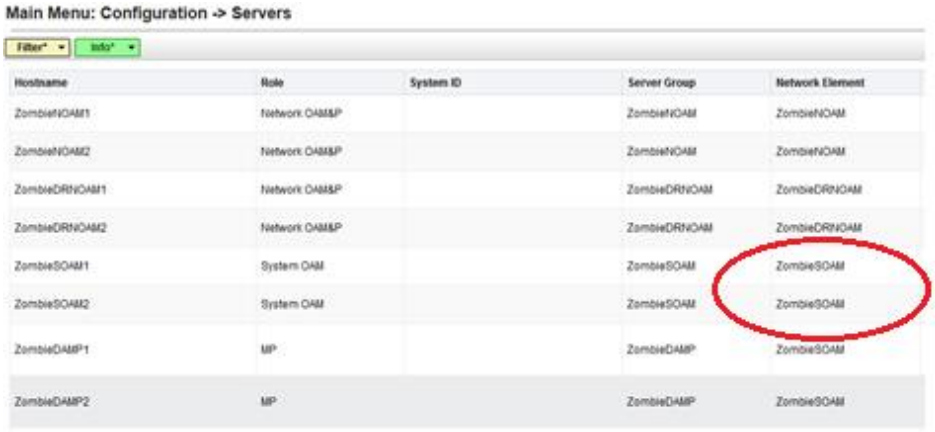
Procedure 15. Inhibit A and B Level Replication on C-level Servers

S T E P #		
	This procedure inhibits A and B level replication on all C-level servers of this site. 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**. The following figure shows 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 inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.
		Verify replication inhibition on MPs 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**.
		`$ iqt NodeInfo`
		Example output:
		`nodeId nodeName hostName nodeCapability inhibitRepPlans siteId excludeTables`
		`A1386.099 NO1 NO1 Active NO_HPC03`
		`B1754.109 SO1 SO1 Active SO_HPC03`
		`C2254.131 MP2 MP2 Active A B SO_HPC03`
		`C2254.233 MP1 MP1 Active A B SO_HPC03`

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

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

S T E P #		
	This procedure un-inhibits A and B level replication on all C-level servers of this site. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Active NOAM**: Login	Log into the active NOAM server using SSH as **admusr**.
2. ☐	**Active NOAM**: Un-Inhibit replication on all C-level servers	Execute this command: `$ for i in $(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<SOAM_Site_NE_name>'"); do iset -finhibitRepPlans='' NodeInfo where "nodeName='$i'"; done` ***Note:*** SOAM Site NE name of the site can be found out by logging into the active NOAM GUI and navigating to **Configuration > Server Groups**. Please see the snapshot below for more details, for example, if ServerSO1 belongs to the site being recovered, then siteID is SO_HPC03. 

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.
		Verify replication inhibition on MPs 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**.
		`$ sudo iqt NodeInfo`
		Example output:
		`nodeId nodeName hostName nodeCapability inhibitRepPlans siteId excludeTables`
		`A1386.099 NO1 NO1 Active NO_HPC03`
		`B1754.109 SO1 SO1 Active SO_HPC03`
		`C2254.131 MP2 MP2 Active A B SO_HPC03`
		`C2254.233 MP1 MP1 Active A B SO_HPC03`

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

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

S T E P #		
	This procedure inhibits A and B level replication on all C-level servers of this site when active, standby, and spare SOAMs are lost. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Active NOAM**: Login	Log into the active NOAM server using SSH as **admusr**.

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

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

<table>
<tr>
<td>3. ☐</td>
<td>Active NOAM:
Verify replication has been inhibited</td>
<td>
After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.
Verify replication inhibition on MPs 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:
<pre>$ iqt NodeInfo</pre>
Example output:
<pre>   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</pre>
</td>
</tr>
</table>

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

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

S T E P #		
	This procedure un-inhibits A and B level replication on all C-level servers of this site when active, standby and spare SOAMs are lost. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Active NOAM**: Login	Log into the active NOAM server using SSH as **admusr**.

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

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

3. ☐	**Active NOAM**: Verify replication has been Inhibited	After executing above steps to un-inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.
		Verify replication inhibition on MPs by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO_SG is set as **A B**.
		Execute this command:
		`$ sudo iqt NodeInfo`
		Example 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 G. Restore TVOE Configuration from Backup Media

Procedure 19. Restore TVOE Configuration from Backup Media

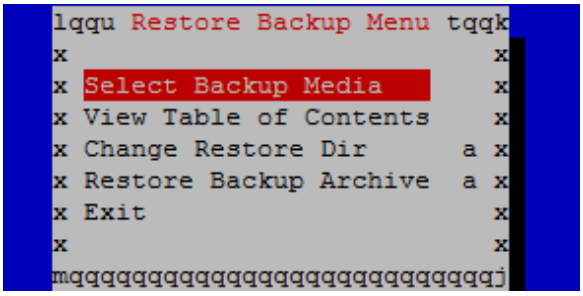
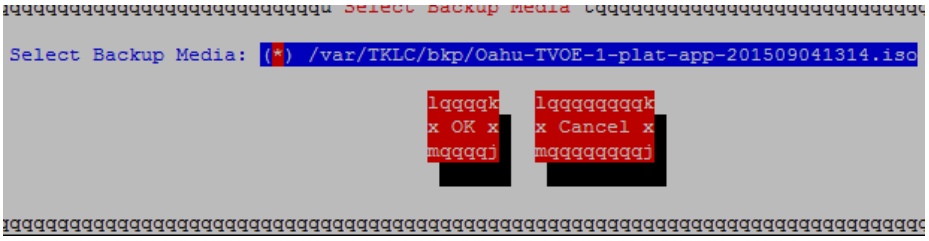
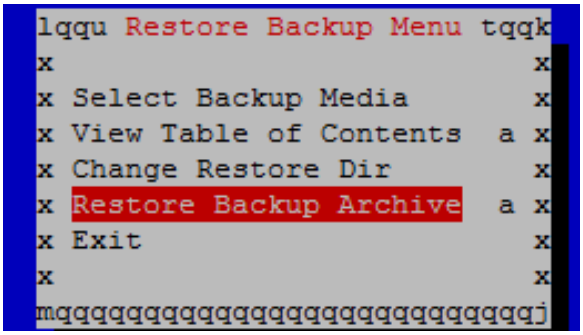
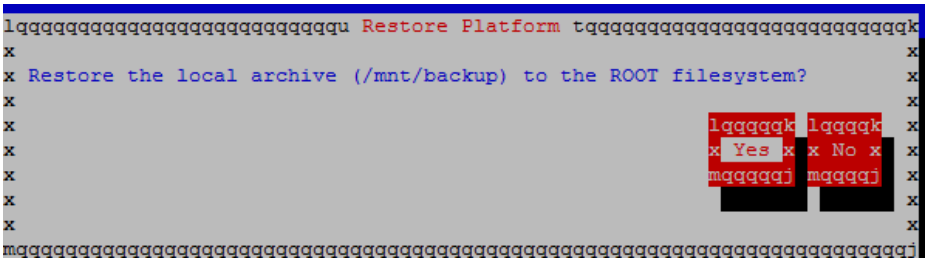
S T E P #	This procedure provides steps to restore the TVOE application configuration from backup media. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask 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 [8]. • If the PMAC is hosted on the failed rack mount server, execute **Installing TVOE on the Management Server** from reference [8].
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 [8]. ***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 19. Restore TVOE Configuration from Backup Media

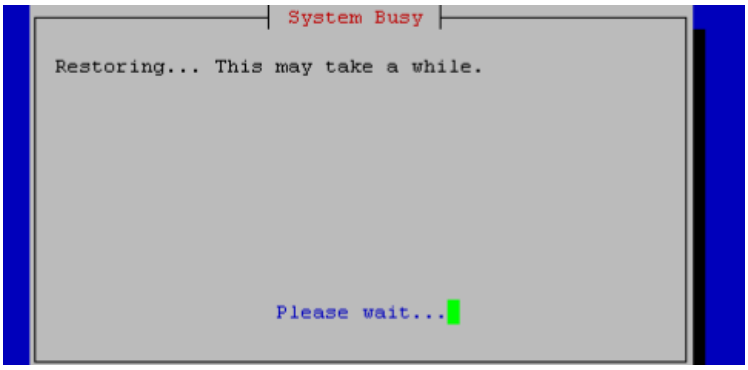
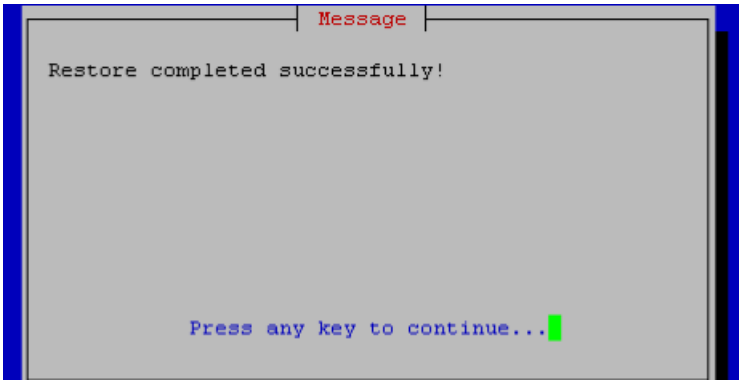
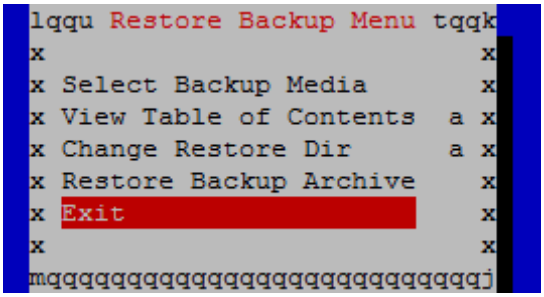
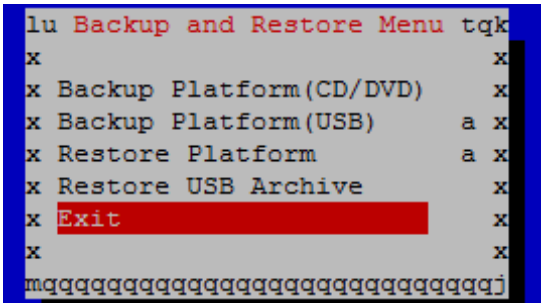
4. ☐	Transfer TVOE backup ISO image to the TVOE host	Restore TVOE backup ISO using SCP.
		Using the IP of the TVOE host, transfer the backup ISO image to the TVOE.
		Linux:
		From the command line of a Linux machine use this command to copy the backup ISO image to the TVOE host:
		`# scp <path_to_image> 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.
		Notes:
		• If the IP is an IPv4 address, then `<TVOE_IP>` is a normal dot-decimal notation (for example, 10.240.6.170).
		• 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.
		• 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. Refer to [8], theUsing WinSCP procedure, to copy the backup image to the customer system.

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

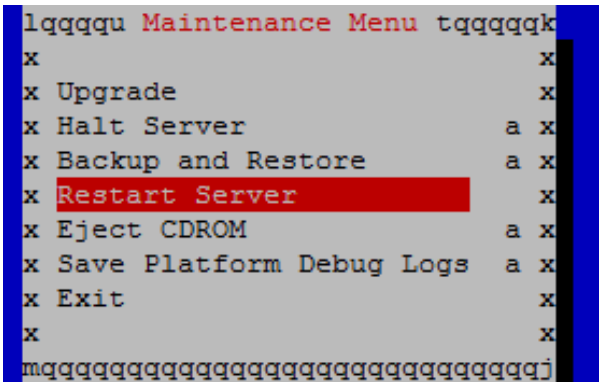
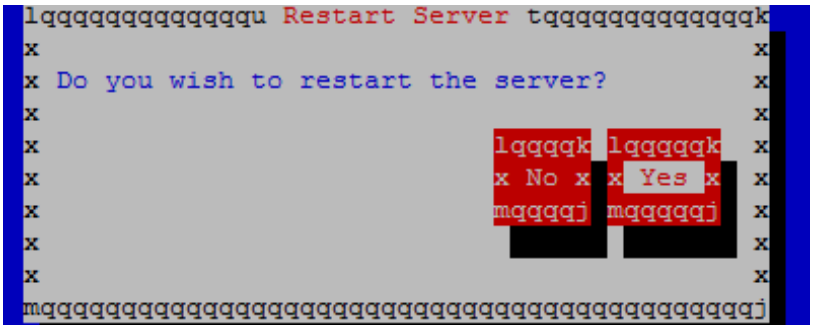
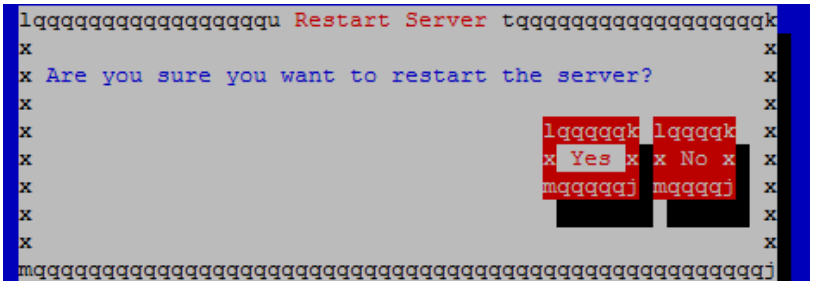
Procedure 19. Restore TVOE Configuration from Backup Media

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. 

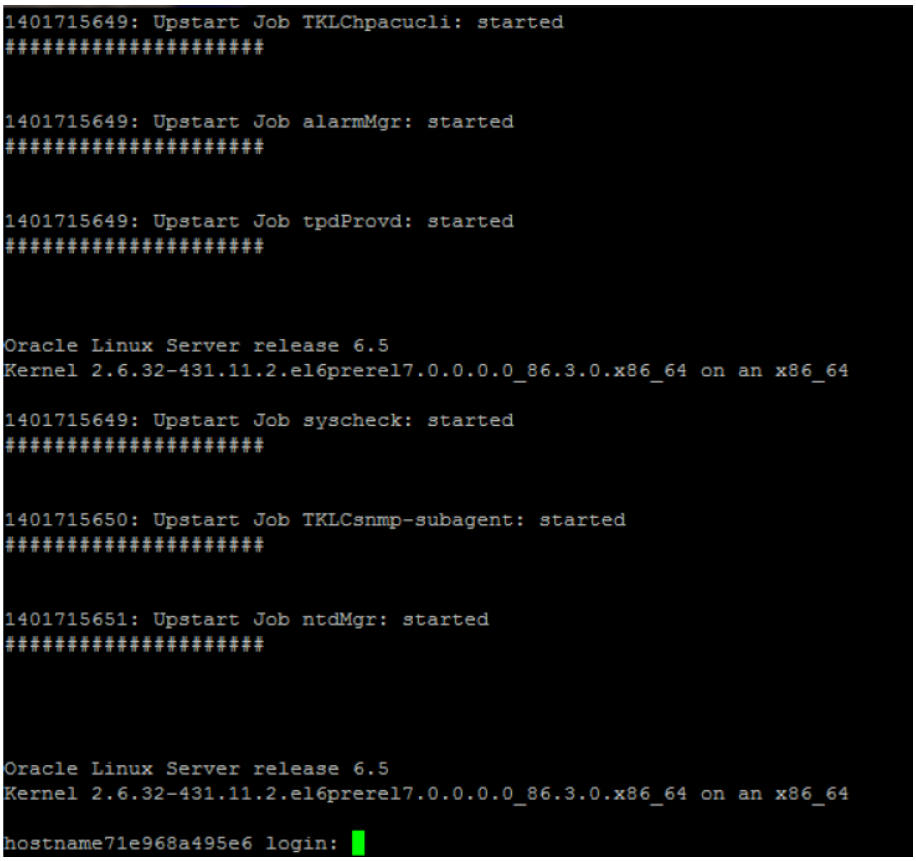
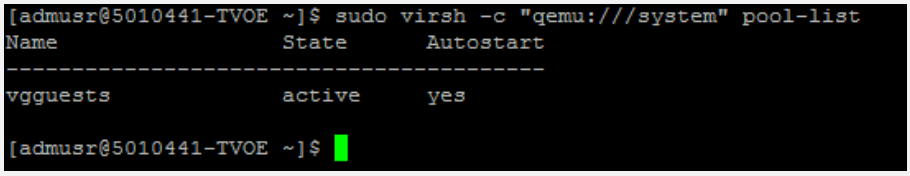
Procedure 19. Restore TVOE Configuration from Backup Media

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

Procedure 19. Restore TVOE Configuration from Backup Media

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

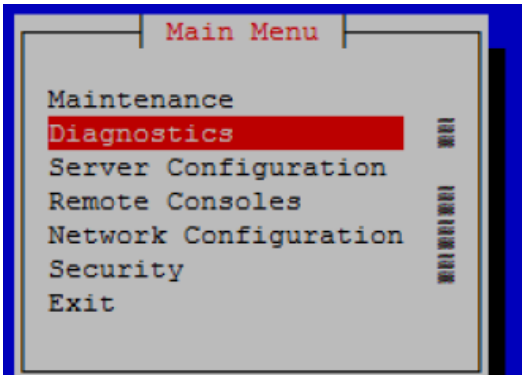
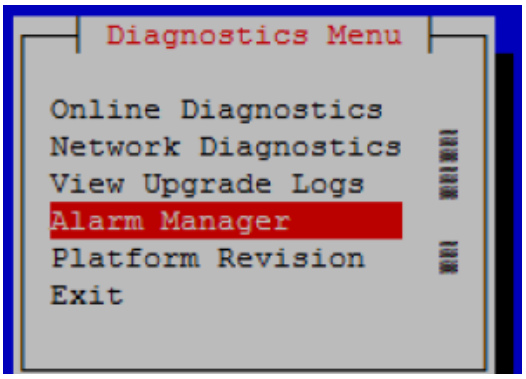
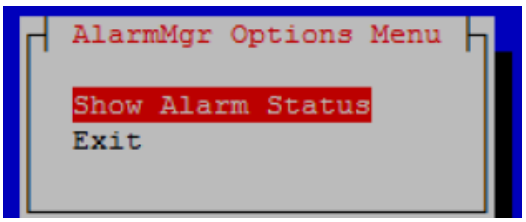
Procedure 19. Restore TVOE Configuration from Backup Media

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).

Procedure 19. Restore TVOE Configuration from Backup Media

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 19. 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 20. Restore PMAC from Backup Media

S T E P #		
	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 [8].
2. ☐	**PMAC**: Login	Establish an SSH session to the PMAC server and 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.

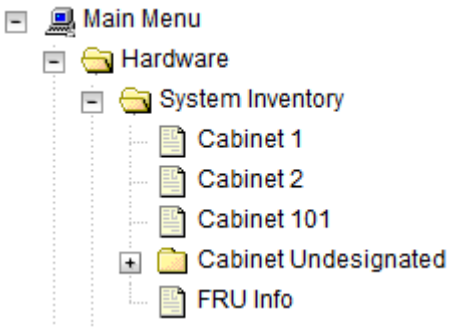
4. ☐	**PMAC**: Verify no Alarms are present	Verify no alarms are present. `$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus`

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

Procedure 20. 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.

Procedure 20. Restore PMAC from Backup Media

8. ☐	**PMAC GUI**: Verify system inventory	1. Navigate to **Hardware > System Inventory**.  2. Verify previously provisioned enclosures are present.

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 DSR, SDS (Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only), and TPD ISOs to the PMAC Server** from reference [8] for all required ISO images.

Procedure 21. Restore PMAC from Backup Server

S T E P #		
	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 [8]. ***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**.

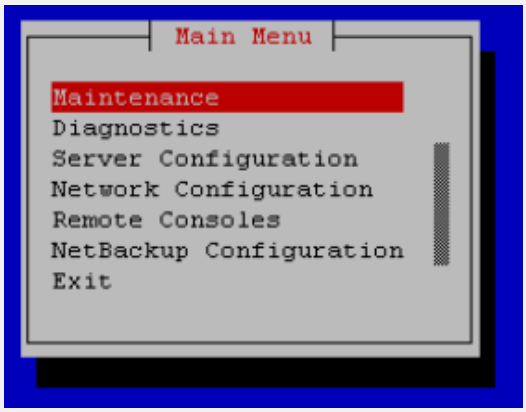
3. ☐	**PMAC TVOE Host**: Log into PMAC guest console	1. On the TVOE host, execute this command:
		`$sudo virsh list`
		This produces a listing of currently running virtual machines.
		`[admusr@Oahu-TVOE-1 ~]$ sudo virsh list`
		` Id Name State`
		`----------------------------------------------------`
		` 1 Oahu-PMAC running`
		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:
		`$sudo virsh console <PMAC-VMID>`
		Where PMAC-VMID is the VM ID you obtained in step 3:
		`[admusr@Oahu-TVOE-1 ~]$ sudo virsh console 1`
		`Connected to domain Oahu-PMAC`
		`Escape character is ^]`
		
		`Oracle Linux Server release 6.7`
		`Kernel 2.6.32-573.3.1.el6prerel7.0.3.0.0_86.37.0.x86_64 on an x86_64`
		
		`Oahu-PMAC login:`
		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 21. 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 21. 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 [8] starting at step 4. ***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 exist 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 21. Restore PMAC from Backup Server

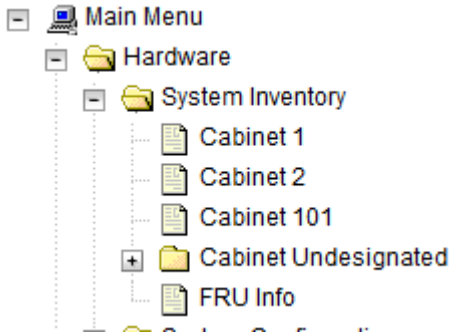
10. ☐	**Backup Server**: Verify appropriate PMAC backup exists	This step is likely executed by customer IT personnel. 1. Log into the backup server as the appropriate user using the user password. 2. Execute the appropriate commands to verify the PMAC backup exists for the desired date. 3. Execute the 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	1. Restore the PMAC data from backup.
		`$ sudo /usr/TKLC/smac/bin/pmacadm restore`
		`PM&C Restore been successfully initiated as task ID 1`
		2. Check the status of the background task:
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		Note: The result eventually displays PMAC Restore successful.

Procedure 21. 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.

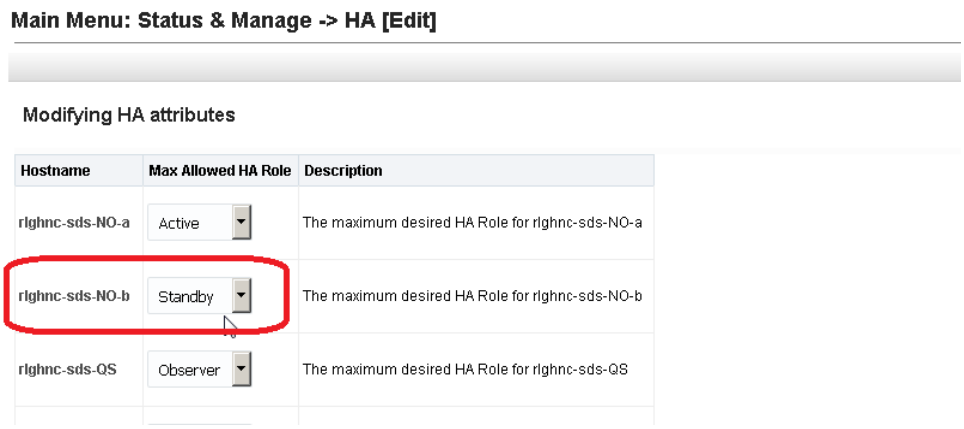
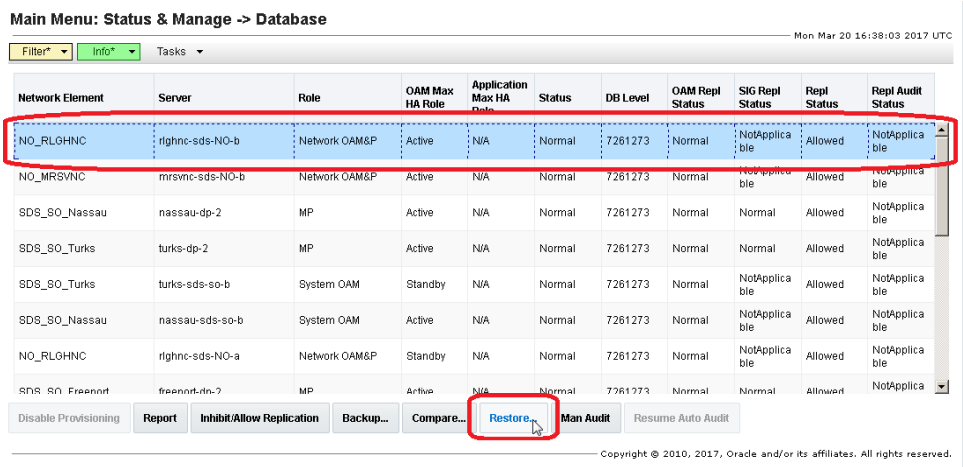
Procedure 21. Restore PMAC from Backup Server

<table>
<tr>
<td>15. ☐</td>
<td>PMAC GUI: Verify system inventory</td>
<td>1. Navigate to Hardware > System Inventory.
 

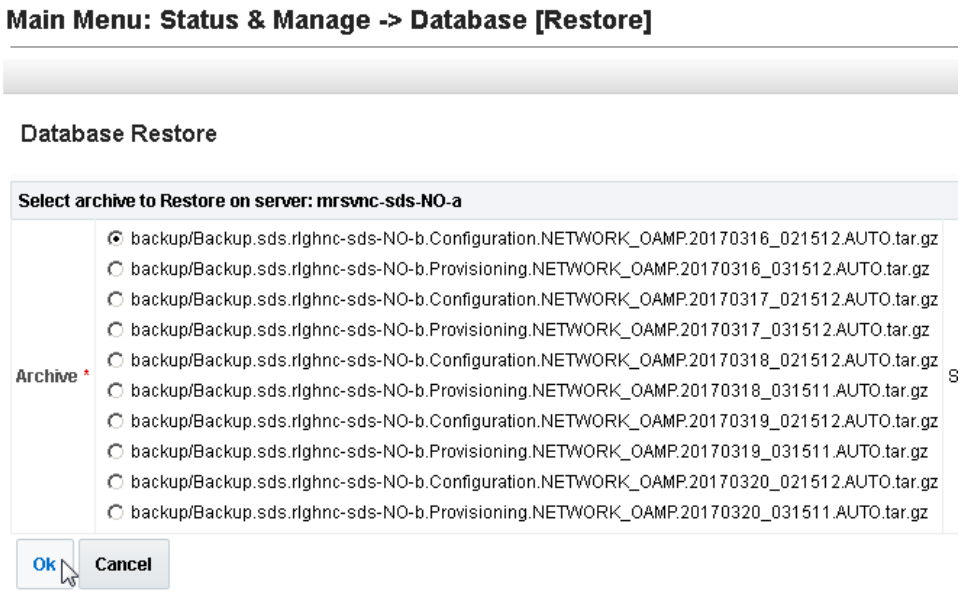
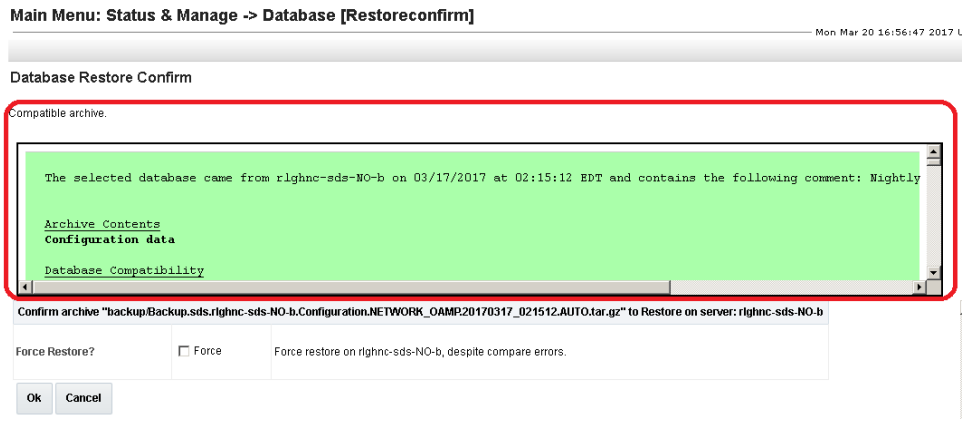
2. Verify previously provisioned enclosures are present</td>
</tr>
<tr>
<td>16. ☐</td>
<td>PMAC: Verify PMAC</td>
<td>Perform a system health check on the PMAC.
<code>$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</code>
This command should return no output on a healthy system.
<code>$ sudo /usr/TKLC/smac/bin/sentry status</code>
All processes should be running, displaying output similar to the following:
<code>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.</code></td>
</tr>
<tr>
<td>17. ☐</td>
<td>PMAC: Add ISO images to the PMAC</td>
<td>Re-add any needed ISO images to the PMAC by executing procedure Load Application and TPD ISO onto PMAC Server from reference [8].</td>
</tr>
</table>

Appendix I. Restore Provisioning Database

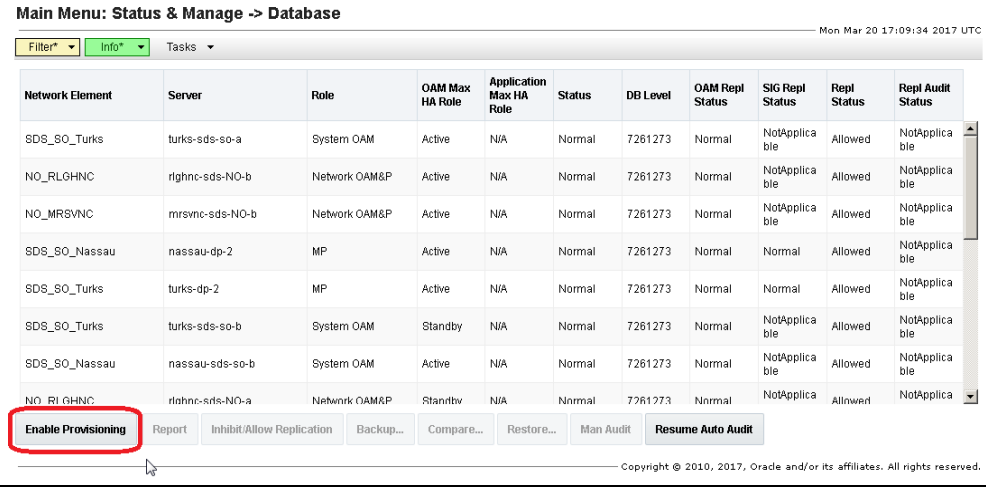
Procedure 22. Restore Provisioning Database

S T E P #	This procedure restores the SDS provisioning database. 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. ☐	**Primary SDS NOAM GUI**: Log into the primary SDS NOAM GUI	Log into primary SDS NOAM GUI using its static IP (not the VIP).
2. ☐	**Primary SDS NOAM GUI**: Place the newly recovered standby NOAM into forced standby	1. Navigate to **Status & Manage > HA**. 2. Click **Edit**. 3. Move the newly recovered standby server to forced **Standby**. 
3. ☐	**Primary SDS NOAM GUI**: Restore provisioning data	1. Navigate to **Status & Manage > Database**. 2. Select the active NOAM and click **Restore**.  3. Select the **Provisioning backup** file from the list (which was previously placed

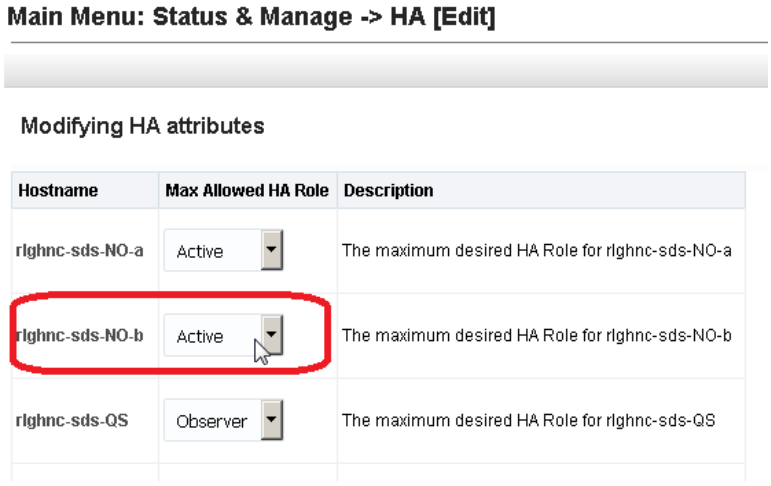
Procedure 22. Restore Provisioning Database

		in the **/var/TKLC/db/filemgmt/backup** directory in step 5 of section 2.6.2) and click **OK**. ***Note:*** You must use a **provisioning only** backup file. Combined backup files contain configuration and provisioning data and cause catastrophic issues, which could lead to a complete re-installation.  4. Verify compatibility and click **OK** to restore. 
4. ☐	**Primary SDS NOAM GUI**: Wait for the restore to begin and track progress until the restore is complete	1. Wait 60 seconds for the restore to begin. 2. Monitor the Info tab under the **Status & Manage > Database** screen and look for the following message: Restore on <Active_NO_hostname> status MAINT_IN_PROGRESS. 3. Wait for the restore to complete by looking for the following message: Success: - Restore on rlghnc-sds-NO-b status MAINT_CMD_SUCCESS. Success ***Note:*** Refresh the Info tab manually to see updated status by navigating to **Status & Manage > Database** again and selecting the Info tab.

Procedure 22. Restore Provisioning Database

5. ☐	Primary SDS NOAM GUI: Uninhibit servers	Uninhibit all servers in the following staggered arrangement: 1. Uninhibit active NOAM. Refresh/monitor the **Status & Manage > Database** screen until a valid **DB Level** displays for the active NOAM. 2. Uninhibit **standby** NOAM/Query server. Refresh/monitor the **Status & Manage > Database** screen until a valid **DB Level** displays for the standby NOAM/Query server. 3. Uninhibit **active** SOAMs. Refresh/monitor the **Status & Manage > Database** screen until a valid **DB Level** displays for the active SOAMs. 4. Uninhibit **standby** SOAMs/DPs. Refresh/monitor the **Status & Manage > Database** screen until a valid **DB Level** displays for the standby SOAMs/DPs.
6. ☐	Recover Pdbrelay (if needed)	Verify whether PDB Relay is **Enabled** by following the instructions in Appendix J Recover PDB Relay.
7. ☐	**Primary SDS NOAM GUI**: Enable provisioning	Navigate to **Status & Manage > Database** and click **Enable Provisioning**. 

Procedure 22. Restore Provisioning Database

8. ☐	**Primary SDS NOAM GUI**: Remove NO from forced standby	1. Navigate to **Status & Manage > HA** and click **Edit**. 2. Select the server, which was moved to forced standby in step 2, change **Max HA Role** to **Active**, and click **OK**. 

Appendix J. Recover PDB Relay

Procedure 23. Recover PDB Relay

S T E P #	This procedure re-establishes the PDB relay connection. 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 console**: Determine if pdbrelay is enabled	Execute following command on console of Active NOAM server (accessed via the VIP) and compare the output:
		`$ iqt -zhp -fvalue ProvOptions where "var='pdbRelayEnabled'"`
		`TRUE`
		Proceed to next step only if the result of above command is **true**.

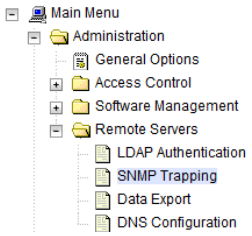
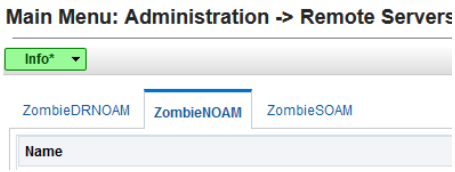
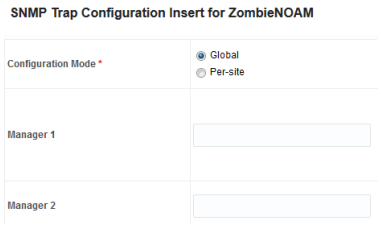
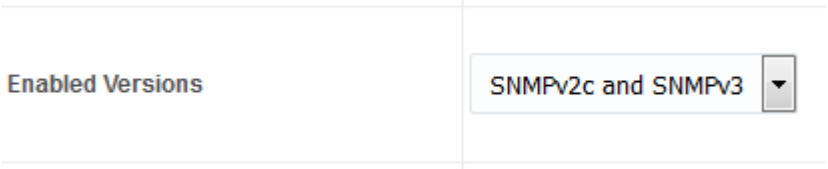
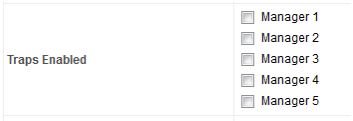
2. ☐	**NOAM VIP GUI**: Disable pdbrelay	Unmark the **PDB Relay Enabled** checkbox on the **SDS > Configuration > Options** screen and click **Apply**.
3. ☐	**NOAM VIP Console**: Emergency restart (start from beginning of Cmd log)	Execute following command on console: `$ iset -fvalue=0 ProvOptions where "var='pdbRelayMsgLogTimeStamp'"`
4. ☐	**NOAM VIP GUI**: Enable pdbrelay	Mark the **PDB Relay Enabled** checkbox on the **SDS > Configuration > Options** screen and click **Apply**.

Appendix K. SNMP Configuration

Procedure 24. Configure SNMP

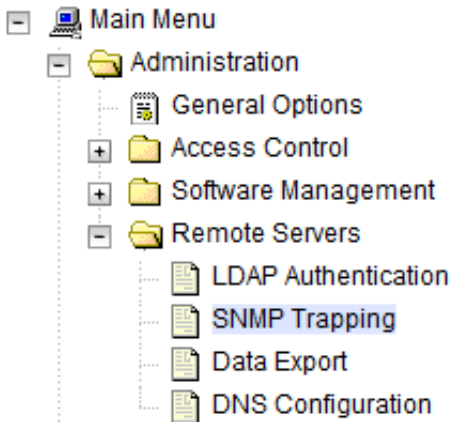
S T E P #	This workaround configures SNMP with SNMPv2c and SNMPv3 as the enabled versions for SNMP traps configuration since PMAC does not support SNMPv3. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended 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: 

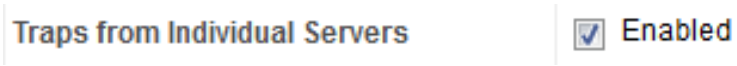
Procedure 24. Configure SNMP

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 24. Configure SNMP

<table>
<tr>
<td>3. ☐</td>
<td>NOAMP VIP: Enable traps from individual servers (optional)</td>
<td>
Note: By default SNMP traps from MPs are aggregated and displayed at the active NOAMP. If, instead, you want every server to send its own traps directly to the NMS, then execute this procedure.

This procedure requires all servers, including MPs, to have an XMI interface on which the customer SNMP target server (NMS) is reachable.
1. Navigate to Administration > Remote Servers > SNMP Trapping.


2. Make sure the Enabled checkbox is marked.


3. Click Apply and verify the data is committed.
</td>
</tr>
<tr>
<td>4. ☐</td>
<td>PMAC GUI: Update the TVOE host SNMP community string</td>
<td>
1. Establish an SSH session to the PMAC.
2. Login as admusr user:
3. Update the TVOE hos community string with this command:
<pre>$ sudo pmaccli setCommStr --accessType=rw --
commStr=<site specific value></pre>
Note: When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest on the PMAC control network are updated. All those servers that match the existing Site Specific Community String are not updated again until the string name is changed.
</td>
</tr>
</table>

Appendix L. Backup Directory

Procedure 25. Backup Directory

S T E P #		
	This procedure checks and creates the backup directory. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	

1. ☐	**NOAM/SOAM VIP Console**: Determine if backup directory exists	1. Execute this command an active NOAM/SOAM server console (accessed using the VIP) and compare the output.
		`$ cd /var/TKLC/db/filemgmt/`
		`$ ls -ltr`
		2. Look for the backup directory in the output.
		3. Make sure the directory is already created with correct permission. The directory looks like this:
		`drwxrwx--- 2 awadmin awadm 4096 Dec 19 02:15 backup`
		4. If the directory is already there with correct permissions, then skip steps 2 and 3.
		5. If directory does not have the correct permissions, then go to step 3.

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

Procedure 25. Backup Directory

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

4. ☐	**NOAM/SOAM VIP Console**: Copy the backup file to the backup directory	1. Copy the backup file to the backup directory.
		`$ cp BACKUPFILE /var/TKLC/db/filemgmt/backup`
		2. Change permissions of files in the backup directory.
		`$ chmod 666 Backup.*`
		3. Change ownership of files in the backup directory.
		`$ sudo chown -R awadmin:awadm Backup.*`

Appendix M. netConfig backupConfiguration/restoreConfiguration/upgradeFirmware with TPD cipher change

Beginning with TPD 7.6.0.0.0_88.50.0, 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), as these switches use other ciphers. Executing these commands with the restricted ciphers would fail as shown below:

```
[admusr@p5-pmac ~]$ /usr/bin/sudo /usr/TKLC/plat/bin/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 following procedure must be executed before and after netConfig backup and restore operations.

Procedure 26. Turn off cipher list before backupConfiguation/restoreConfiguration/upgradeFirmware command

STEP #	Procedure	Description
This procedure prepares the PM&C to avoid the cipher mismatch issue with Cisco switches. This is performed before the netConfig backup, restore or upgrade 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	From the PMAC shell enter the following:
		`/usr/bin/sudo /bin/vi /etc/ssh/sshd_config`
		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	`/usr/bin/sudo service sshd restart`

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

Procedure 27. Resume cipher list after backupConfiguation/restoreConfiguration/upgradeFirmware command

STEP #	Task	Description
This procedure restores the PM&C restricted cipher list after perform the netConfig backup, restore or upgrade 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	From the PMAC shell enter the following: /usr/bin/sudo /bin/vi /etc/ssh/sshd_config Uncomment the three lines: Ciphers aes256-ctr,aes192-ctr,aes128-ctr MaxAuthTries 4 LoginGraceTime 1m
2 ☐	Restart sshd	/usr/bin/sudo service sshd restart

Appendix N. My Oracle Support (MOS)

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. 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.