Oracle® Communications

Diameter Signaling Router

Rack Mount Server Disaster Recovery Guide

Release 8.0

E76187-02

June 2017

ORACLE

Oracle Communications Diameter Signaling Router Rack Mount Server Disaster Recovery Procedure

CAUTION:

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

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

Table of Contents

List of Tables

List of Figures

List of Procedures

1.0 Introduction

1.1 Purpose and Scope

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/HP DL380 Gen9 Only).

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

1.2 References

[1] TPD Initial Product Manufacture, E54521-01
[2] Platform 7.2 Configuration Procedure Reference, E64363
[3] DSR FABR Feature Activation Procedure, E78925
[4] DSR RBAR Feature Activation Procedure, E78926
[5] DSR MAP-Diameter Feature Activation Procedure, E78927
[6] PM&C 6.4 Disaster Recovery Guide, E82637
[7] DSR PCA Activation Guide, E81528
[8] DSR Rack Mount Server Installation Guide, E76182
[9] DSR Hardware and Software Installation Procedure 1/2, E76180
[10] DCA Framework and Application Activation and Deactivation Guide, E76934
[11] DSR Security Guide, E76974
[12] DSR DTLS Feature Activation Procedure, E78942
[13] DSR / SDS 8.x NOAM Failover User's Guide, E85595

1.3 Acronyms

Table 1 Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CD	Compact Disk
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
FRU	Field Replaceable Unit
iLO	Integrated Lights Out manager
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
MSA	Modular Smart Array
NB	NetBackup
OA	HP Onboard Administrator
OS	Operating System (e.g. TPD)
RMS	Rack Mounted Server
PMAC	Platform Management & Configuration
SAN	Storage Area Network
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtual Operating Environment
VM	Virtual Machine
VSP	Virtual Serial Port
IPFE	IP Front End
PCA	Policy and Charging Application
IDIH	Integrated Diameter Intelligence Hub
SDS	Subscriber Database Server

1.4 Terminology

Table 2 Terminology

Base hardware	Base hardware includes all hardware components (bare metal) and electrical wiring to allow a server to power on.
Base software	Base software includes installing the server's operating system: Oracle Platform Distribution (TPD).
Failed server	A failed server in disaster recovery context refers to a server that has suffered partial or complete software and/or hardware failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-install the software and/or hardware.
Software Centric	The business practice of delivering an Oracle software product, while relying upon the customer to procure the requisite hardware components. Oracle provides the hardware specifications, but does not provide the hardware or hardware firmware, and is not responsible for hardware installation, configuration, or maintenance.
Enablement	The business practice of providing support services (hardware, software, documentation, etc) that enable a 3rd party entity to install, configuration, and maintain Oracle products for Oracle customers.

1.5 Optional Features

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

Table 3 Optional Features

Feature	Document
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation Procedure, E78926
Map-Diameter Interworking (MAP-IWF)	DSR MAP-Diameter Feature Activation Procedure, E78927
Policy and Charging Application (PCA)	DSR PCA Activation, E81528
Full Address Based Resolution (FABR)	DSR FABR Feature Activation Procedure, E78925
Diameter Custom Applications (DCA)	DCA Framework and Application Activation and Deactivation Guide, E76934
Host Intrusion Detection System (HIDS)	DSR Security Guide, E76974 (Section 3.2)

1.6 Revision History

Date	Description
October 2016	Initial Release

2.0 General Description

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

Recovery of the entire network from a total outage	• All NOAM servers failed • All SOAM servers failed
Recovery of one or more servers with at least one NOAM server intact	• 1 or more NOAM servers intact • 1 or more SOAM or MP servers failed
Recovery of the NOAM pair with one or more SOAM servers intact	• All NOAM servers failed • 1 or more SOAM servers intact
Recovery of one or more server with at least one NOAM and one SOAM server intact.	• 1 or more NOAM servers intact • 1 or more SOAM servers intact • 1 SOAM or 1 or more MP servers failed
Recovery of one or more server with corrupt databases that cannot be restored via replication from the active parent node.	

Note: For Failed Aggregation switches (HP DL380 Gen 8 Only) refer to **Appendix B**. Recovering/Replacing Failed Cisco 4948 Aggregation Switches.

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

2.2 Partial server outage with one NOAM server intact and all 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 will recover 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 will recover the database to all servers. (**Note:** this includes failures of any disaster recovery 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

3.0 Procedure Overview

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

3.1 Required Materials

The following items are needed for disaster recovery:

1. A hardcopy of this document (E76187) 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/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/HP DL380 Gen9 Only)
15. Latest RADIUS shared secret encryption key file backup (DpiKf.bin.encr)
16. List of activated and enabled features

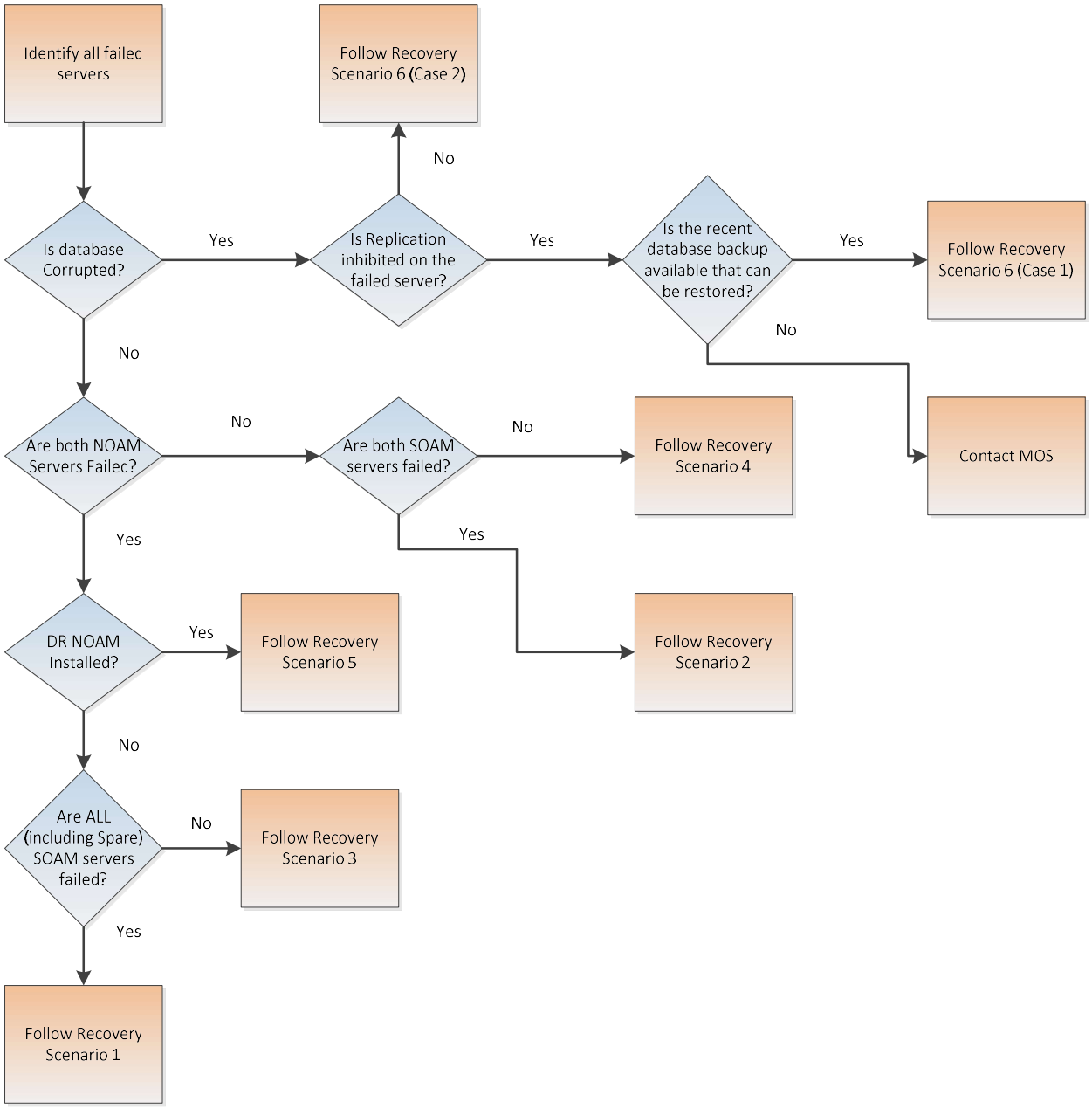
Note: For all Disaster Recovery scenarios, we assume that the NOAM Database backup and the SOAM database backup were performed around the same time, and that no synchronization issues exist among them.

3.2 Disaster Recovery Strategy

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

1. Evaluate failure conditions in the network and determine that normal operations cannot continue without disaster recovery procedures. This means the failure conditions in the network match one of the failure scenarios described in **section 2.0**.
2. Read and review the content in this document.
3. Gather required materials in **section 3.1** Required Materials
4. From the failure conditions, determine the Recovery Scenario and procedure to follow (using **Figure 1.** Determining Recovery Scenario and **Table 4.** Recovery Scenarios.
5. Execute appropriate recovery procedures (listed in **Table 4.** Recovery Scenarios).

Figure 1. Determining Recovery Scenario



4.0 Procedure Preparation

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

Note: A failed server in disaster recovery context refers to a server that has suffered partial or complete software 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.

Table 4. Recovery Scenarios

Recovery Scenario	Failure Condition	Section
1	• All NOAM servers failed. • All SOAM servers failed. • MP servers may or may not be failed.	Section 5.1.1 Recovery Scenario 1 (Complete Server Outage)
2	• At least 1 NOAM server is intact and available. • All SOAM servers failed. • MP servers may or may not be failed.	Section 5.1.2 Recovery Scenario 2 (Partial Server Outage with at least one NOAM server intact and all SOAMs failed)
3	• All NOAM servers failed. • At least 1 SOAM server out of Active, StandBy, Spare is intact and available. • MP servers may or may not be failed.	Section 5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact)
4	• At least 1 NOAM server is intact and available. • At least 1 SOAM server out of Active, StandBy, Spare is intact and available. • 1 or more MP servers have failed.	Section 5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)
5	• Both NOAM servers failed. • DR NOAM is Available • SOAM servers may or may not be failed. • MP servers may or may not be failed.	Section 5.1.5 Recovery Scenario 5 (Both NOAM servers

		failed with DR-NOAM available)
6: Case 1	• Server is intact • Database gets corrupted on the server • Replication channel from parent is inhibited because of upgrade activity	Section 5.1.6.1 Recovery Scenario 6: Case 1
6: Case 2	• Server is intact • Database gets corrupted on the server • Latest Database backup of the corrupt server is NOT present • Server having a corrupted database • Replication channel is not inhibited • Server has the same release as that of its Active parent	Section 5.1.6.2 Recovery Scenario 6: Case 2

5.0 Disaster Recovery Procedure

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

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

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

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

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

Recovering Base Hardware:

1. Hardware Recovery will be executed by the appropriate HW vendor.
2. Base Hardware Replacement must be controlled by engineer familiar with DSR Application

5.1 Recovering and Restoring System Configuration

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

5.1.1 Recovery Scenario 1 (Complete Server Outage)

For a complete server outage, TVOE is recovered on all RMS 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 will recover the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures' detailed steps are in Procedure 1. The major activities are summarized as follows:

Recover Base Hardware and Software for all RMSs:

- 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 IDIH 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 are failed. This procedure also caters the C-Level Sever failure Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact **Appendix K. My Oracle Support (MOS)** and ask for assistance.	
1. ☐	**Workarounds**	Refer to **Appendix G**. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
2. ☐	**Gather Required Materials**	Gather the documents and required materials listed in **Section 3.1** Required Materials
3. ☐	**Replace Failed Equipment**	HW vendor to replace the failed equipment
4. ☐	**Recover PMAC TVOE Host (If Required):** 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:"***Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings"* • **HP DL380 Gen9:** *"Configure HP Gen9 Server BIOS Settings"* 2. Verify and/or upgrade server firmware by executing procedure *"Upgrade Rack Mount Server Firmware"* from reference [8]
5. ☐	**Recover PMAC and PMAC TVOE Host:** Backup Available	This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, **skip this step**. 1. Restore the TVOE backup by executing **Appendix E**. Restore TVOE Configuration from Backup Media on **ALL** failed rack mount servers 2. Restore the PMAC backup by executing **Appendix F**. Restore PMAC from Backup **Proceed to Step 7**
6. ☐	**Recover PMAC and PMAC TVOE Host:** Backup Not Available	This step assumes that TVOE and PMAC backups are **NOT** available, if the TVOE and PMAC have already been restored, **skip this step** 1. Execute procedure *"Install and Configure TVOE on First RMS (PMAC Host)"* from reference [8] 2. Execute section *"Install PMAC"* from reference [8] 3. Execute section *"Initialize the PMAC Application"* from reference [8] **Proceed to Next Step**

Procedure 1: Recovery Scenario 1

7. ☐	**Recovery Failed Cisco 4948 Aggregation Switches** (HP DL380 Only)	**Oracle X5-2/Netra X5-2/X6-2/HP DL380 GEN 9 SKIP THIS STEP** Recover failed Cisco 4948 aggregation switches, if needed: Backup configuration files available: Refer to **Appendix B**. Recovering/Replacing Failed Cisco 4948 Aggregation Switches to recover failed Cisco 4948 aggregation switches Backup configuration files **NOT** available: Execute section "Configure Cisco 4948E-F Aggregation Switches (HP DL 380 Gen 8 Only)" 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 sections *"Configure PMAC Server (NetBackup Only)"* and *"Add RMS to the PMAC Inventory"* from reference [8]
9. ☐	**Install/Configure Additional Rack Mount Servers** (Backups available)	This step assumes that TVOE backups are available, if backups are **NOT** available, **skip this step**. 1. Execute procedure *"Install TVOE on Additional Rack Mount Servers"* from reference [8] 2. Restore the TVOE backup by executing **Appendix E**. Restore TVOE Configuration from Backup Media on **ALL** failed rack mount servers
10. ☐	**Install/Configure Additional Rack Mount Servers** (Backups ***NOT*** available)	This step assumes that TVOE backups are ***NOT*** available, if backups are available, execute the previous step. 1. Execute procedure *"Install TVOE on Additional Rack Mount Servers"* from reference [8] 2. Execute *"Configure TVOE on Additional Rack Mount Servers"* from reference [8]
11. ☐	**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:** *"Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings"* • **HP DL380 Gen9:** *"Configure HP Gen9 Server BIOS Settings"* 2. Verify and/or upgrade server firmware by executing procedure *"Upgrade Rack Mount Server Firmware"* from reference [8]

Procedure 1: Recovery Scenario 1

12. ☐	**Determine VM Placement and Socket Pinning** (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen9 Only)	**HP DL380 GEN 8 SKIP THIS STEP** Determine the VM placement and Pinning for proper VM placement and pinning.Refer 12 for workbook reference
13. ☐	**Deploy Redundant PMAC (if required)**	Refer to procedure *"Deploy Redundant PMAC (Optional)"* to re-deploy and configure any redundant PMACs previously configured.
14. ☐	**PMAC: Determine if a fdconfig file exists from the initial deployment.**	Determine whether the fdconfig backup file exists: [admusr@melbourne-pmac-1 ~]$ ll /usr/TKLC/smac/etc/fdc/ Examine the results and verify whether the rms config file <hostname>.cfg exists Note: There may be multiple fdconfig backup files here with respect to each RMS. Select the respective one according to the RMS.
15. ☐	**If fdc backup file does NOT exist:**	**Execute this step ONLY If the fdconfig backup file does NOT exist:** If the fdconfig file does NOT exist : Create the needed file(s) by executing section "Virtual Machine/Network Fast Deployment" from reference [8] **WARNING**: It is very important to ensure the file(s) created only affect the TVOE server(s) and its 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. Skip to step 24 if this step was executed
16. ☐	**PMAC [If fdc backup file exists]: Load ISOs into PMAC if not done already**	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:** If the DSR, SDS, and TPD ISOs are NOT loaded in to the PMAC: Execute procedures 14 of section "Virtual Machine/Network Fast Deployment" from reference [8] If already loaded into PMAC, skip this step.
17.	**PMAC [If fdc backup**	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:**

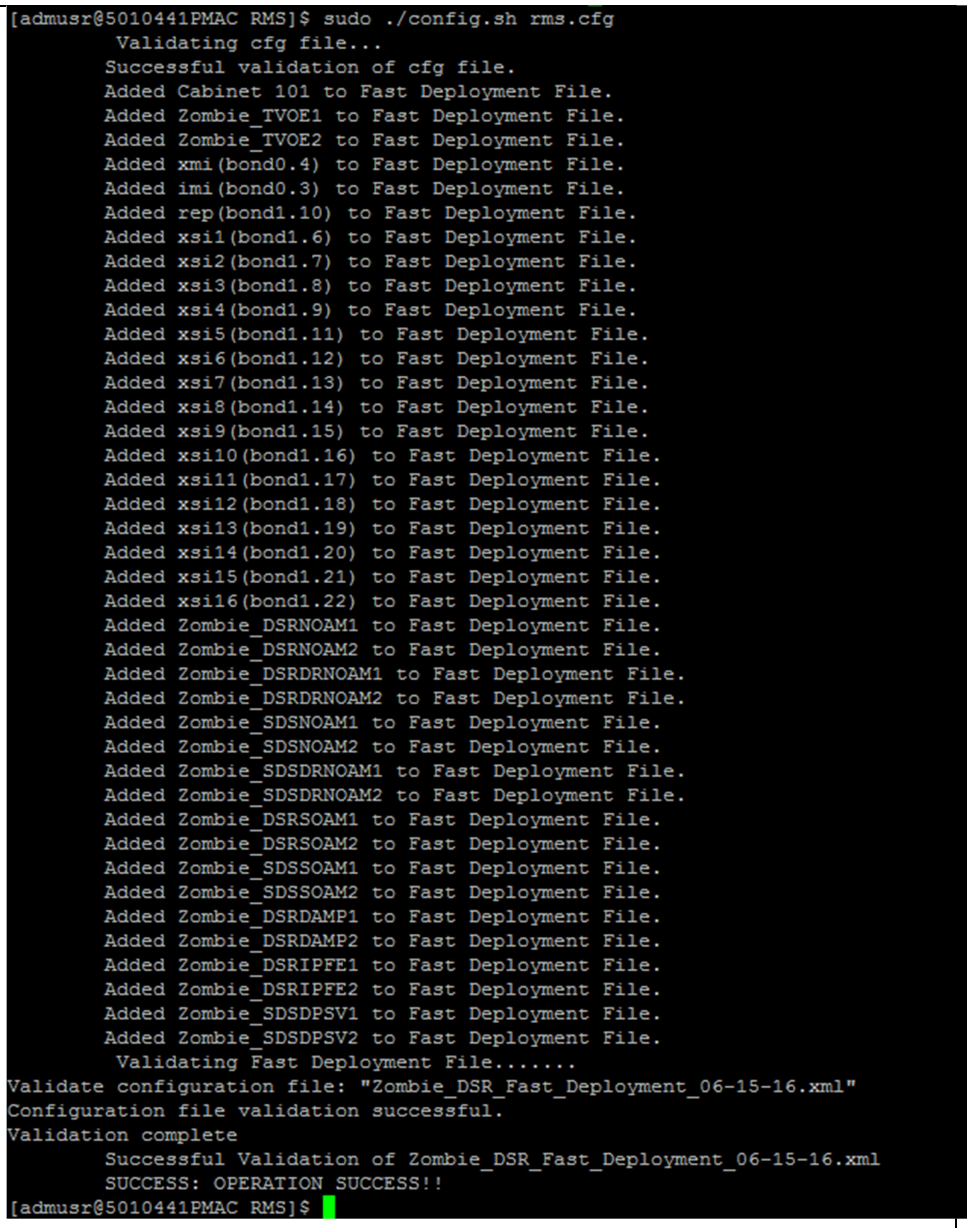
Procedure 1: Recovery Scenario 1

☐	**file exists]:** Edit/Update Configuration File	**Edit the fdconfig file to include only the required/failed servers.** **Note:** Comment out configuration items that are not needed. **Note:** It is recommended that a separate configuration file be created for **EACH** rack mount server being deployed. Note:Cabinet ID in the config file needs to match the cabinet already defined in PM&C" 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) • SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured) • SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured) • SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured) • SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured) **Note:** Refer to **Appendix R: VM Automation Profile Values** for DSR and SDS profile values with the configuration file from reference [8] Note: Comment out SDS and DSR profile items if corresponding products are not used. **Note: [Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/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] **Note:** The VM names should not be modified in the .cfg file. The names are fixed and will be prefixed in the siteName. **Note:** The VM locations should not be changed from their 'RMSx' format. Each RMS should correspond with a separate Rack Mount Server. **WARNING**: It is very important to ensure the file(s) created only affect the TVOE server(s) and its 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.

Procedure 1: Recovery Scenario 1

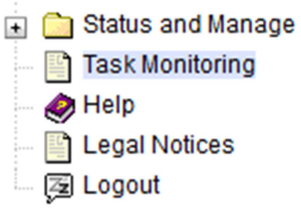
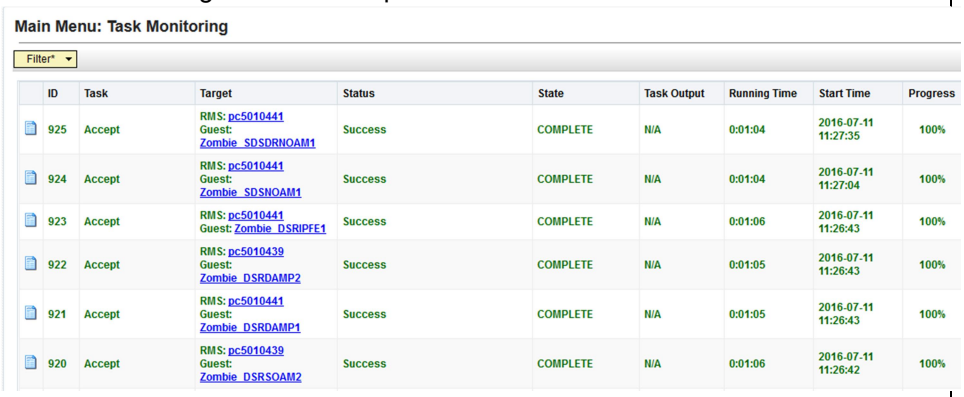
18. ☐	**PMAC [If fdc backup file exists]: Copy the located backed up fdc file to the RMS directory**	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:** Copy the located fdconfig backup file to the RMS directory: `$ cp /usr/TKLC/smac/etc/fdc/<back up_fdc_file> /usr/TKLC/smac/etc/RMS/`
19. ☐	**PMAC [If fdc backup file exists]:** Execute the config.sh script	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:** Execute config.sh against the modified back up config file defined above: **Note:** If the below command is executed on multiple cfg files, it will overwrite the existing xml file. It is recommended to rename the xml file before running the below command again. `$ sudo ./config.sh <config file>` Sample Output:

Procedure 1: Recovery Scenario 1

20. ☐	**PMAC [If fdc backup file exists]:** Execute Fast Deployment	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:**
		
		With the file generated from the config.sh script, execute the following command to start fast deployment:
		
		`$ screen`
		
		`$ sudo fdconfig config --file=<fd_config.xml>`
		
		Note: This is a long duration command. If the screen command was run prior

Procedure 1: Recovery Scenario 1

		to executing the fdconfig, perform a *"screen -dr"* to resume the screen session in the event of a terminal timeout etc.
21. ☐	**PMAC GUI [If fdc backup file exists]:** Monitor the Configuration	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:** If not already done so, establish a GUI session on the PMAC server. Navigate to **Main Menu -> Task Monitoring**  Monitor the configuration to completion:  ID / Task / Target / Status / State / Task Output / Running Time / Start Time / Progress 925 Accept RMS: pc5010441 Guest: Zombie_SDSDRNOAM1 Success COMPLETE N/A 0:01:04 2016-07-11 11:27:35 100% 924 Accept RMS: pc5010441 Guest: Zombie_SDSNOAM1 Success COMPLETE N/A 0:01:04 2016-07-11 11:27:04 100% 923 Accept RMS: pc5010441 Guest: Zombie_DSRIPFE1 Success COMPLETE N/A 0:01:06 2016-07-11 11:26:43 100% 922 Accept RMS: pc5010439 Guest: Zombie_DSRDAMP2 Success COMPLETE N/A 0:01:05 2016-07-11 11:26:43 100% 921 Accept RMS: pc5010441 Guest: Zombie_DSRDAMP1 Success COMPLETE N/A 0:01:05 2016-07-11 11:26:43 100% 920 Accept RMS: pc5010439 Guest: Zombie_DSRSOAM2 Success COMPLETE N/A 0:01:06 2016-07-11 11:26:42 100% **Note:** Should a failure occur with fdconfig, logs can be accessed in /var/TKLC/log/fdconfig/fdconfig.log [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

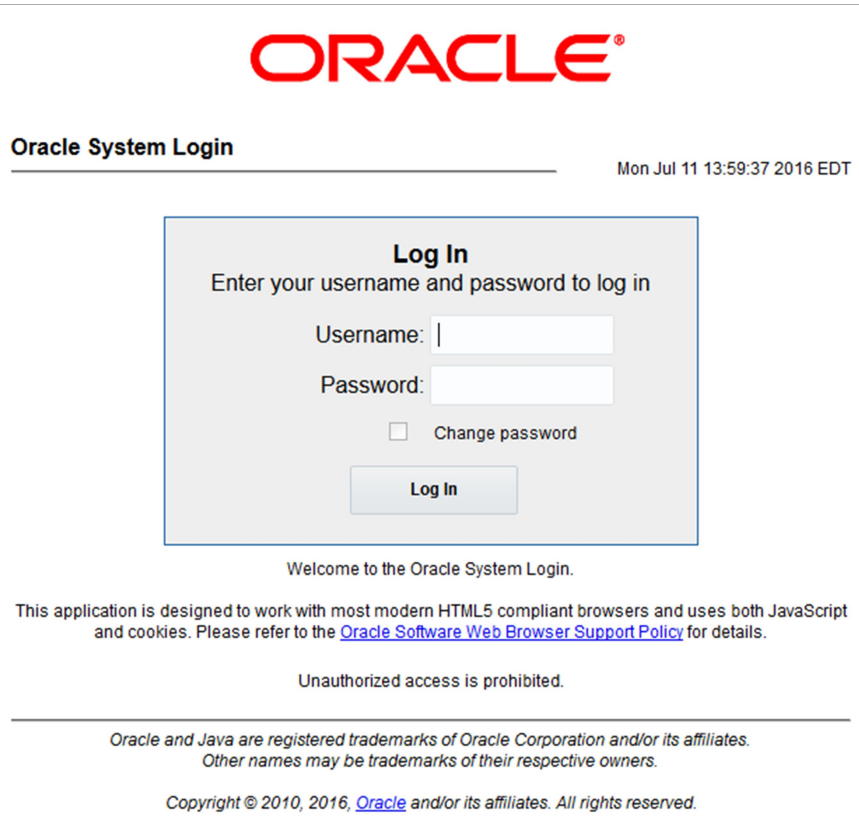
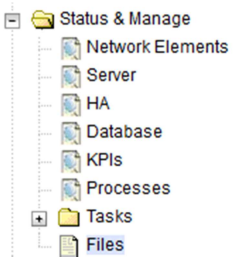
Procedure 1: Recovery Scenario 1

		Run Below command to restart the fdconfig after a failure has occurred and has been resolved: $ sudo fdconfig restart -- file=deploy_melbourne_20170329T202458_701b.fdcdb
22. ☐	**PMAC** **[If fdc backup file exists]:** Repeat for each Rack mount server configuration file	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:** Repeat **steps 14-21** for each rack mount server/configuration file located at step 14, if required.
23. ☐	**PMAC** **[If fdc backup file exists]:** Backup FDC file	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:** Copy the updated fdc file to the fdc backup directory: **$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> /usr/TKLC/smac/etc/fdc/** 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 procedure *"CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen9 Only)"* from reference [8]
25. ☐	**Obtain Latest Database Backup and Network Configuration Data.**	1. Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. 2. Obtain most recent "RADIUS shared secret encryption key" file DpiKf.bin.encr from external backup sources (Only when the RADIUS Key Revocation MOP has been executed on the system) From required materials list in **Section 3.1** `Required Materials`; use site survey documents and Network Element report (if available), to determine network configuration data.
26. ☐	**Execute DSR Installation Procedure for the First NOAM**	Verify the networking data for Network Elements **Note:** Use the backup copy of network configuration data and site surveys (Step 2) **Note:** SDS disaster recovery actions can and should be worked simultaneously, doing so would allow faster recovery of the complete solution

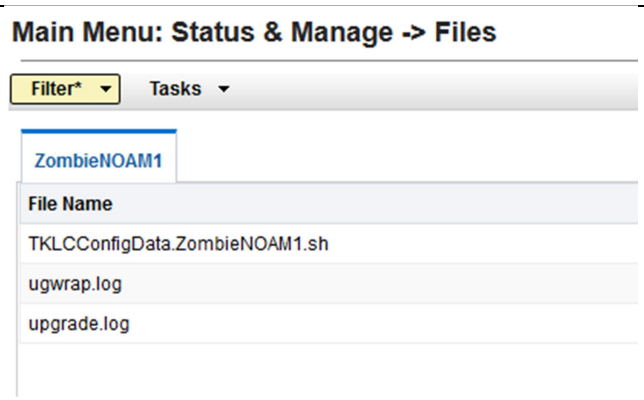
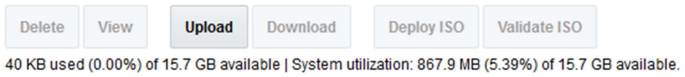
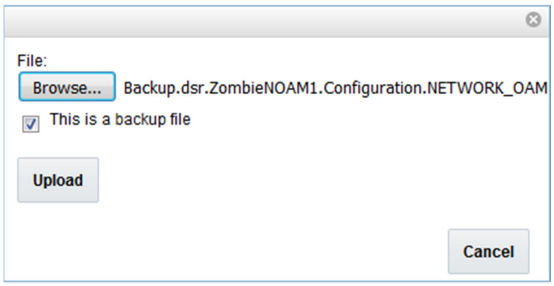
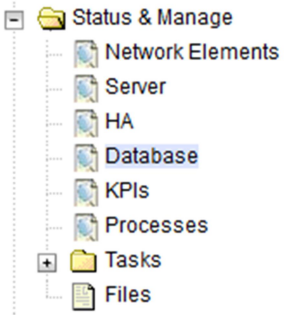
Procedure 1: Recovery Scenario 1

		(i.e. stale DB on DP servers will not receive updates until SDS-SOAM servers are recovered. The following steps will be written to 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 procedure *"Configure First NOAM NE and Server"* from reference [8] 2. Configure the NOAM server group by executing procedure *"Configure the NOAM Server Group"* from reference [8] **SDS:** 1. Configure the first SDS NOAM server by executing procedure *"Configure First SDS NOAM NE and Server"* from reference [8] 2. Configure the SDS NOAM server group by executing procedure *"Configure the SDS NOAM Server Group"* from reference [8]
27. ☐	**NOAM GUI:** Login	**DSR Only, if SDS, Skip to Step 32** Login to the NOAM GUI as the ***guiadmin*** user:

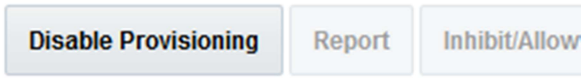
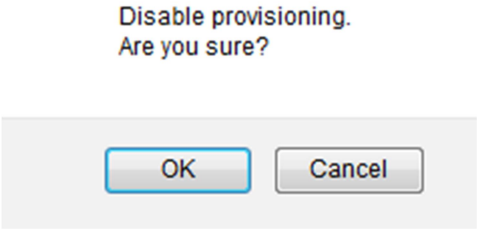
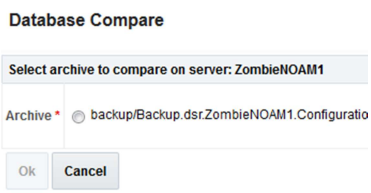
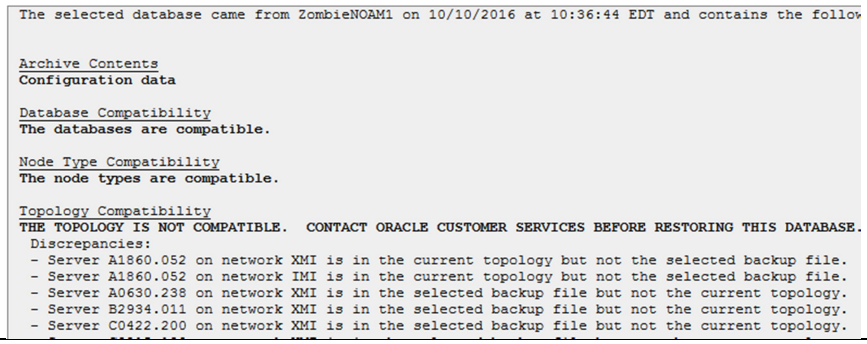
Procedure 1: Recovery Scenario 1

		
28. ☐	**NOAM GUI:** Upload the Backed up Database File	**DSR Only, if SDS, Skip to Step 32** Browse to **Main Menu->Status & Manage->Files**  Select the Active NOAM server. The following screen will appear:

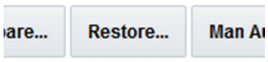
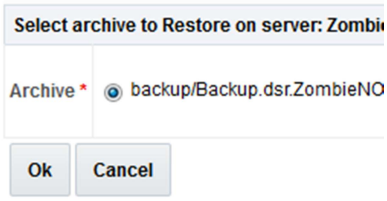
Procedure 1: Recovery Scenario 1

		 Click on **Upload** as shown below and select the file *"NO Provisioning and Configuration:"* file backed up after initial installation and provisioning.  1. Click on **Browse** and locate the backup file 2. Check **This is a backup file** Box 3. Click on Open as shown below.  Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.
29. ☐	**NOAM GUI:** Disable Provisioning	**DSR Only, if SDS, Skip to Step 32** Click on **Main Menu->Status & Manage->Database** 

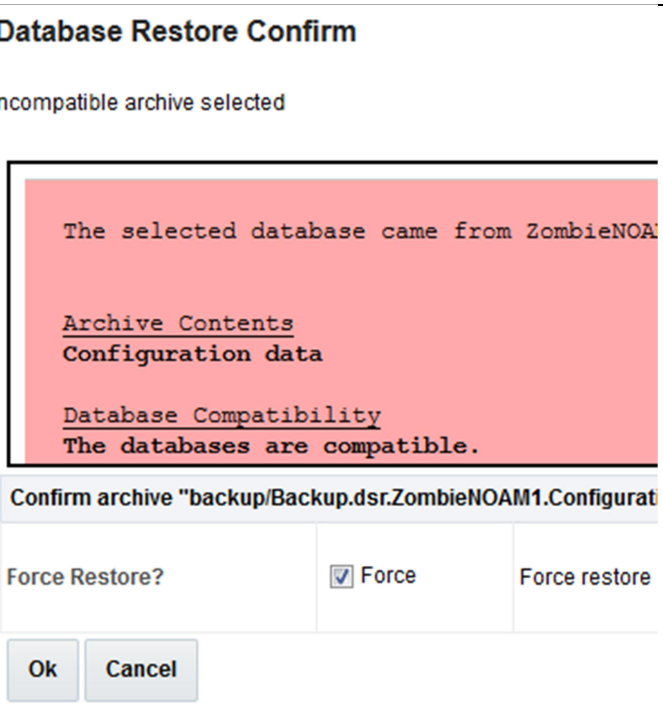
Procedure 1: Recovery Scenario 1

		Disable Provisioning by clicking on **Disable Provisioning** button at the bottom of the screen as shown below.  A confirmation window will appear, press **OK** to disable Provisioning. 
30. ☐	**NOAM GUI:** Verify the Archive Contents and Database Compatibility	**DSR Only, if SDS, Skip to Step 32** Select the **Active NOAM** server and click on the **Compare**.  The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step**28 of this procedure.  **Verify** that the output window matches the screen below. **Note:** You will get a database mismatch regarding the Topology Compatibility and possibly User compatibility (due to authentication) These warnings are expected. If these are the only mismatches, proceed, otherwise stop and contact Appendix K. My Oracle Support (MOS) and ask for assistance. **Database Archive Compare** 

Procedure 1: Recovery Scenario 1

		Note: Archive Contents and Database Compatibilities must be the following: **Archive Contents:** Configuration data **Database Compatibility:** The databases are compatible. **Note:** The following is expected Output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one NOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. **Note:** We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility. If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.
31. ☐	**ACTIVE NOAM:** Restore the Database	**DSR Only, if SDS, Skip to Step 32** From **Main Menu->Status & Manage->Database** Select the **Active NOAM** server, and click on **Restore** as shown below.  The following screen will be displayed. Select the proper back up provisioning and configuration file.  Click **OK** Button. The following confirmation screen will be displayed. If you get errors related to the warnings highlighted in the previous step, that is expected. If no other errors are displayed, select the **Force** checkbox as shown above and Click **OK** to proceed with the DB restore.

Procedure 1: Recovery Scenario 1

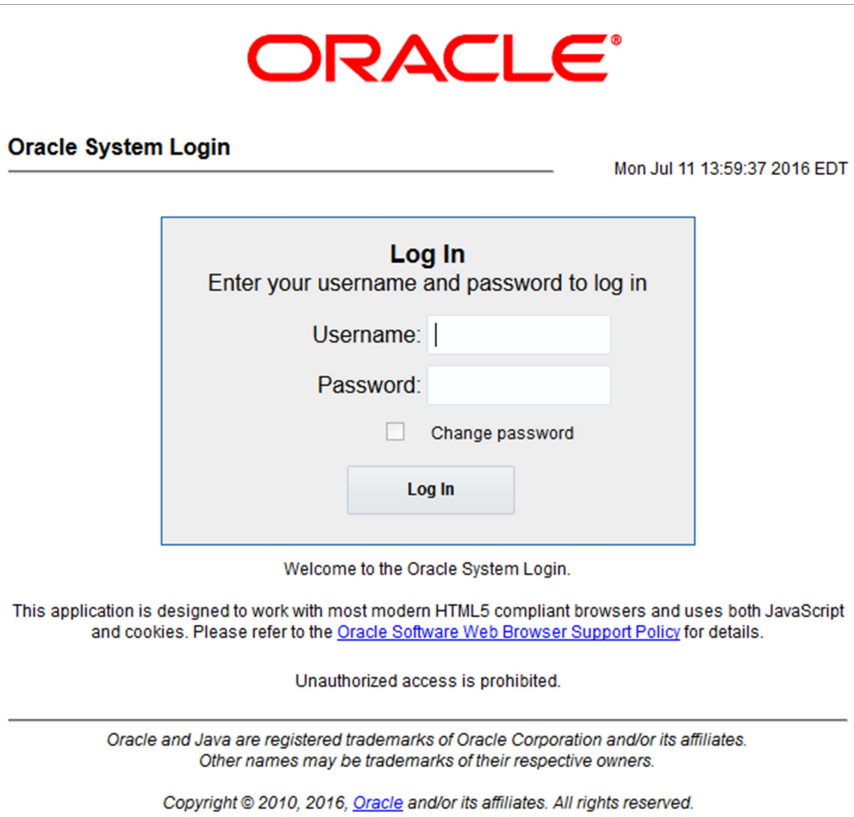
		 **Note:** After the restore has started, the user will be logged out of XMI NO GUI since the restored Topology is old data.

32. ☐	**SDS NOAM:** Transfer SDS Configuration and Provisioning backup Database Files	**SDS Only, if DSR, Skip this step**
		
		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 use the following command to 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 use the following command to copy the provisioning backup file to the SDS NOAM guest:
		
		`# scp < path_to_provisioning_db _file> admusr@<SDS_NOAM_IP>:/var/TKLC/db/filemgmt`
		
		Note: 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.

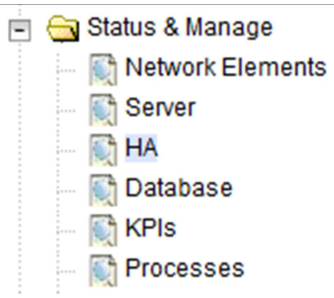
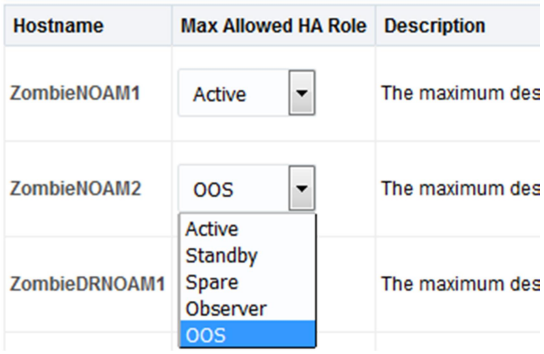
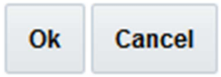
Procedure 1: Recovery Scenario 1

		Windows: Use WinSCP to copy the backup database files into the */var/TKLC/db/filemgmt* directory. Please refer to [9] procedure *Using WinSCP* to copy the backup image to the customer system.
33. ☐	**SDS NOAM:** Login	**SDS Only, if DSR, Skip this step** Establish an SSH session to the SDS active NOAM XMI IP address, login as ***admusr.***
34. ☐	**SDS NOAM:** Stop running applications	**SDS Only, if DSR, Skip this step** 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.
35. ☐	**SDS NOAM:** Restore configuration Database	**SDS Only, if DSR, Skip this step** 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>`
36. ☐	**SDS NOAM:** Restore provisioning Database	**SDS Only, if DSR, Skip this step** Refer Appendix I. Restore Provisioning Database to restore the provisioning DB.
37. ☐	**SDS NOAM:** Start running applications	**SDS Only, if DSR, Skip this step** Start the SDS application by executing the following command: `$ sudo prod.start`
38. ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:

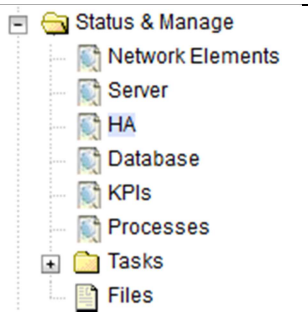
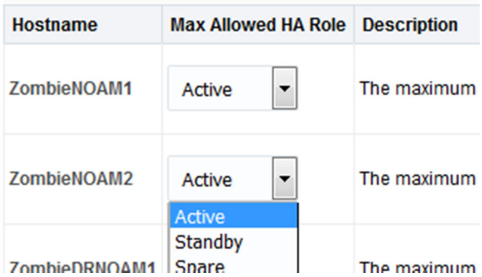
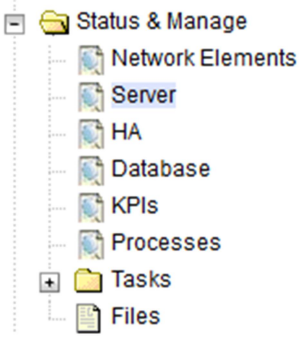
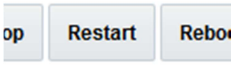
Procedure 1: Recovery Scenario 1

		
39. ☐	**NOAM VIP GUI:** Monitor and Confirm database restoral	Wait for **5-10 minutes** for the System to stabilize with the new topology: Monitor the Info tab for **"Success"**. This will indicate that the restore is complete and the system is stabilized. The following alarms **must** be ignored for NOAM and MP Servers until all the Servers are configured: Alarms with Type Column as **"REPL"** , **"COLL", "HA"** (with mate NOAM), **"DB"** (about Provisioning Manually Disabled) **Note:** Do not pay attention to these alarms until all the servers in the system are completely restored. **Note:** The Configuration and Maintenance information will be in the same state it was backed up during initial backup.
40. ☐	**Active NOAM:** Set Failed Servers to OOS	Navigate to **Main Menu -> Status & Manage -> HA**

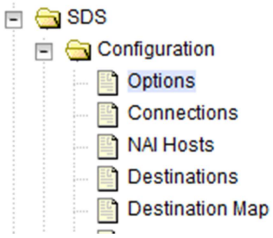
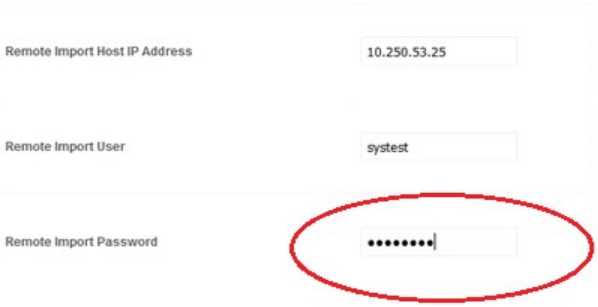
Procedure 1: Recovery Scenario 1

		 Select **Edit** **Modifying HA attributes**  Set the Max Allowed HA Role drop down box to **OOS** for the failed servers. Select **Ok** 
41. ☐	**NOAM VIP GUI:** Recover Standby NOAM	Install the second NOAM server: **DSR:** Execute procedure *"Configure the Second NOAM Server",* steps 1, 3-6 from reference [8] **SDS:** Execute procedure *"Configure the Second SDS NOAM Server",* steps 1, 3-6 from reference [8]
42. ☐	**Install NetBackup Client (Optional)**	If NetBackup is used execute procedure *"Install NetBackup Client (Optional)"* from reference [8]
43. ☐	**NOAM VIP GUI:** Set HA on Standby NOAM	Navigate to **Status & Manage -> HA**

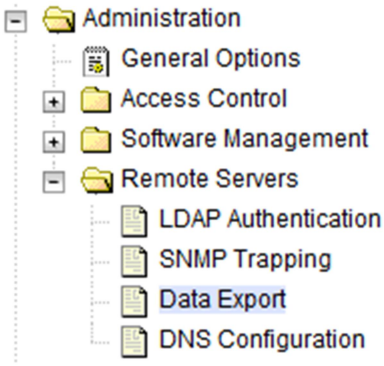
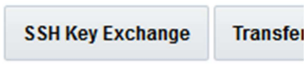
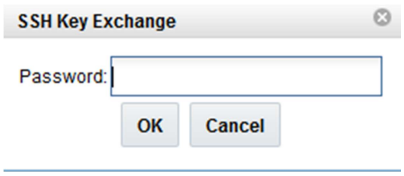
Procedure 1: Recovery Scenario 1

		 Click on **Edit** at the bottom of the screen Select the standby NOAM server, set it to **Active** **Modifying HA attributes**  Press **OK**
44. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered standby NOAM server and click on **Restart**. 
45. ☐	**Active NOAM:** Correct the RecognizedAuthority table	Establish an SSH session to the active NOAM, login as ***admusr***. Execute the following command:

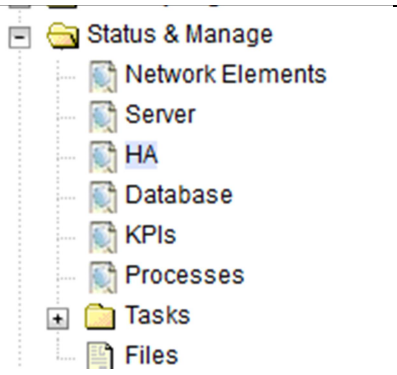
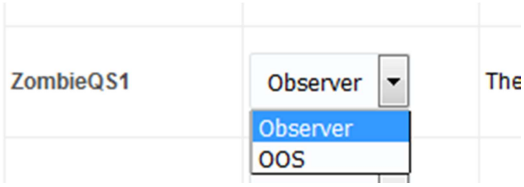
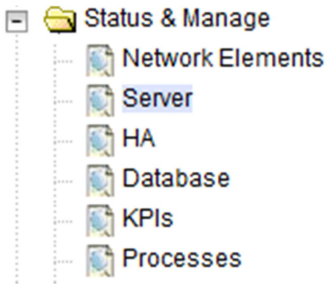
Procedure 1: Recovery Scenario 1

		$ 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*>
46. ☐	**NOAM VIP GUI:** Perform Keyexchange with Remote Import Server	**SDS Only, DSR Skip This Step** 1) Navigate to **Main Menu -> SDS -> Configuration -> Options**  2) Uncheck the **Remote Import Enabled Box**:  3) Click **Apply** **Note:** Re-navigate to **Main Menu -> SDS -> Configuration -> Options** to clear Success banner. 4) Re-Enter the **Remote Import Password**:  5) Click **Apply**  **Note:** Re-navigate to **Main Menu -> SDS -> Configuration -> Options** to clear Success banner. 6) Check the **Remote Import Enabled Box**:

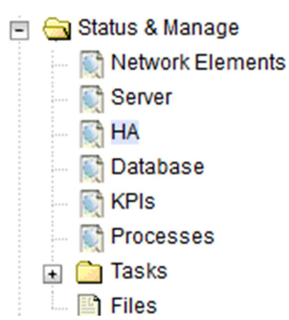
Procedure 1: Recovery Scenario 1

		
47. ☐	**NOAM VIP GUI:** Repeat for Remote Export Server	**SDS Only, DSR Skip This Step** Repeat **Step** 46 for the remote Export Server
48. ☐	**NOAM VIP GUI:** Perform Keyexchange with Export Server	Navigate to **Main Menu -> Administration -> Remote Servers -> Data Export**  Click on **SSH Key Exchange** at the bottom of the screen  Enter the Password and press **OK** 
49. ☐	**NOAM VIP GUI:** Recover Query Servers	**SDS Only, DSR Skip This Step** Execute procedure *"Configuring SDS Query Servers",* steps 1, 4-7 from reference [8]
50. ☐	**SDS NOAM VIP GUI:** Set HA on Query Server	**SDS Only, DSR Skip This Step** Navigate to **Status & Manage -> HA**

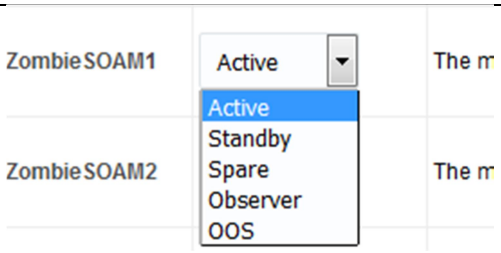
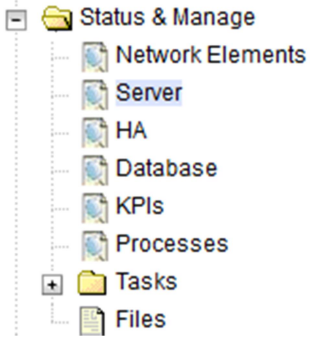
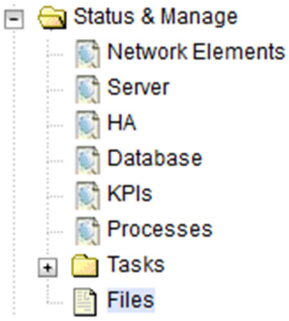
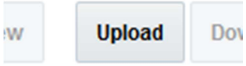
Procedure 1: Recovery Scenario 1

		 Click on **Edit** at the bottom of the screen Select the Query server, set it to **Observer**  Press **OK**
51. ☐	**SDS NOAM VIP GUI:** Restart SDS application	**SDS Only, DSR Skip This Step** Navigate to **Main Menu->Status & Manage->Server**  Select the recovered Query server and click on **Restart**. 
52. ☐	**NOAM VIP GUI:** Stop Replication to the C-Level Servers of this Site. (DSR Only)	**DSR Only, if SDS, Skip This Step** 

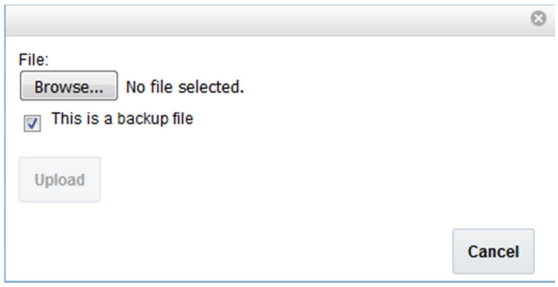
Procedure 1: Recovery Scenario 1

		!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Warning !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !! Prior to continuing this procedure, replication to C Level servers at the SOAM site being recovered ***MUST*** be inhibited. **Failure to inhibit replication to the working c-level servers will result in their database being destroyed!** Execute **Appendix C**. Inhibit A and B Level Replication on C-Level Servers to inhibit replication to working C Level servers before continuing.
53. ☐	**NOAM VIP GUI:** Recover Active SOAM Server	Install the SOAM servers **DSR:** Execute procedure *"Configure the SOAM Servers"*, steps 1-3, and 5-9 from reference [8] **Note:** If you are using NetBackup, also execute step 12 of procedure "*Configure the SOAM Servers"* from reference [8] **SDS:** Execute procedure *"Configure the SDS DP SOAM Servers"*, steps 1-3, and 5-8 from reference [8]
54. ☐	**NOAM VIP GUI:** Set HA on SOAM Server	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Select the SOAM server, set it to **Active**

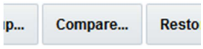
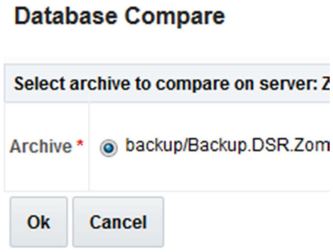
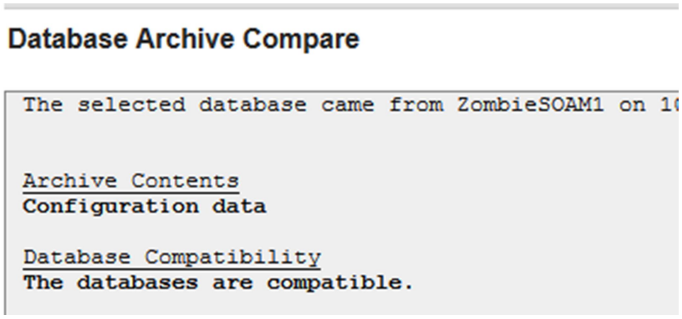
Procedure 1: Recovery Scenario 1

		 Press **OK**
55. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered SOAM server and click on **Restart**. 
56. ☐	**NOAM VIP GUI:** Upload the backed up SOAM Database file (DSR Only)	**DSR Only, if SDS, Skip This Step** Navigate to **Main Menu->Status & Manage->Files**  Select the Active SOAM server tab. The following screen will appear. Click on Upload as shown below and select the file *"SO Provisioning and Configuration:"* file backed up after initial installation and provisioning.  1. Click on **Browse** and locate the backup file

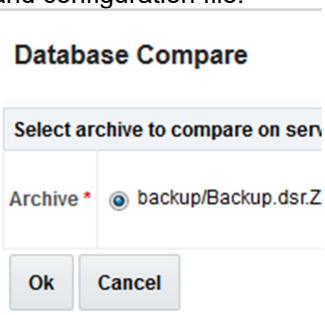
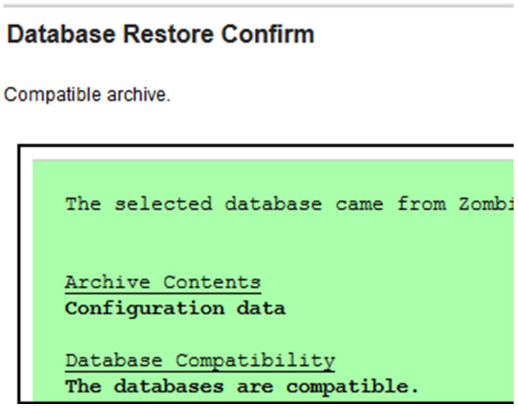
Procedure 1: Recovery Scenario 1

		2. Check **This is a backup file** Box 3. Click on Open as shown below.  Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.
57. ☐	**Recovered SOAM GUI:** Login (DSR Only)	**DSR Only, if SDS, Skip This Step** Establish a GUI session on the recovered SOAM server. Open the web browser and enter a URL of: `http://<Recovered_SOAM_IP_Address>` Login as the ***guiadmin*** user: 

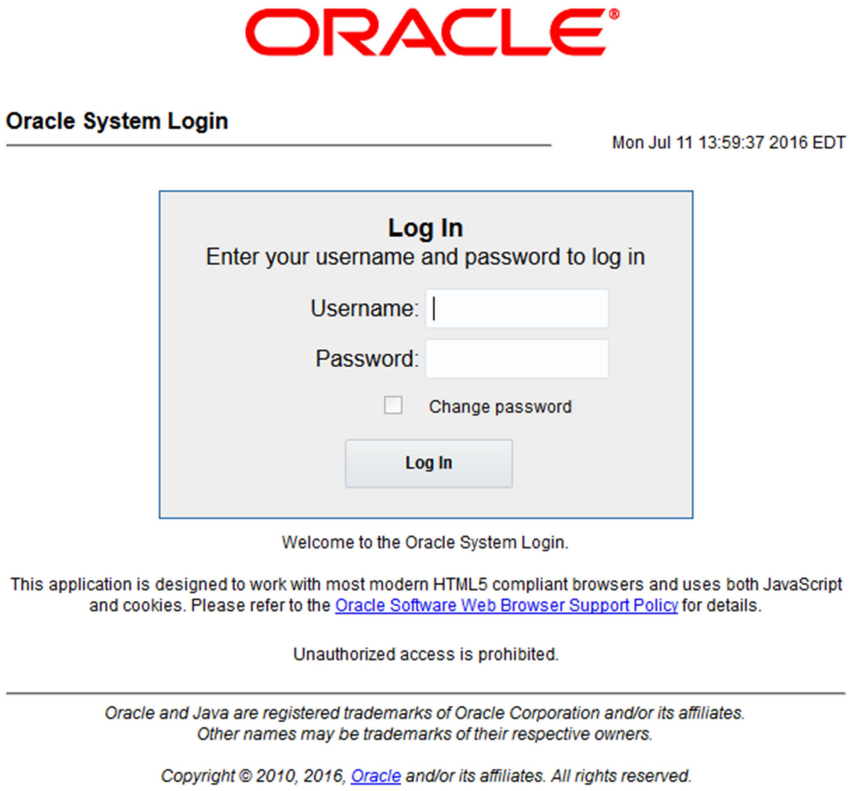
Procedure 1: Recovery Scenario 1

58. ☐	**Recovered SOAM GUI:** Verify the Archive Contents and Database Compatibility (DSR Only)	**DSR Only, if SDS, Skip This Step** Click on **Main Menu->Status & Manage->Database** Select the **Active SOAM** server and click on the **Compare**.  The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 56** of this procedure.  **Verify** that 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. If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.

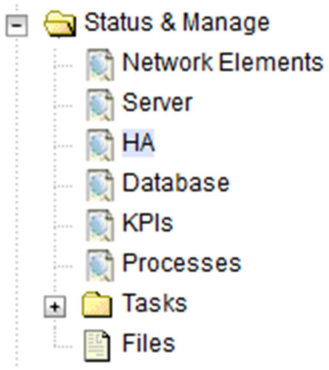
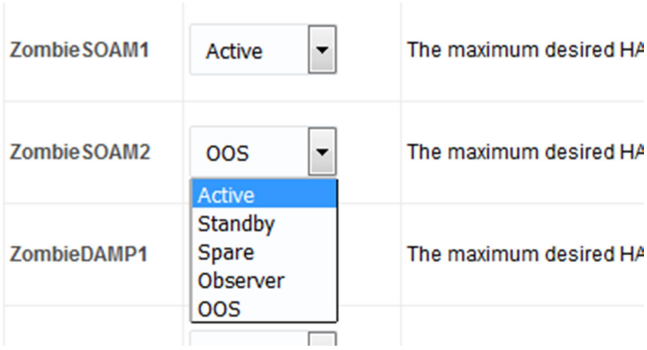
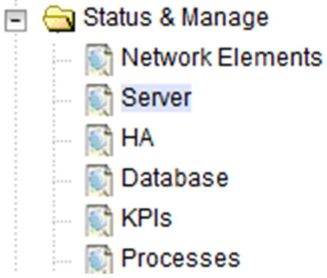
Procedure 1: Recovery Scenario 1

59. ☐	**Recovered SOAM GUI:** Restore the Database (DSR Only)	**DSR Only, if SDS, Skip This Step** Select the **Active SOAM** server, and click on **Restore** as shown below. The following screen will be displayed. Select the proper back up provisioning and configuration file.  Click **OK** Button. The following confirmation screen will be displayed. If you get an error for Node Type Compatibility, that is expected. If no other errors are displayed, select the **Force** checkbox as shown above and Click **OK** to proceed with the DB restore.  **Note:** After the restore has started, the user will be logged out of XMI SOAM GUI since the restored Topology is old data. **Note**: 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), kill the hung ping processes and the restore will proceed.
60. ☐	**Recovered SOAM GUI**: Monitor and Confirm database	**DSR Only, if SDS, Skip This Step** Wait for **5-10 minutes** for the System to stabilize with the new topology:

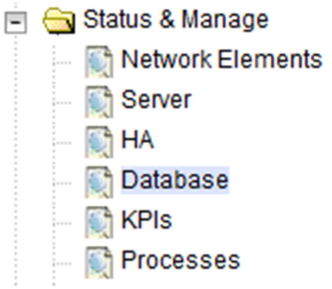
Procedure 1: Recovery Scenario 1

	restoral (DSR Only)	Monitor the Info tab for **"Success"**. This will indicate that the restore is complete and the system is stabilized. **Note:** Do not pay attention to alarms until all the servers in the system are completely restored. **Note:** The Configuration and Maintenance information will be in the same state it was backed up during initial backup.
61. ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 
62. ☐	**NOAM VIP GUI:** Recover the Remaining SOAM Servers	Recover the **remaining** SOAM servers (**Standby, Spare):** **DSR:** Execute procedure *"Configure the SOAM Servers"*, steps 1-3, and 5-9, from reference [8] **Note:** If you are using NetBackup, also execute step 12 of procedure "*Configure the SOAM Servers"* from reference [8]

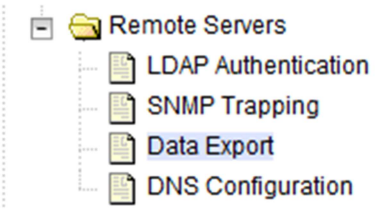
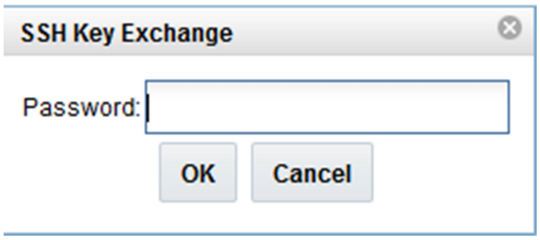
Procedure 1: Recovery Scenario 1

		SDS: Execute procedure *"Configure the SDS DP SOAM Servers"*, steps 1-3, and 5-8 from reference [8]
63. ☐	**NOAM VIP GUI:** Set HA on Remaining SOAMs	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen  Select the recovered SOAM server, set it to **Active** Press **OK**
64. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered standby SOAM server and click on **Restart**.

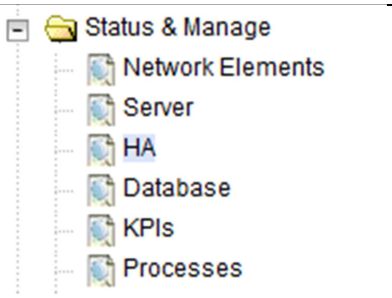
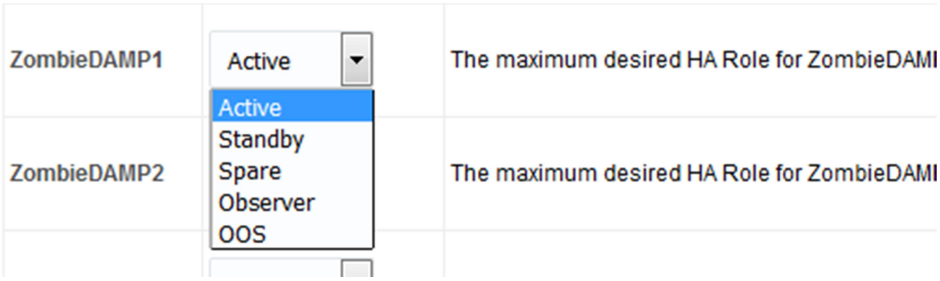
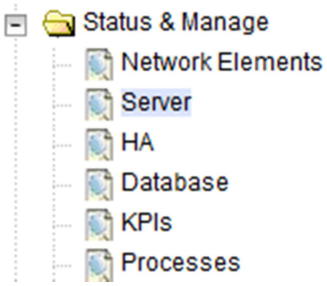
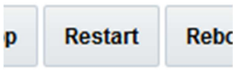
Procedure 1: Recovery Scenario 1

		p Restart Rebo
65. ☐	**NOAM VIP GUI:** Start Replication on Working C-Level Servers (DSR Only)	**DSR Only, if SDS, Skip This Step** Un-Inhibit *(Start)* Replication to the **working** C-Level Servers which belongs to the same site as of the failed SOAM servers. Execute **Appendix D**. Un-Inhibit A and B Level Replication on C-Level Servers Navigate to **Status & Manage -> Database**  If the *"Repl Status"* is set to "Inhibited", click on the **Allow Replication** button as shown below using the following order, 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/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/HP DL380 Gen 9 Only Verify that the replication on all the working servers is allowed. This can be done by examining the Repl Status table as seen below: OAM Repl Status / SIG Repl Status / Repl Status / Repl Audit Status NotApplicable / NotApplicable / Allowed / NotApplicable Normal / NotApplicable / Allowed / NotApplicable Normal / NotApplicable / Allowed / NotApplicable Normal / NotApplicable / Allowed / NotApplicable

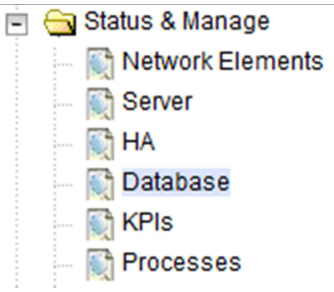
Procedure 1: Recovery Scenario 1

66. ☐	**SOAM VIP GUI:** Perform Keyexchange with Export Server	Navigate to **Main Menu -> Administration -> Remote Servers -> Data Export**  Click on **SSH Key Exchange** at the bottom of the screen Enter the Password and press **OK** 
67. ☐	**(DSR Only) Activate PCA Feature**	If you have PCA installed in the system being recovered, execute the procedure "PCA Activation on entire network" on recovered NOAM Server from [7] to re-activate PCA. **Note:** If not all SOAM sites are recovered at this point, then you should repeat activation for each *new* SOAM site that comes online.
68. ☐	**NOAM VIP GUI:** Recover the C-Level Server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs	Recover C-Level Servers: **DSR:** Execute procedure *"Configure the MP Servers"*, Steps 1, 9-13 from reference [8] **Note:** Execute steps 14-16 of procedure *"Configure the MP Servers"*, from reference [8] 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/HP DL380 Gen 9 Only):** Execute procedure *"Configure the SDS DP Servers"*, Steps 1, 5-8 from reference [8] Repeat this step for any remaining failed MP servers.
69. ☐	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**

Procedure 1: Recovery Scenario 1

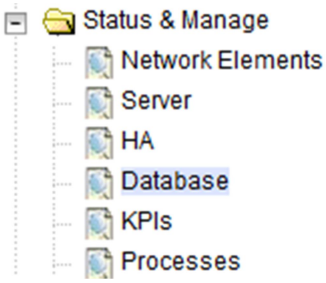
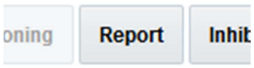
		 Click on **Edit** at the bottom of the screen For each recovered C-Level whose Max Allowed HA Role is set to OOS, set it to **Active**  Press **OK**
70. ☐	**NOAM VIP GUI:** Restart DSR Application on recovered C-Level Servers.	Navigate to **Main Menu->Status & Manage->Server**  Select the recovered C-Level servers and click on **Restart**. 
71. ☐	**NOAM VIP GUI:** Start replication on all C-Level Servers (DSR Only)	**DSR Only, SDS Skip This Step** Un-Inhibit *(Start)* Replication to the **ALL** C-Level Servers Navigate to **Status & Manage -> Database**

Procedure 1: Recovery Scenario 1

		 If the *"Repl Status"* is set to "Inhibited", click on the Allow Replication button as shown below using the following order: • Active NOAM Server • Standby NOAM Server • Active SOAM Server • Standby SOAM Server • Spare SOAM Server *(if applicable)-Oracle X5-2/Netra X5-2/X6-2/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/HP DL380 Gen 9 Only Verify that the replication on all the working servers is allowed. This can be done by examining the Repl Status table as seen below: **OAM Repl Status** | **SIG Repl Status** | **Repl Status** | **Repl Audit Status** NotApplicable | NotApplicable | Allowed | NotApplicable Normal | NotApplicable | Allowed | NotApplicable Normal | NotApplicable | Allowed | NotApplicable Normal | NotApplicable | Allowed | NotApplicable
72. ☐	**ACTIVE NOAM:** Perform key exchange between the active-NOAM and recovered servers.	Establish an SSH session to the Active NOAM, login as ***admusr.*** Execute the following command to perform a keyexchange from the active NOAM to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>`
73. ☐	**ACTIVE NOAM:** Activate Optional Features	**DSR Only, if SDS, Skip This Step** Establish an SSH session to the active NOAM, login as ***admusr.*** **Note For PCA Activation:** If you have PCA installed in the system being recovered, execute the

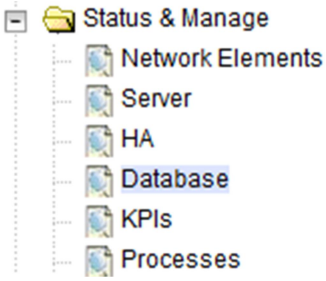
Procedure 1: Recovery Scenario 1

		procedure "*PCA Activation on entire server*" on recovered NOAM Server from [6] to re-activate PCA. **Note:** If not all SOAM sites are recovered at this point, then you should repeat activation for each *new* SOAM site that comes online. **Note**: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature. Refer to **Section** 1.5 Optional Features to activate any features that were previously activated.

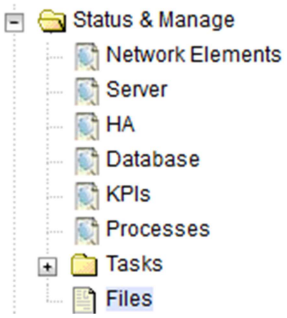
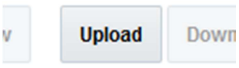
74. ☐	**NOAM VIP GUI:** Fetch and Store the database Report for the Newly Restored Data and Save it	Navigate to **Main Menu -> Status & Manage -> Database**
		
		 
		
		Select the **active** NOAM server and click on the **Report** button at the bottom of the page.
		
		 
		
		The following screen is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

Procedure 1: Recovery Scenario 1

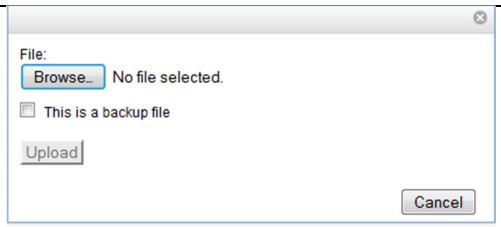
75. ☐	**ACTIVE NOAM:** Verify Replication Between Servers.	Login to the Active NOAM via SSH terminal as ***admusr***.
		
		Execute the following command:
		
		$ sudo irepstat –m
		
		Output like below shall be generated:
		
		`-- Policy 0 ActStb [DbReplication] ----------`
		`Oahu-DAMP-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.15%cpu 25B/s  A=me`
		`  CC To  Oahu-DAMP-2  Active  0  0.10  0.14%cpu 25B/s  A=me`
		`Oahu-DAMP-2 -- Stby`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.11%cpu 31B/s A=C3642.212`
		`  CC From Oahu-DAMP-1  Active  0  0.10 ^0.14 1.16%cpu 31B/s A=C3642.212`
		`Oahu-IPFE-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 24B/s A=C3642.212`
		`Oahu-IPFE-2 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 28B/s A=C3642.212`
		`Oahu-NOAM-1 -- Stby`
		`  AA From Oahu-NOAM-2  Active  0  0.25 ^0.03%cpu 23B/s`
		`Oahu-NOAM-2 -- Active`
		`  AA To  Oahu-NOAM-1  Active  0  0.25 1%R 0.04%cpu 61B/s`
		`  AB To  Oahu-SOAM-2  Active  0  0.50 1%R 0.05%cpu 75B/s`
		`Oahu-SOAM-1 -- Stby`
		`  BB From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 27B/s`
		`Oahu-SOAM-2 -- Active`
		`  AB From Oahu-NOAM-2  Active  0  0.50 ^0.03%cpu 24B/s`
		`  BB To  Oahu-SOAM-1  Active  0  0.50 1%R 0.04%cpu 32B/s`
		`  BC To  Oahu-IPFE-1  Active  0  0.50 1%R 0.04%cpu 21B/s`
		`  BC To  Oahu-SS7MP-2 Active  0  0.50 1%R 0.04%cpu 21B/s`
		`irepstat ( 40 lines) (h)elp (m)erged`

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

Procedure 1: Recovery Scenario 1

		status is “Normal” as shown below: **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
77. ☐	**NOAM VIP GUI:** Upload the backed up RADIUS Key file (RADIUS Only)	**DSR Only, if SDS, Skip This 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)** Navigate to **Main Menu->Status & Manage->Files**  Select the Active NOAM server tab. The following screen will appear. Click on Upload as shown below and select the file *“RADIUS shared secret encryption key:”* file backed up after initial installation and provisioning or after key revocation execution.  Click on Browse and Locate the DpiKf.bin.encr file and click on Open as shown below.

Procedure 1: Recovery Scenario 1

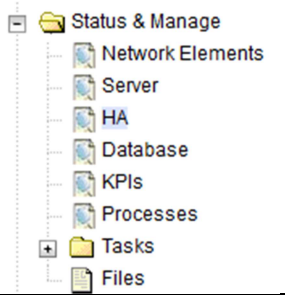
		 Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the file. The file will be visible on the list of entries after the upload is complete. **Note:** This file should be deleted from the operator's local servers as soon as key file is uploaded to Active NOAM server.

78. ☐	**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)**
		
		Login to the Active NOAM VIP via SSH terminal as ***admusr*** user.
		
		Execute the following commands to copy the key file:
		
		`$ cd /usr/TKLC/dpi/bin`
		
		`$ ./sharedKrevo -decr`
		
		`$ sudo rm /var/TKLC/db/filemgmt/<backed up key file name>`
		
		Execute following command to check if all the servers in 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.`

Procedure 1: Recovery Scenario 1

		Note: If all the servers are not accessible, contact Appendix K. My Oracle Support (MOS)

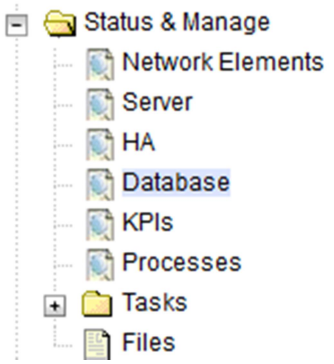
79. ☐	**NOAM VIP:** Copy and distribute RADIUS Key file on Active NOAM (RADIUS Only)- Part 2	**If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)**
		
		Execute following command to distribute key file to all the servers in the topology :
		
		`$ ./sharedKrevo -synchronize`
		
		`$ ./sharedKrevo -updateData`
		
		Example output:
		
		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]$
		
		Note: For any errors contact Appendix K. My Oracle Support (MOS)

80. ☐	**NOAM VIP GUI:** Verify the HA Status	Click on **Main Menu->Status and Manage->HA** 

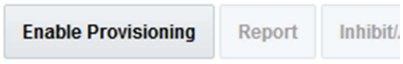
Procedure 1: Recovery Scenario 1

<table>
<tr><td></td><td></td><td>Select the row for all of the servers
Verify that the “HA Role” is either “Active” or “Standby”.

<table><tr><th>Hostname</th><th>OAM HA Role</th><th>Application HA Role</th><th>Max Allowed HA Role</th></tr><tr><td>ZombieNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieDRNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieDRNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieSOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieSOAM2</td><td>Standby</td><td>N/A</td><td>Standby</td></tr></table></td></tr>
<tr><td>81.
☐</td><td>NOAM GUI:
Enable Provisioning</td><td>Click on Main Menu->Status & Manage->Database

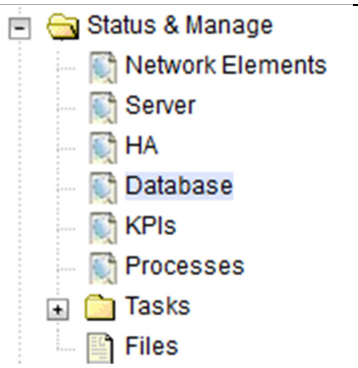
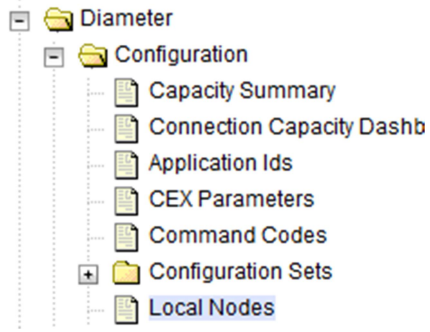
Enable Provisioning by clicking on Enable Provisioning button at the bottom of the screen as shown below.

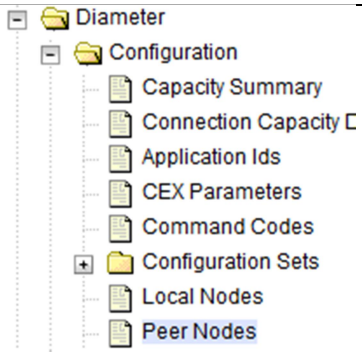
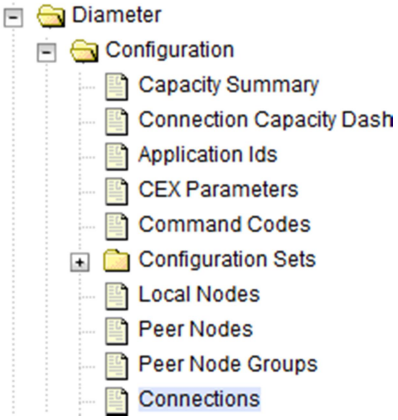
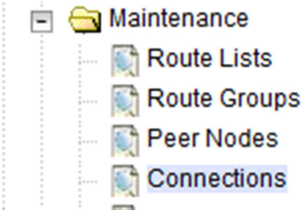
A confirmation window will appear, press OK to enable Provisioning.</td></tr>
<tr><td>82.
☐</td><td>SOAM GUI:
Enable Provisioning</td><td>DSR Only, if SDS, Skip This Step

Click on Main Menu->Status & Manage->Database</td></tr>
</table>

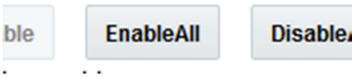
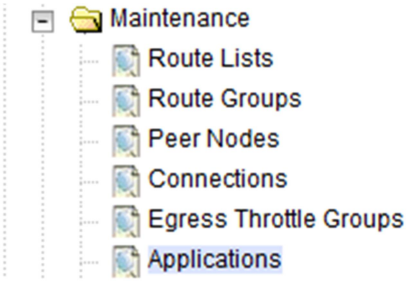
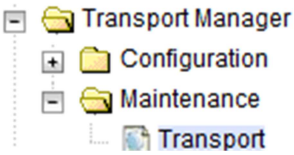
Procedure 1: Recovery Scenario 1

		 Enable Provisioning by clicking on **Enable Site Provisioning** button at the bottom of the screen as shown below.  A confirmation window will appear, press **OK** to enable Provisioning.
83. ☐	**SOAM VIP GUI:** Verify the Local Node Info (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Configuration->Local Node**  Verify that all the local nodes are shown.
84. ☐	**SOAM VIP GUI:** Verify the Peer Node Info (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Configuration->Peer Node**

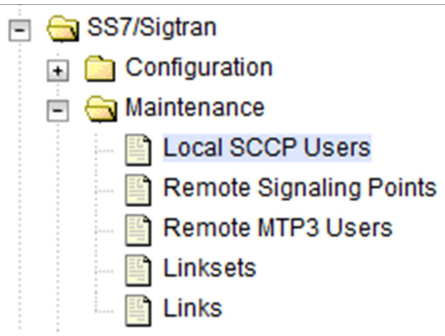
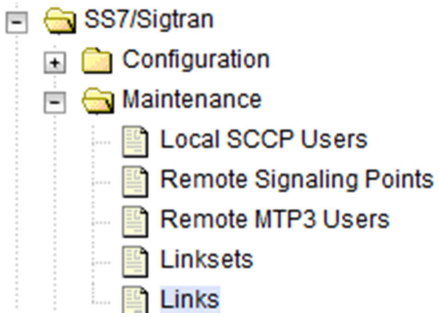
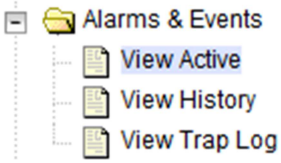
Procedure 1: Recovery Scenario 1

		 Verify that all the peer nodes are shown.
85. ☐	**SOAM VIP GUI:** Verify the Connections Info (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Configuration->Connections**  Verify that all the connections are shown.
86. ☐	**MP Servers:** Disable SCTP Auth Flag (DSR Only)	**DSR Only, SDS Skip This Step** For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [12] Execute this procedure on all Failed MP Servers.
87. ☐	**SOAM VIP GUI:** Enable Connections if needed (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Maintenance->Connections**  Select each connection and click on the **Enable** button. Alternatively you can

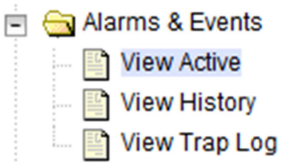
Procedure 1: Recovery Scenario 1

		enable all the connections by selecting the **EnableAll** button.  Verify that the Operational State is Available. **Note:** If a Disaster Recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution
88. ☐	**SOAM VIP GUI:** Enable Optional Features (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Select the optional feature application configured in **step 73** Click the **Enable** button. 
89. ☐	**SOAM VIP GUI:** Re-enable Transports if Needed (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Transport Manager -> Maintenance -> Transport**  Select each transport and click on the **Enable** button  Verify that the Operational Status for each transport is Up.
90. ☐	**SOAM VIP GUI:** Re-enable MAPIWF application if	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users**

Procedure 1: Recovery Scenario 1

	needed(DSR Only)	 Click on the **Enable** button corresponding to MAPIWF Application Name.  Verify that the SSN Status is Enabled.
91. ☐	**SOAM VIP GUI:** Re-enable links if needed (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->SS7/Sigtran->Maintenance->Links**  Click on **Enable** button for each link.  Verify that the Operational Status for each link is Up.
92. ☐	**SOAM VIP GUI:** Examine All Alarms	Navigate to **Main Menu->Alarms & Events->View Active**  Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix K.** My Oracle Support (MOS).

Procedure 1: Recovery Scenario 1

93. ☐	**NOAM VIP GUI:** Examine All Alarms	Login to the NOAM VIP if not already logged in. Navigate to **Main Menu->Alarms & Events->View Active**  Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix K.** My Oracle Support (MOS).
94. ☐	**Restore GUI Usernames and Passwords**	If applicable, Execute steps in **Section 6.0** to recover the user and group information restored.
95. ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**. Database Backup to back up the Configuration databases:
96. ☐	**Recover IDIH** (If Configured)	If any components of IDIH were affected, refer to **Section 7.0** to perform the disaster recovery on IDIH.
97. ☐	**SNMP Workaround**	Refer to Appendix H. SNMP Configuration to configure SNMP as a workaround in the following cases: 1) If SNMP is not configured in DSR/SDS 2) If SNMP is already configured and **SNMPv3** is selected as enabled version

5.1.2 Recovery Scenario 2 (Partial Server Outage with at least 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. The actual procedures' 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.

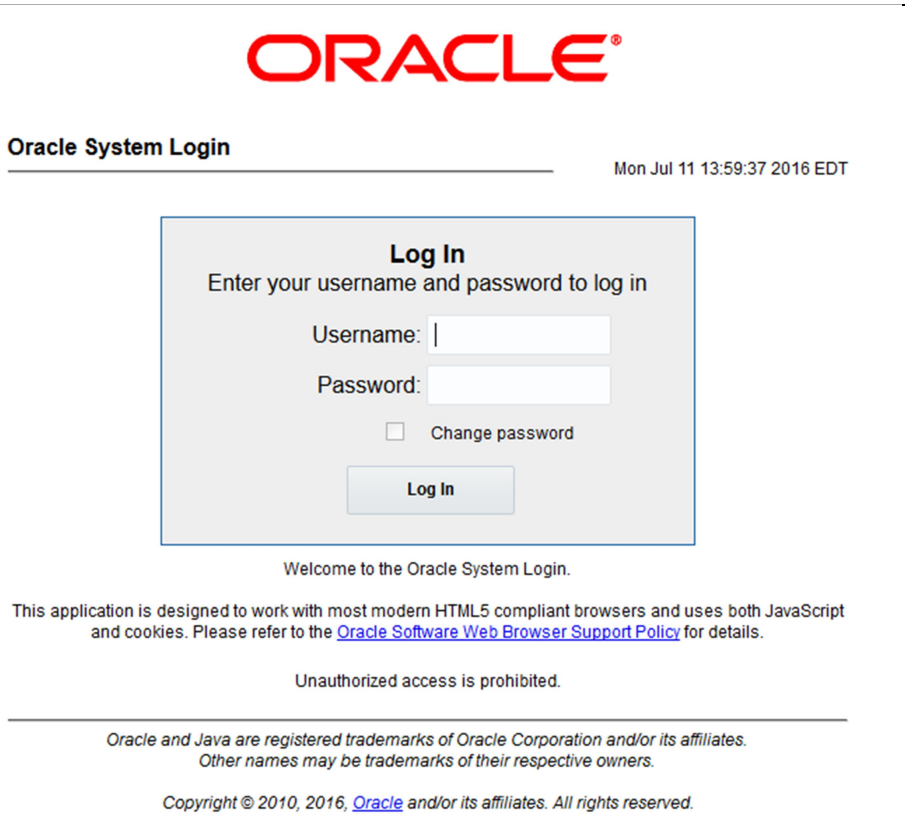
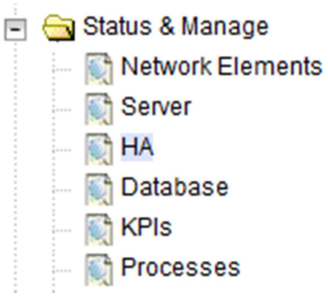
- Recover the base hardware.
- Recover the software.
- The database has already been restored at the active SOAM server and does not require restoration at the SO and MP/DP servers.

Recover IDIH if necessary

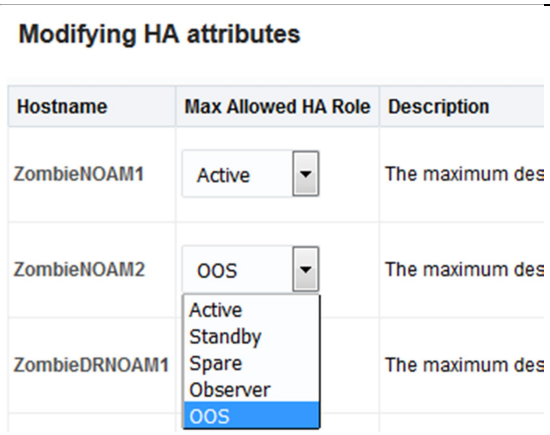
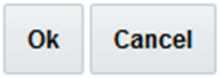
Procedure 2: Recovery Scenario 2

S T E P #	This procedure performs recovery if at least 1 NOAM server is available but all SOAM servers in a site have failed. This includes any SOAM server that is in another location. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Workarounds**	Refer to **Appendix G**. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure. Refer to **Appendix H**. SNMP Configuration to configure SNMP as a workaround in the following cases: 1) If SNMP is not configured in DSR/SDS 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 **Section 3.1** Required Materials**.**
3. ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:

Procedure 2: Recovery Scenario 2

		
4. ☐	**Active NOAM:** Set Failed Servers to OOS	Navigate to **Main Menu -> Status & Manage -> HA**  Select **Edit**

Procedure 2: Recovery Scenario 2

		 Set the Max Allowed HA Role drop down box to **OOS** for the failed servers. Select **Ok** 
5. ☐	**Replace Failed Equipment**	HW vendor to replace the failed equipment
6. ☐	**Recover PMAC TVOE Host (If Required):** 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:** *"Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings"* • **HP DL380 Gen9:** *"Configure HP Gen9 Server BIOS Settings"* 2. Verify and/or upgrade server firmware by executing procedure *"Upgrade Rack Mount Server Firmware"* from reference [8]
7. ☐	**Recover PMAC and PMAC TVOE Host:** Backup Available	**If the PMAC is located on the failed rack mount server(s), execute this step. Otherwise skip to step 10.** This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, **skip this step**. 1. Restore the TVOE backup by executing **Appendix E**. Restore TVOE Configuration from Backup Media on **ALL** failed rack mount servers 2. Restore the PMAC backup by executing **Appendix F**. Restore PMAC from Backup **Proceed to Step 10**

Procedure 2: Recovery Scenario 2

8. ☐	**Recover PMAC and PMAC TVOE Host:** Backup Not Available	**If the PMAC is located on the failed rack mount server(s), execute this step. Otherwise skip to step 10.** This step assumes that TVOE and PMAC backups are NOT available, if the TVOE and PMAC have already been restored, **skip this step** 1. Execute procedure *"Install and Configure TVOE on First RMS (PMAC Host)"* from reference [8] 2. Execute section *"Install PMAC"* from reference [8] 3. Execute section *"Initialize the PMAC Application"* from reference [8] **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 sections *"Configure PMAC Server (NetBackup Only)"* and *"Add RMS to the PMAC Inventory"* from reference [8]
10. ☐	**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 procedure *"Install TVOE on Additional Rack Mount Servers"* from reference [8] 2. Execute *"Configure TVOE on Additional Rack Mount Servers"* from reference [8] 3. 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:"***Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings"* • **HP DL380 Gen9:** *"Configure HP Gen9 Server BIOS Settings"*
11. ☐	**Determine VM Placement and Socket Pinning** (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only)	**HP DL380 GEN 8 SKIP THIS STEP** Refer to the DSR VM placement and Pinning workbook to determine proper VM placement and pinning.
12. ☐	**Deploy Redundant PMAC**	**If the redundant PMAC is located on the failed rack mount server(s), execute this step. Otherwise skip to next step.** Refer to procedure *"Deploy Redundant PMAC (Optional)"* to re-deploy and configure any redundant PMACs previously configured.
13. ☐	**PMAC: Determine if an fdconfig file exists from the**	Determine whether the fdconfig backup file exists: [admusr@melbourne-pmac-1 ~]$ ll /usr/TKLC/smac/etc/fdc/

Procedure 2: Recovery Scenario 2

	initial deployment.	Examine the results and verify whether the rms config file <hostname>.cfg exists **Note**: There may be multiple fdconfig backup files here with respect to each RMS. Select the respective one according to the RMS.
14. ☐	**If FDCONFIG backup file does NOT exist:**	**Execute this step ONLY If the fdconfig backup file does NOT exist:** If the fdconfig file does NOT exist : Create the needed file(s) by executing section "Virtual Machine/Network Fast Deployment" from reference [8] **WARNING:** It is very important to ensure the file(s) created only affect the TVOE server(s) and its 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 [If fdc backup file exists]: Load ISOs into PMAC if not done already**	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:** If the DSR, SDS, and TPD ISOs are NOT loaded in to the PMAC: Execute procedures 14 of section "Virtual Machine/Network Fast Deployment" from reference [8] If already loaded into PMAC, skip this step.
16. ☐	**PMAC [If fdc backup file exists]:** Edit/Update Configuration File	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:** **Edit the fdconfig file to include only the required/failed servers.** **Note:** Comment out configuration items that are not needed. **Note:** It is recommended that a separate configuration file be created for **EACH** rack mount server being deployed. Note:Cabinet ID in the config file needs to match the cabinet already defined in PM&C" 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)

Procedure 2: Recovery Scenario 2

		• 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) **Note:** Refer to **Appendix R: VM Automation Profile Values** for DSR and SDS profile values with the configuration file from reference [8] Note: Comment out SDS and DSR profile items if corresponding products are not used. **Note: [Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/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] **Note:** The VM names should not be modified in the .cfg file. The names are fixed and will be prefixed in the siteName. **Note:** The VM locations should not be changed from their 'RMSx' format. Each RMS should correspond with a separate Rack Mount Server. **WARNING**: It is very important to ensure the file(s) created only affect the TVOE server(s) and its 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** **[If fdc backup file exists]:** Copy the located backedup fdc file to the RMS directory	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:** Copy the located fdconfig backup file to the RMS directory: `$ cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file> /usr/TKLC/smac/etc/RMS/`
18. ☐	**PMAC** **[If fdc backup file exists]:** Execute the config.sh script	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:**

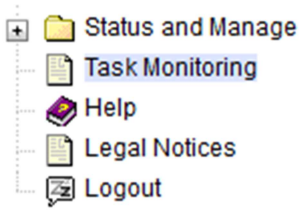
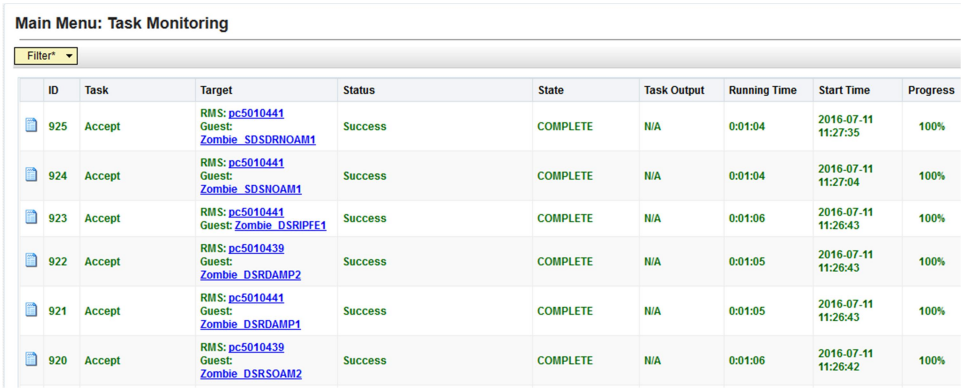
Procedure 2: Recovery Scenario 2

		Execute config.sh against the modified back up config file defined above:
		Note: If the below command is executed on multiple cfg files, it will overwrite the existing xml file. It is recommended to rename the xml file before running the below command again.
		$ sudo ./config.sh <config file>
		Sample 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]$`

19. ☐	**PMAC [If fdc backup file exists]:**	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:**

Procedure 2: Recovery Scenario 2

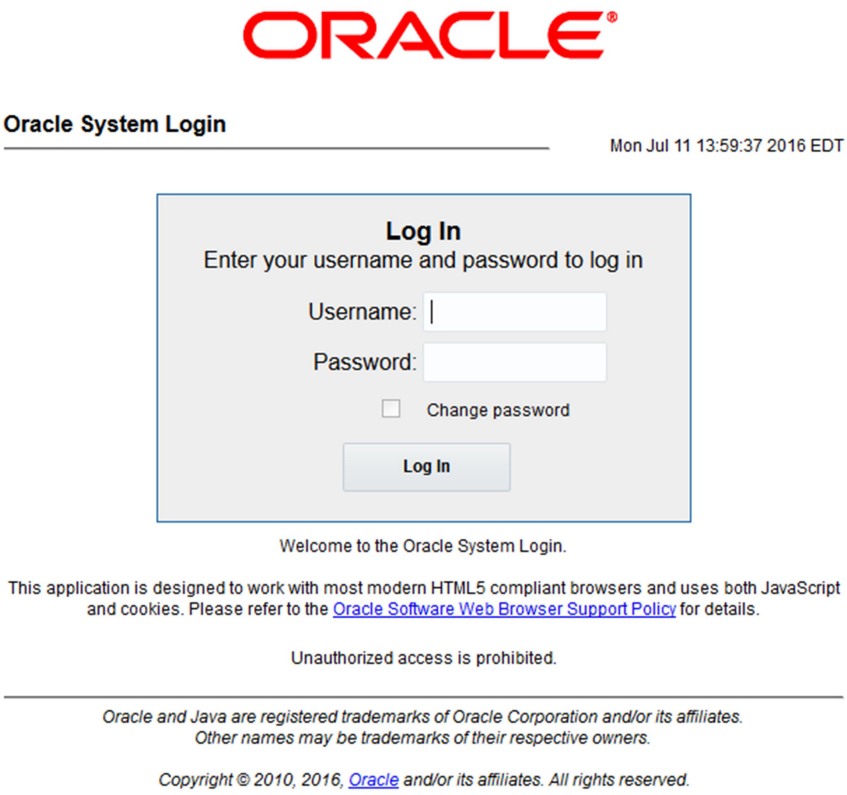
	Execute Fast Deployment	With the file generated from the config.sh script, execute the following command to start fast deployment:
		
		`$ screen`
		
		`$ sudo fdconfig config --file=<fd_config.xml>`
		
		Note: This is a long duration command. If the screen command was run prior to executing the fdconfig, perform a *"screen -dr"* to resume the screen session in the event of a terminal timeout etc.

20. ☐	**PMAC GUI [If fdc backup file exists]:** Monitor the Configuration	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:** If not already done so, establish a GUI session on the PMAC server. Navigate to **Main Menu -> Task Monitoring**  Monitor the configuration to completion:  ID / Task / Target / Status / State / Task Output / Running Time / Start Time / Progress 925 / Accept / RMS: pc5010441 Guest: Zombie_SDSDRNOAM1 / Success / COMPLETE / N/A / 0:01:04 / 2016-07-11 11:27:35 / 100% 924 / Accept / RMS: pc5010441 Guest: Zombie_SDSNOAM1 / Success / COMPLETE / N/A / 0:01:04 / 2016-07-11 11:27:04 / 100% 923 / Accept / RMS: pc5010441 Guest: Zombie_DSRIPFE1 / Success / COMPLETE / N/A / 0:01:06 / 2016-07-11 11:26:43 / 100% 922 / Accept / RMS: pc5010439 Guest: Zombie_DSRDAMP2 / Success / COMPLETE / N/A / 0:01:05 / 2016-07-11 11:26:43 / 100% 921 / Accept / RMS: pc5010441 Guest: Zombie_DSRDAMP1 / Success / COMPLETE / N/A / 0:01:05 / 2016-07-11 11:26:43 / 100% 920 / Accept / RMS: pc5010439 Guest: Zombie_DSRSOAM2 / Success / COMPLETE / N/A / 0:01:06 / 2016-07-11 11:26:42 / 100% **Note:** Should a failure occur with fdconfig, logs can be accessed in /var/TKLC/log/fdconfig/fdconfig.log [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 ----------

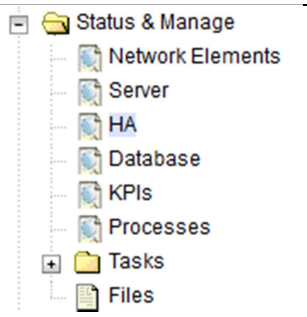
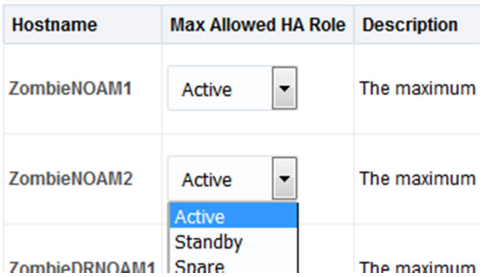
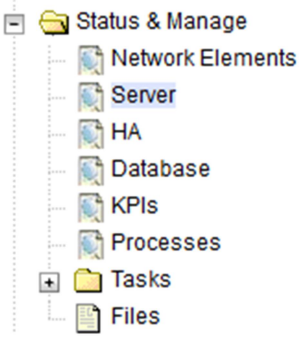
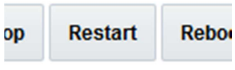
Procedure 2: Recovery Scenario 2

		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 Run Below command to restart the fdconfig after a failure has occurred and has been resolved: $ sudo fdconfig restart --file=deploy_melbourne_20170329T202458_701b.fdcdb
21. ☐	**PMAC [If fdc backup file exists]:** Repeat for each Rack mount server configuration file	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:** Repeat **steps 13-20** for each rack mount server/configuration file located at step 13, if required.
22. ☐	**PMAC [If fdc backup file exists]:** Backup FDC file	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:** Create the fdc directory so that the fdc file is backed up by PMAC: Issue the following commands: Copy the updated fdc file to the fdc backup directory: **$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> /usr/TKLC/smac/etc/fdc/** 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 procedure *"CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only)"* from reference [8]
24. ☐	**NOAM VIP GUI:** Login	**If the failed server(s) are NOT OAM type, skip to step 49** Establish a GUI session on the NOAM server by using the VIP IP address of the

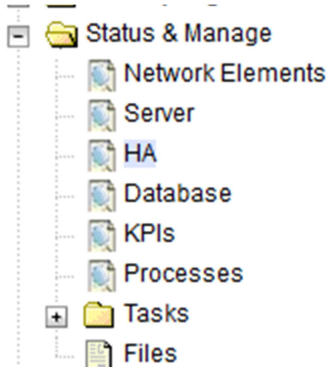
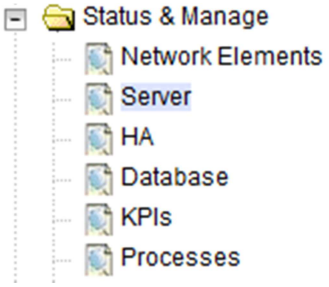
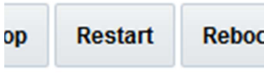
Procedure 2: Recovery Scenario 2

		NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 
25. ☐	**NOAM VIP GUI:** Recover Standby NOAM (if needed)	Install the second NOAM server if needed: **DSR:** Execute procedure *"Configure the Second NOAM Server",* steps 1, 3-6 from reference [8] **SDS:** Execute procedure *"Configure the Second SDS NOAM Server",* steps 1, 3-6 from reference [8]
26. ☐	**Install NetBackup Client (Optional)**	If NetBackup is used execute procedure *"Install NetBackup Client (Optional)"* from reference [8]
27. ☐	**NOAM VIP GUI:** Set HA on Standby NOAM	Navigate to **Status & Manage -> HA**

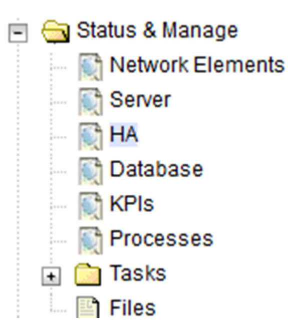
Procedure 2: Recovery Scenario 2

		 Click on **Edit** at the bottom of the screen Select the standby NOAM server, set it to **Active** **Modifying HA attributes**  Press **OK**
28. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered standby NOAM server and click on **Restart.** 
29. ☐	**NOAM VIP GUI:** Recover Query Servers	**SDS Only, DSR Skip This Step** Execute procedure *"Configuring SDS Query Servers",* steps 1, 4-7 from reference [8] if recovering query servers.

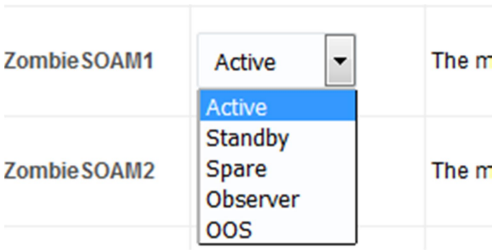
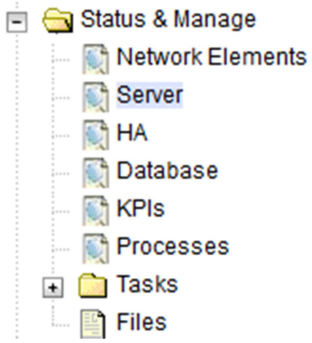
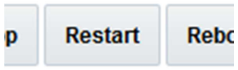
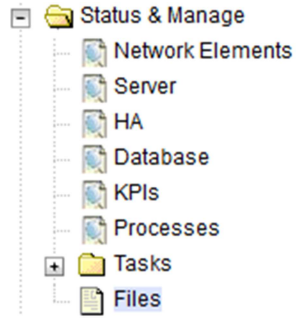
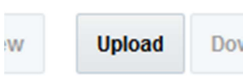
Procedure 2: Recovery Scenario 2

30. ☐	**SDS NOAM VIP GUI:** Set HA on Query Server	**SDS Only, DSR Skip This Step** Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Select the Query server, set it to **Observer**  Press **OK**
31. ☐	**SDS NOAM VIP GUI:** Restart SDS application	**SDS Only, DSR Skip This Step** Navigate to **Main Menu->Status & Manage->Server**  Select the recovered Query server and click on **Restart**. 
32. ☐	**NOAM VIP GUI:** Stop Replication to the C-Level Servers of this	**DSR Only, if SDS, Skip This Step**

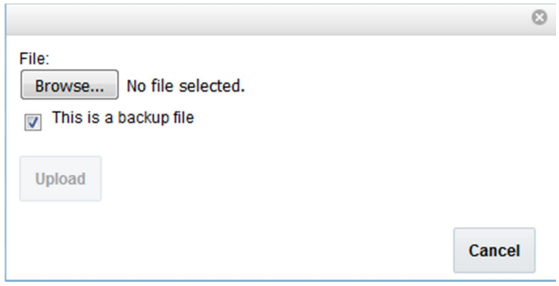
Procedure 2: Recovery Scenario 2

	Site. (DSR Only)	 **_!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Warning !!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!_** Prior to continuing this procedure, replication to C Level servers at the SOAM site being recovered ***MUST*** be inhibited. **Failure to inhibit replication to the working c-level servers will result in their database being destroyed!** Execute **Appendix C**. Inhibit A and B Level Replication on C-Level Servers to inhibit replication to working C Level servers before continuing.
33. ☐	**NOAM VIP GUI:** Recover Active SOAM Server	Install the SOAM servers **DSR:** Execute procedure *“Configure the SOAM Servers”*, steps 1-3, and 5-9 from reference [8] **Note:** If you are using NetBackup, also execute step 12 of procedure *“Configure the SOAM Servers”* from reference [8] **SDS:** Execute procedure *“Configure the SDS DP SOAM Servers”*, steps 1-3, and 5-8 from reference [8]
34. ☐	**NOAM VIP GUI:** Set HA on SOAM Server	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Select the SOAM server, set it to **Active**

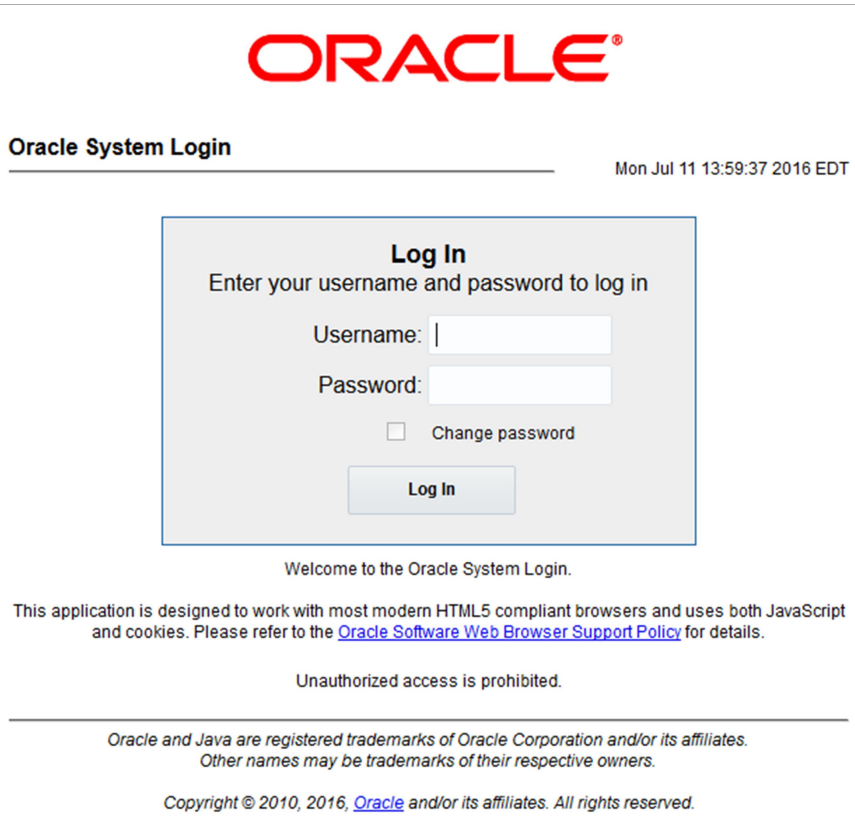
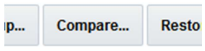
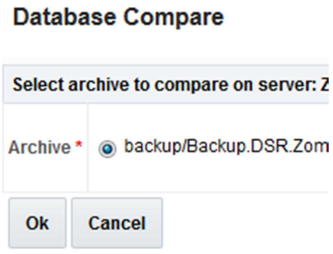
Procedure 2: Recovery Scenario 2

		 Press **OK**
35. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered SOAM server and click on **Restart**. 
36. ☐	**NOAM VIP GUI:** Upload the backed up SOAM Database file (DSR Only)	**DSR Only, if SDS, Skip This Step** Navigate to **Main Menu->Status & Manage->Files**  Select the Active SOAM server tab. The following screen will appear. Click on Upload as shown below and select the file *"SO Provisioning and Configuration:"* file backed up after initial installation and provisioning. 

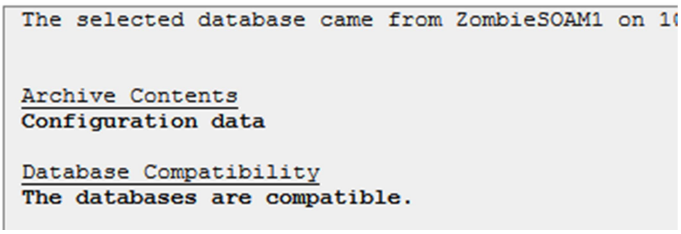
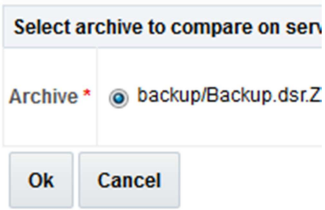
Procedure 2: Recovery Scenario 2

		1. Click on **Browse** and locate the backup file 2. Check **This is a backup file** Box 3. Click on Open as shown below.  Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.
37. ☐	**Recovered SOAM GUI:** Login (DSR Only)	**DSR Only, SDS Skip This Step** Establish a GUI session on the recovered SOAM server. Open the web browser and enter a URL of: `http://<Recovered_SOAM_IP_Address>` Login as the ***guiadmin*** user:

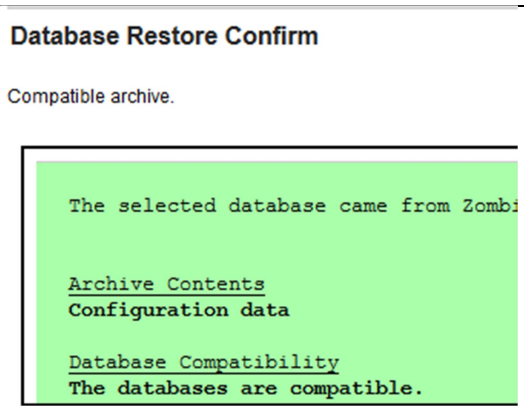
Procedure 2: Recovery Scenario 2

		
38. ☐	**Recovered SOAM GUI:** Verify the Archive Contents and Database Compatibility (DSR Only)	**DSR Only, if SDS, Skip This Step** Click on **Main Menu->Status & Manage->Database** Select the **Active SOAM** server and click on the **Compare**.  The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 36,** of this procedure.  **Verify** that the output window matches the screen below.

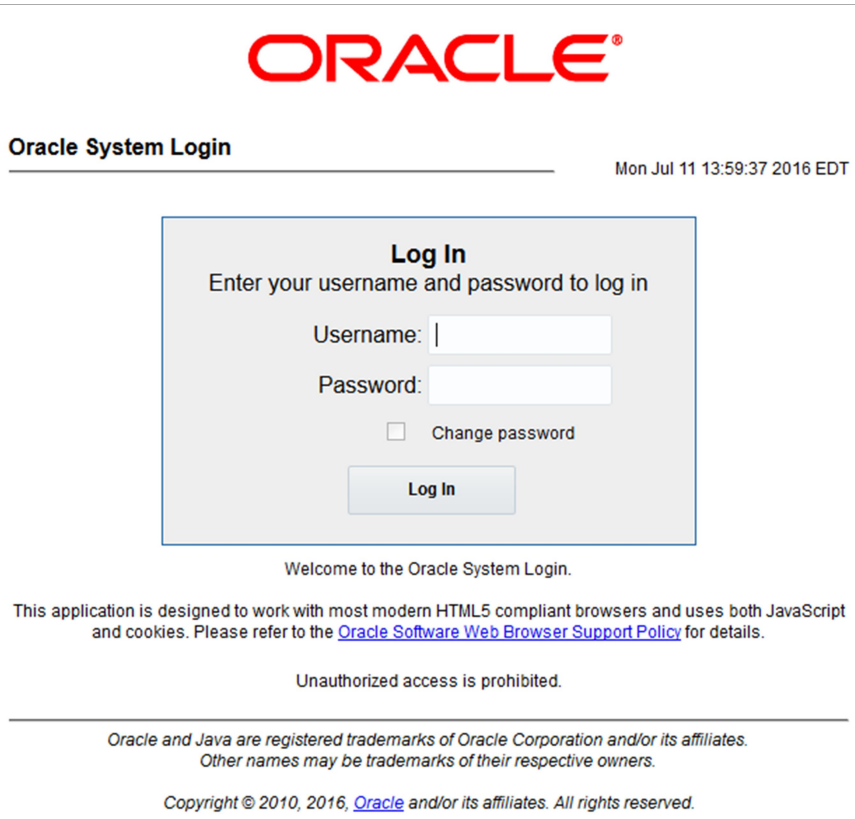
Procedure 2: Recovery Scenario 2

		Database Archive Compare  The selected database came from ZombieSOAM1 on 1(Archive Contents Configuration data Database Compatibility The databases are compatible. **Note:** Archive Contents and Database Compatibilities must be the following: **Archive Contents:** Configuration data **Database Compatibility:** The databases are compatible. **Note:** The following is expected Output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. **Note:** We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility. If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.
39. ☐	**Recovered SOAM GUI:** Restore the Database (DSR Only)	**DSR Only, if SDS, Skip This Step** Select the **Active SOAM** server, and click on **Restore** as shown below. The following screen will be displayed. Select the proper back up provisioning and configuration file. **Database Compare**  Select archive to compare on serv Archive * backup/Backup.dsr.Z Ok Cancel Click **OK** Button. The following confirmation screen will be displayed. If you get an error for Node Type Compatibility, that is expected. If no other errors are displayed, select the **Force** checkbox as shown above and Click **OK** to proceed with the DB restore.

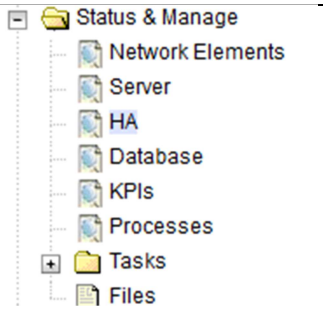
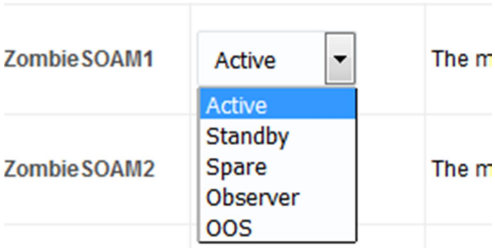
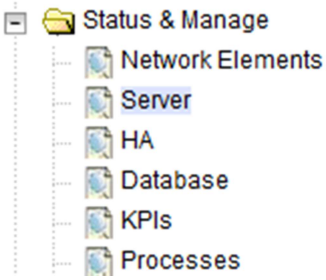
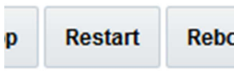
Procedure 2: Recovery Scenario 2

		 **Note:** After the restore has started, the user will be logged out of XMI SOAM GUI since the restored Topology is old data. **Note**: 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), kill the hung ping processes and the restore will proceed.
40. ☐	**Recovered SOAM GUI**: Monitor and Confirm database restoral (DSR Only)	**DSR Only, if SDS, Skip This Step** Wait for **5-10 minutes** for the System to stabilize with the new topology: Monitor the Info tab for **"Success"**. This will indicate that the restore is complete and the system is stabilized. **Note:** Do not pay attention to alarms until all the servers in the system are completely restored. **Note:** The Configuration and Maintenance information will be in the same state it was backed up during initial backup.
41. ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:

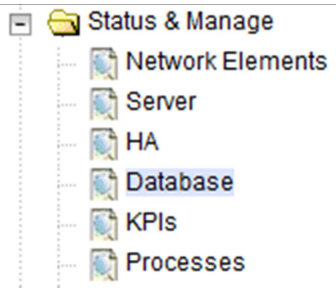
Procedure 2: Recovery Scenario 2

		
42. ☐	**NOAM VIP GUI:** Recover the Remaining SOAM Servers	Recover the **remaining** SOAM servers (**Standby, Spare**): **DSR:** Execute procedure *"Configure the SOAM Servers"*, steps 1-3, and 5-9, from reference [8] **Note:** If you are using NetBackup, also execute step 12 of procedure *"Configure the SOAM Servers"* from reference [8] . **SDS:** Execute procedure *"Configure the SDS DP SOAM Servers"*, steps 1-3, and 5-8 from reference [8]
43. ☐	**NOAM VIP GUI:** Set HA on Recovered standby SOAM Server	Navigate to **Status & Manage -> HA**

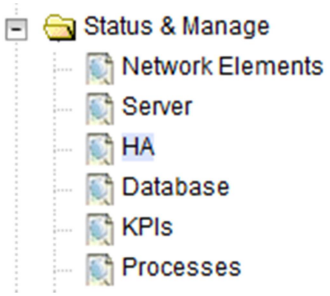
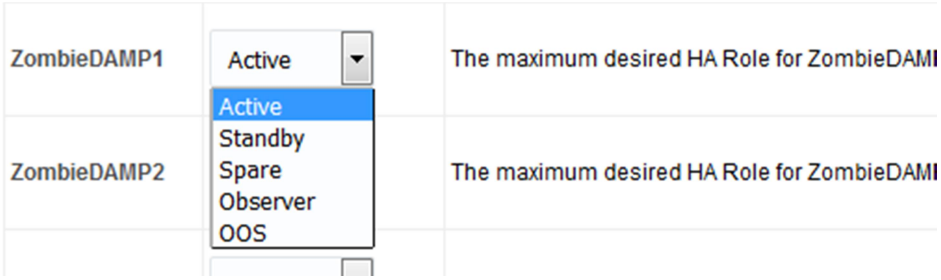
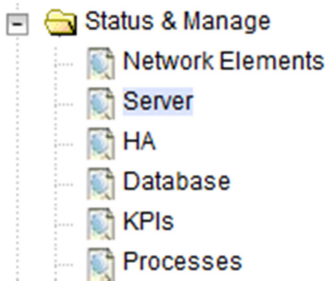
Procedure 2: Recovery Scenario 2

		 Click on **Edit** at the bottom of the screen Select the recovered standby SOAM server, set it to **Active**  Press **OK**
44. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered standby SOAM server and click on **Restart**. 
45. ☐	**NOAM VIP GUI:** Start Replication on Working C-Level Servers (DSR Only)	**DSR Only, if SDS, Skip This Step** Un-Inhibit *(Start)* Replication to the **working** C-Level Servers which belongs to the same site as of the failed SOAM servers. Execute **Appendix D**. Un-Inhibit A and B Level Replication on C-Level Servers Navigate to **Status & Manage -> Database**

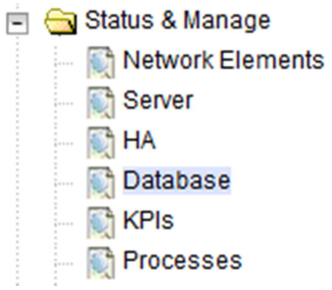
Procedure 2: Recovery Scenario 2

		 If the *"Repl Status"* is set to "Inhibited", click on the **Allow Replication** button as shown below using the following order, otherwise if none of the servers are inhibited, skip this step and continue with the next step: • Active NOAM Server • Standby NOAM Server • Active SOAM Server • Standby SOAM Server • Spare SOAM Server *(if applicable)* –Oracle X5-2/Netra X5-2/X6-2/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/HP DL380 Gen 9 Only Verify that the replication on all the working servers is allowed. This can be done by examining the Repl Status table as seen below: **OAM Repl Status** | **SIG Repl Status** | **Repl Status** | **Repl Audit Status** NotApplicable | NotApplicable | Allowed | NotApplicable Normal | NotApplicable | Allowed | NotApplicable Normal | NotApplicable | Allowed | NotApplicable Normal | NotApplicable | Allowed | NotApplicable
46. ☐	**(DSR Only) Activate PCA Feature**	If you have PCA installed in the system being recovered, execute the procedures "*PCA Activation on Stand By NOAM network*" on recovered StandBy NOAM Server and "*PCA Activation on Active SOAM network*" on recovered Active SOAM Server from **[7]** to re-activate PCA.
47. ☐	**NOAM VIP GUI:** Recover the C-Level Server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs	Recover C-Level Servers: **DSR:** Execute procedure *"Configure the MP Servers"*, Steps 1, 9-13 from reference [8] **Note:** Execute steps 14-16 of procedure *"Configure the MP Servers"* from reference [8] if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.

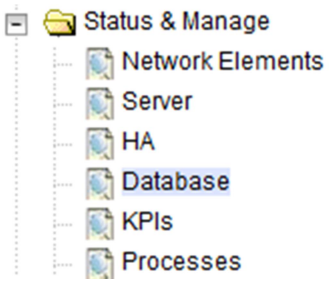
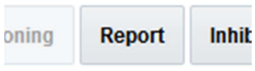
Procedure 2: Recovery Scenario 2

		SDS: Execute procedure *"Configure the SDS DP Servers"*, Steps 1, 5-8 from reference [8]. Repeat this step for any remaining failed MP servers.
48. ☐	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen For each recovered C-Level whose Max Allowed HA Role is set to OOS, set it to **Active**  Press **OK**
49. ☐	**NOAM VIP GUI:** Restart DSR Application on recovered C-Level Servers.	Navigate to **Main Menu->Status & Manage->Server**  Select the recovered C-Level servers and click on **Restart**. 
50.	**NOAM VIP GUI:** Start replication	**DSR Only, if SDS, Skip This Step**

Procedure 2: Recovery Scenario 2

☐	on all C-Level Servers (DSR Only)	Un-Inhibit *(Start)* Replication to the **ALL** C-Level Servers Navigate to **Status & Manage -> Database**  If the *"Repl Status"* is set to "Inhibited", click on the Allow Replication button as shown below using the following order: • Active NOAM Server • Standby NOAM Server • Active SOAM Server • Standby SOAM Server • Spare SOAM Server *(if applicable)-Oracle X5-2/Netra X5-2/X6-2/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/HP DL380 Gen 9 Only Verify that the replication on all the working servers is allowed. This can be done by examining the Repl Status table as seen below: **OAM Repl Status** | **SIG Repl Status** | **Repl Status** | **Repl Audit Status** NotApplicable | NotApplicable | Allowed | NotApplicable Normal | NotApplicable | Allowed | NotApplicable Normal | NotApplicable | Allowed | NotApplicable Normal | NotApplicable | Allowed | NotApplicable
51. ☐	**ACTIVE NOAM:** Perform key exchange between the active-NOAM and recovered servers.	Establish an SSH session to the Active NOAM, login as ***admusr.*** Execute the following command to perform a keyexchange from the active NOAM to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>` **Note:** If an export server is configured, perform this step.

Procedure 2: Recovery Scenario 2

52. ☐	**ACTIVE NOAM:** Activate Optional Features	**DSR Only, if SDS, Skip This Step** Establish an SSH session to the active NOAM, login as ***admusr.*** **Note For PCA Activation:** If you have PCA installed in the system being recovered, execute the procedure "*PCA Activation on Stand By NOAM server*" on recovered Standby NOAM Server and procedure "*PCA Activation on Active SOAM server*" on recovered Active SOAM Server from [6] to re-activate PCA. **Note:** If not all SOAM sites are recovered at this point, then you should repeat activation for each *new* SOAM site that comes online. **Note**: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature. Refer to **Section** 1.5 Optional Features to activate any features that were previously activated. **Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: `iload#31000{S/W Fault}`
53. ☐	**NOAM VIP GUI:** Fetch and Store the database Report for the Newly Restored Data and Save it	Navigate to **Main Menu -> Status & Manage -> Database**  Select the **active** NOAM server and click on the **Report** button at the bottom of the page.  The following screen is displayed:

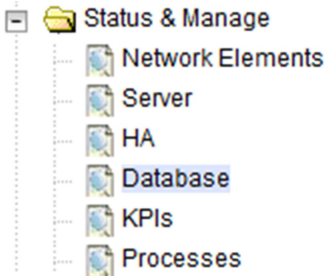
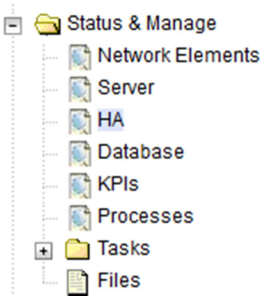
Procedure 2: Recovery Scenario 2

		Main Menu: Status & Manage -> Database [Report]
		
		`dsr Database Status Report`
		`Report Generated: Tue Oct 11 13:24:26 2016 EDT`
		`From: Active Network OAM&P on host ZombieNOAM1`
		`Report Version: 8.0.0.0.0-80.9.0`
		`User: guiadmin`
		
		`General`
		`Hostname : ZombieNOAM1`
		`Database Birthday : 2016-07-11 11:21:50 EDT`
		`Appworks Database Version : 6.0`
		`Application Database Version :`
		
		`Capacities and Utilization`
		`Disk Utilization 8.4%: 585M used of 7.0G total, 6.0G available`
		`Memory Utilization 0.0%: used of total, 0M available`
		
		Click on **Save** and save the report to your local machine.

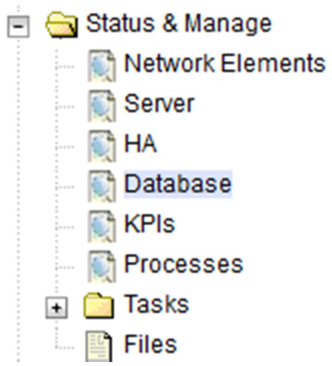
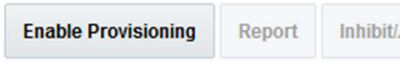
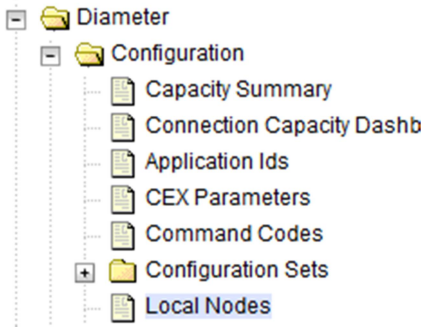
54. ☐	**ACTIVE NOAM:** Verify Replication Between Servers.	Login to the Active NOAM via SSH terminal as ***admusr***.
		
		Execute the following command:
		
		`$ sudo irepstat –m`
		
		Output like below shall be generated:
		
		`-- Policy 0 ActStb [DbReplication] ----------`
		`Oahu-DAMP-1 -- Active`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

Procedure 2: Recovery Scenario 2

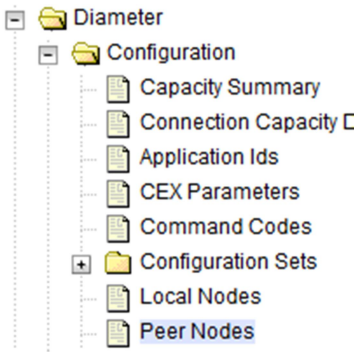
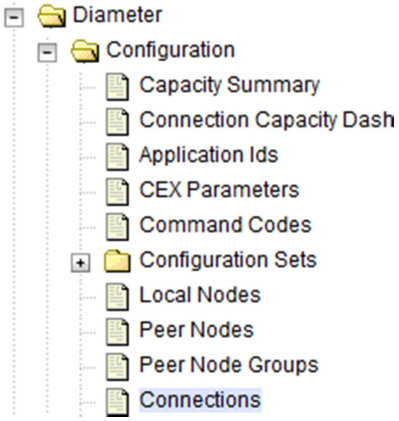
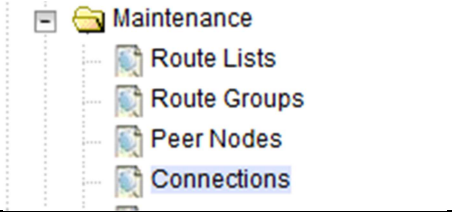
		<pre> BB To Oahu-SOAM-1 Active 0 0.50 1%R 0.04%cpu 32B/s
		  BC To Oahu-IPFE-1 Active 0 0.50 1%R 0.04%cpu 21B/s
		  BC To Oahu-SS7MP-2 Active 0 0.50 1%R 0.04%cpu 21B/s
		irepstat (40 lines) (h)elp (m)erged</pre>

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

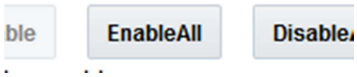
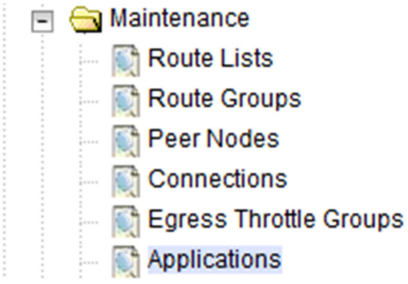
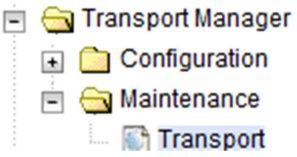
Procedure 2: Recovery Scenario 2

		<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>
57. ☐	**SOAM GUI:** Enable Provisioning	**DSR Only, if SDS, Skip This Step** Click on **Main Menu->Status & Manage->Database**  Enable Provisioning by clicking on **Enable Provisioning** button at the bottom of the screen as shown below.  A confirmation window will appear, press **OK** to enable Provisioning.
58. ☐	**SOAM VIP GUI:** Verify the Local Node Info (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Configuration->Local Node**  Verify that all the local nodes are shown.
59.	**SOAM VIP GUI:** Verify the Peer	**DSR Only, SDS Skip This Step**

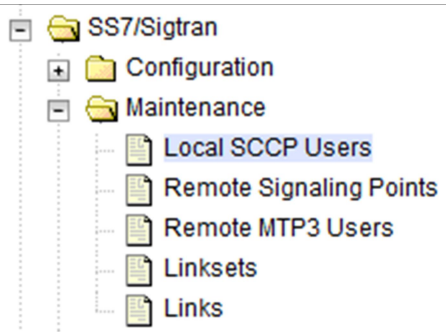
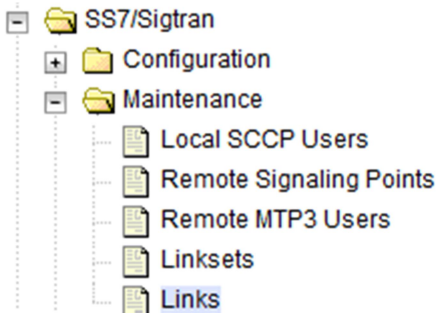
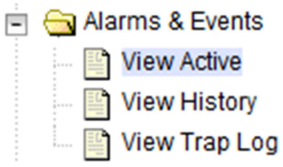
Procedure 2: Recovery Scenario 2

☐	Node Info (DSR Only)	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.
60. ☐	**SOAM VIP GUI:** Verify the Connections Info (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Configuration->Connections**  Verify that all the connections are shown.
61. ☐	**MP Servers:** Disable SCTP Auth Flag (DSR Only)	**DSR Only, SDS Skip This Step** For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [8] Execute this procedure on all Failed MP Servers.
62. ☐	**SOAM VIP GUI:** Enable Connections if needed (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Maintenance->Connections** 

Procedure 2: Recovery Scenario 2

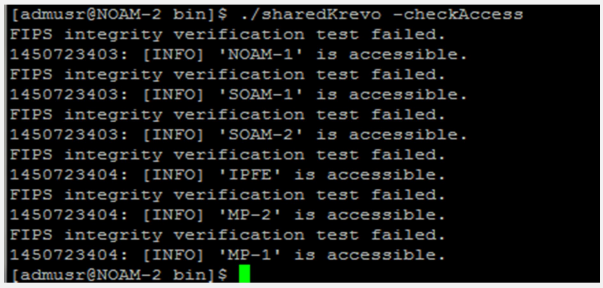
		Select each connection and click on the **Enable** button. Alternatively you can enable all the connections by selecting the **EnableAll** button.  Verify that the Operational State is Available. **Note:** If a Disaster Recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution
63. ☐	**SOAM VIP GUI:** Enable Optional Features (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Select the optional feature application configured in **step 71** Click the **Enable** button. 
64. ☐	**SOAM VIP GUI:** Re-enable Transports if Needed (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Transport Manager -> Maintenance -> Transport**  Select each transport and click on the **Enable** button  Verify that the Operational Status for each transport is Up.
65. ☐	**SOAM VIP GUI:** Re-enable MAPIWF application if	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users**

Procedure 2: Recovery Scenario 2

	needed(DSR Only)	 Click on the **Enable** button corresponding to MAPIWF Application Name.  Verify that the SSN Status is Enabled.
66. ☐	**SOAM VIP GUI:** Re-enable links if needed (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->SS7/Sigtran->Maintenance->Links**  Click on **Enable** button for each link.  Verify that the Operational Status for each link is Up.
67. ☐	**SOAM VIP GUI:** Examine All Alarms	Navigate to **Main Menu->Alarms & Events->View Active**  Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix K.** My Oracle Support (MOS).

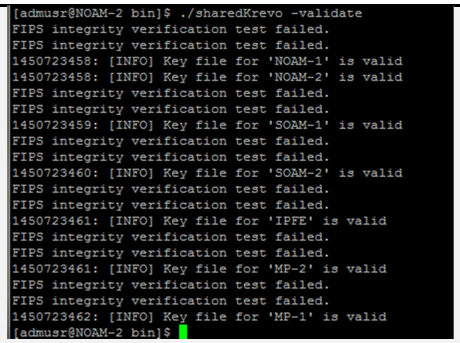
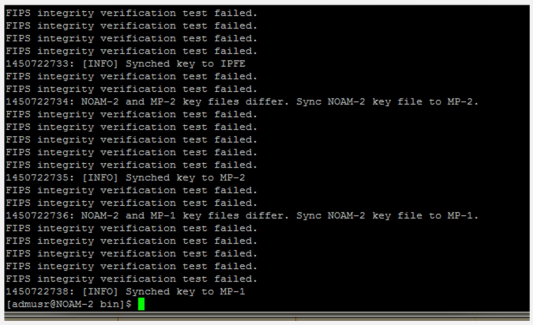
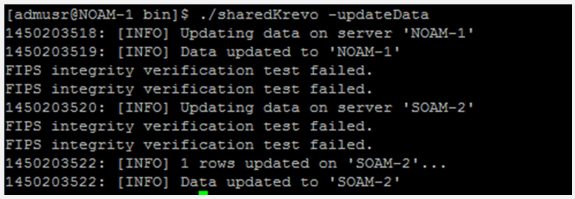
Procedure 2: Recovery Scenario 2

68. ☐	**NOAM VIP GUI:** Examine All Alarms	Login to the NOAM VIP if not already logged in. Navigate to **Main Menu->Alarms & Events->View Active**  Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix K.** My Oracle Support (MOS).

69. ☐	**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)**
		
		Establish an SSH session to the NOAM VIP. Login as ***admusr.***
		
		Execute following commands to check if all the servers in the Topology are accessible :
		
		`$ cd /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo -checkAccess`
		
		Example Output:
		
		 

70. ☐	**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)**
		
		Execute following commands to 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`

Procedure 2: Recovery Scenario 2

		 If output of above command shows that the existing key file is not valid, contact Appendix K. My Oracle Support (MOS) Execute following command to copy the key file to all the servers in the Topology: **$ ./sharedKrevo –synchronize**  **$ ./sharedKrevo –updateData**  **Note:** If any errors are present, stop and contact Appendix K. My Oracle Support (MOS)
71. ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**. Database Backup to back up the Configuration databases:
72. ☐	**Recover IDIH** (If Configured)	If any components of IDIH were affected, refer to **Section 7.0** to perform the disaster recovery on IDIH.

5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact)

For a partial server outage with an SOAM server intact and available; NOAM servers are recovered using recovery procedures 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 will recover the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures' detailed steps are in **Procedure 3**. The major activities are summarized as follows:

Recover **Active NOAM** server by recovering 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, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Workarounds**	Refer to Appendix G. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.
2. ☐	**Gather Required Materials**	Gather the documents and required materials listed in **Section 3.1** Required Materials**.**
3. ☐	**Replace Failed Equipment**	HW vendor to replace the failed equipment
4. ☐	**Recover PMAC TVOE Host (If Required):** 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:"***Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings"* • **HP DL380 Gen9:** *"Configure HP Gen9 Server BIOS Settings"* 2. Verify and/or upgrade server firmware by executing procedure *"Upgrade Rack Mount Server Firmware"* from reference [8]
5. ☐	**Recover PMAC and PMAC TVOE Host:** Backup Available	This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, **skip this step**. 1. Restore the TVOE backup by executing **Appendix E**. Restore TVOE Configuration from Backup Media on **ALL** failed rack mount servers 2. Restore the PMAC backup by executing **Appendix F**. Restore PMAC from Backup **Proceed to Step 7**

Procedure 3: Recovery Scenario 3

6. ☐	**Recover PMAC and PMAC TVOE Host:** Backup Not Available	This step assumes that TVOE and PMAC backups are **NOT** available, if the TVOE and PMAC have already been restored, **skip this step** 1. Execute procedure *"Install and Configure TVOE on First RMS (PMAC Host)"* from reference [8] 2. Execute section *"Install PMAC"* from reference [8] 3. Execute section *"Initialize the PMAC Application"* from reference [8] **Proceed to Next Step**
7. ☐	**Recover Failed Cisco 4948 Aggregation Switches** (HP DL380 Only)	**Oracle X5-2/Netra X5-2/X6-2/HP DL380 GEN 9 SKIP THIS STEP** Recover failed Cisco 4948 aggregation switches, if needed: Backup configuration files available: Refer to **Appendix B**. Recovering/Replacing Failed Cisco 4948 Aggregation Switches to recover failed Cisco 4948 aggregation switches Backup configuration files **NOT** available: Execute section "Configure Cisco 4948E-F Aggregation Switches (HP DL 380 Gen 8 Only)" 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 sections *"Configure PMAC Server (NetBackup Only)"* and *"Add RMS to the PMAC Inventory"* from reference [8]
9 ☐	**Install/Configure Additional Rack Mount Servers** (Backups available)	This step assumes that TVOE backups are available, if backups are **NOT** available, **skip this step**. 1. Execute procedure *"Install TVOE on Additional Rack Mount Servers"* from reference [8] 2. Restore the TVOE backup by executing **Appendix E**. Restore TVOE Configuration from Backup Media on **ALL** failed rack mount servers
10 ☐	**Install/Configure Additional Rack Mount Servers** (Backups ***NOT*** available)	This step assumes that TVOE backups are ***NOT*** available, if backups are available, execute the previous step. 1. Execute procedure *"Install TVOE on Additional Rack Mount Servers"* from reference [8] 2. Execute *"Configure TVOE on Additional Rack Mount Servers"* from reference [8]

Procedure 3: Recovery Scenario 3

11 ☐	**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:** *"Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings"* • **HP DL380 Gen9:** *"Configure HP Gen9 Server BIOS Settings"* 2. Verify and/or upgrade server firmware by executing procedure *"Upgrade Rack Mount Server Firmware"* from reference [8]
12 ☐	**Determine VM Placement and Socket Pinning** (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen9 Only)	**HP DL380 GEN 8 SKIP THIS STEP** Determine the VM placement and Pinning for proper VM placement and pinning. Refer 12 for workbook reference
13 ☐	**Deploy Redundant PMAC (if required)**	Refer to procedure *"Deploy Redundant PMAC (Optional)"* to re-deploy and configure any redundant PMACs previously configured.
14 ☐	**PMAC: Determine if an fdconfig file exists from the initial deployment.**	Determine whether the fdconfig backup file exists: [admusr@melbourne-pmac-1 ~]$ ll /usr/TKLC/smac/etc/fdc/ Examine the results and verify whether the rms config file <hostname>.cfg exists Note: There may be multiple fdconfig backup files here with respect to each RMS. Select the respective one according to the RMS.
15 ☐	**If fdc backup file does NOT exist**	**Execute this step ONLY If the fdconfig backup file does NOT exist:** If the fdconfig file does NOT exist : Create the needed file(s) by executing section "Virtual Machine/Network Fast Deployment" from reference [8] **WARNING:** It is very important to ensure the file(s) created only affect the TVOE server(s) and its 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. Skip to step 24 if this step was executed

Procedure 3: Recovery Scenario 3

16 ☐	**PMAC [If fdc backup file exists]: Load ISOs into PMAC if not done already**	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:** If the DSR, SDS, and TPD ISOs are NOT loaded in to the PMAC: Execute procedures 14 of section "Virtual Machine/Network Fast Deployment" from reference [8] If already loaded into PMAC, skip this step.

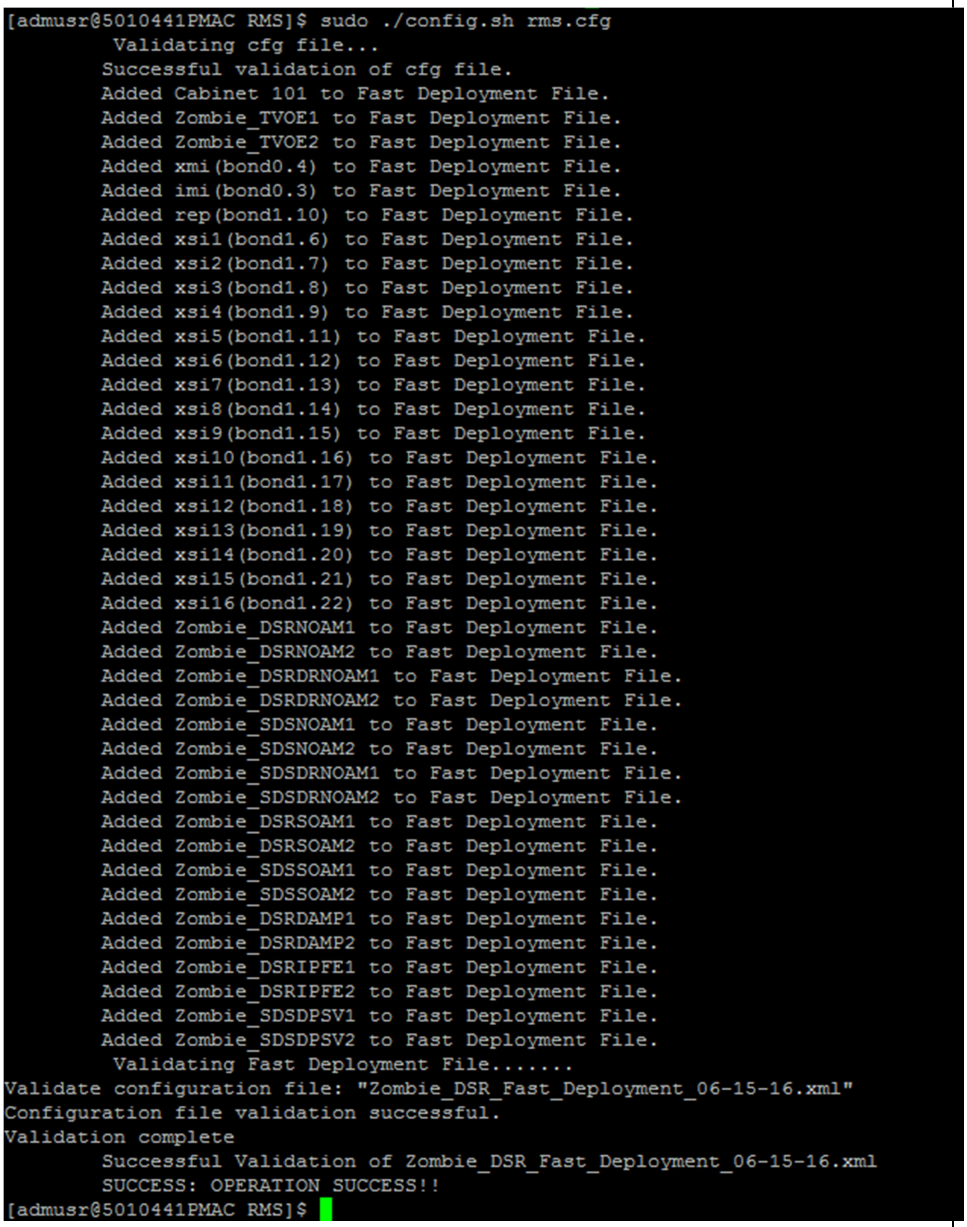
Procedure 3: Recovery Scenario 3

17 ☐	**PMAC** **[If fdc backup file exists]:** Edit/Update Configuration File	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:** **Edit the fdconfig file to include only the required/failed servers.** **Note:** Comment out configuration items that are not needed. **Note:** It is recommended that a separate configuration file be created for **EACH** rack mount server being deployed. Note:Cabinet ID in the config file needs to match the cabinet already defined in PM&C" 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) • SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured) • SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured) • SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured) • SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured) **Note:** Refer to **Appendix R: VM Automation Profile Values** for DSR and SDS profile values with the configuration file from reference [8] Note: Comment out SDS and DSR profile items if corresponding products are not used. **Note: [Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/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] **Note:** The VM names should not be modified in the .cfg file. The names are fixed and will be prefixed in the siteName. **Note:** The VM locations should not be changed from their 'RMSx' format. Each RMS should correspond with a separate Rack Mount Server. **WARNING**: It is very important to ensure the file(s) created only affect the TVOE server(s) and its 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.

Procedure 3: Recovery Scenario 3

18 ☐	**PMAC** **[If fdc backup file exists]:** Copy the located backed up fdc file to the RMS directory	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:** Copy the located fdconfig backup file to the RMS directory: `$ cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file> /usr/TKLC/smac/etc/RMS/`

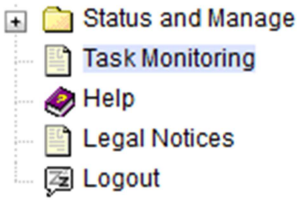
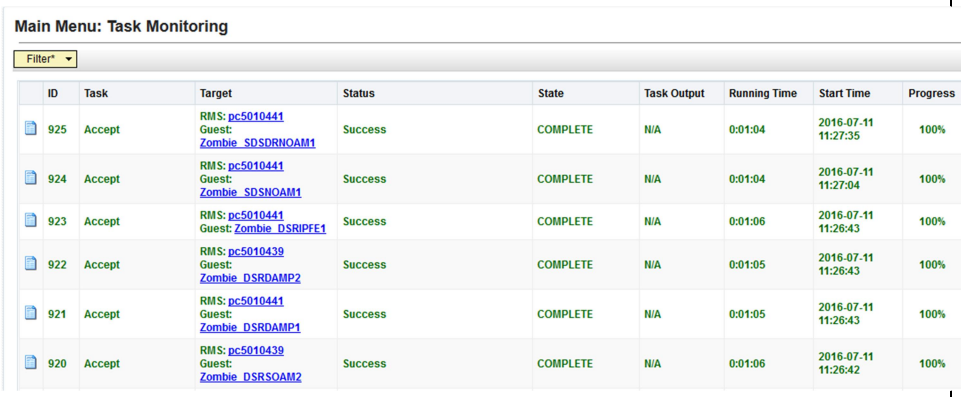
Procedure 3: Recovery Scenario 3

19 ☐	**PMAC [If fdc backup file exists]:** Execute the config.sh script	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:** Execute config.sh against the modified back up config file defined above: **Note:** If the below command is executed on multiple cfg files, it will overwrite the existing xml file. It is recommended to rename the xml file before running the below command again. **$ sudo ./config.sh <config file>** Sample 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

20
☐
	PMAC
	[If fdc backup file exists]:
	Execute Fast Deployment
		Execute this step ONLY If the fdconfig backup file exists and located at step 14:
		
		With the file generated from the config.sh script, execute the following command to start fast deployment:
		
		`$ screen`
		
		`$ sudo fdconfig config --file=<fd_config.xml>`
		
		Note: This is a long duration command. If the screen command was run prior to executing the fdconfig, perform a *"screen -dr"* to resume the screen session in the event of a terminal timeout etc.

Procedure 3: Recovery Scenario 3

21 ☐	**PMAC GUI [If fdc backup file exists]:** Monitor the Configuration	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:** If not already done so, establish a GUI session on the PMAC server. Navigate to **Main Menu -> Task Monitoring**  Monitor the configuration to completion:  **Note:** Should a failure occur with fdconfig, logs can be accessed in /var/TKLC/log/fdconfig/fdconfig.log [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 Run Below command to restart the fdconfig after a failure has occurred and has been resolved: $ sudo fdconfig restart --

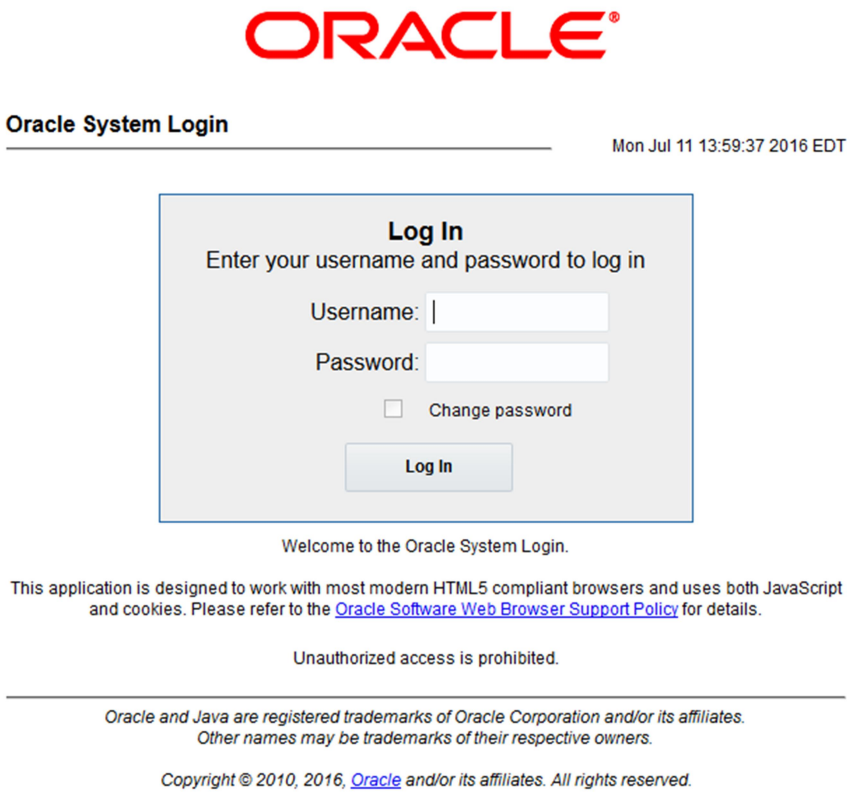
Procedure 3: Recovery Scenario 3

22 ☐	**PMAC [If fdc backup file exists]:** Repeat for each Rack mount server configuration file	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:** Repeat **steps 14-21** for each rack mount server/configuration file located at step 14, if required.
23 ☐	**PMAC [If fdc backup file exists]:** Backup FDC file	**Execute this step ONLY If the fdconfig backup file exists and located at step 14:** Copy the updated fdc file to the fdc backup directory: **`$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> /usr/TKLC/smac/etc/fdc/`** 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 procedure *"CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen9 Only)"* from reference [8]
25 ☐	**Obtain Latest Database Backup and Network Configuration Data.**	1. Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. 2. Obtain most recent "RADIUS shared secret encryption key" file DpiKf.bin.encr from external backup sources (Only when the RADIUS Key Revocation MOP has been executed on the system) From required materials list in **Section 3.1** `Required Materials`; use site survey documents and Network Element report (if available), to determine network configuration data.

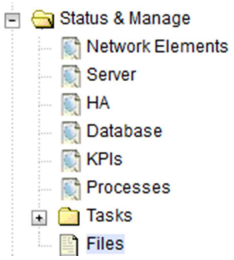
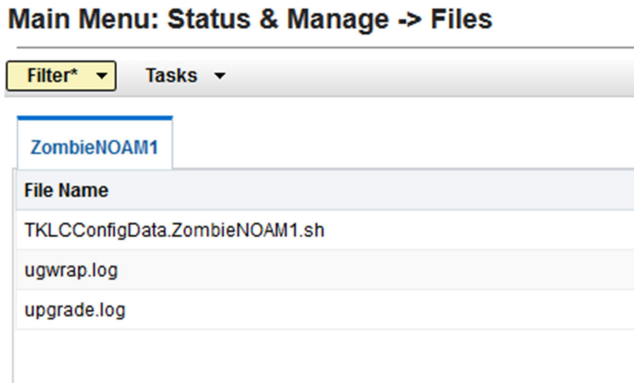
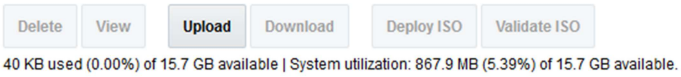
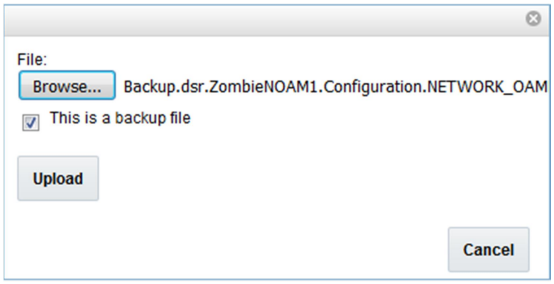
Procedure 3: Recovery Scenario 3

26 ☐	**Execute DSR Installation Procedure for the First NOAM**	Verify the networking data for Network Elements **Note:** Use the backup copy of network configuration data and site surveys (Step 2) **Note:** SDS disaster recovery actions can and should be worked simultaneously, doing so would allow faster recovery of the complete solution (i.e. stale DB on DP servers will not receive updates until SDS-SOAM servers are recovered. The following steps will be written to 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 procedure *"Configure First NOAM NE and Server"* from reference [8] 2. Configure the NOAM server group by executing procedure *"Configure the NOAM Server Group"* from reference [8] **SDS:** 1. Configure the first SDS NOAM server by executing procedure *"Configure First SDS NOAM NE and Server"* from reference [8] 2. Configure the SDS NOAM server group by executing procedure *"Configure the SDS NOAM Server Group"* from reference [8]

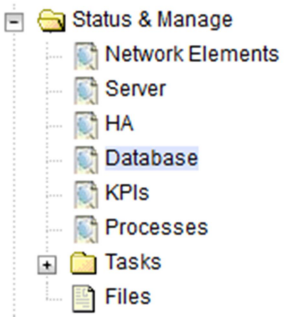
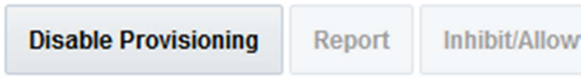
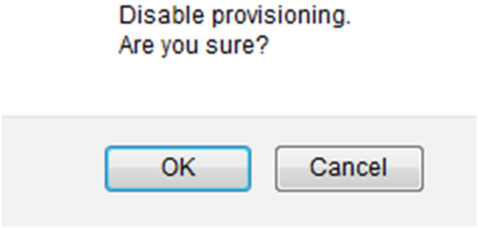
Procedure 3: Recovery Scenario 3

27 ☐	**NOAM GUI:** Login	**DSR Only, if SDS, Skip to Step 32** **If the failed server(s) are NOT OAM type, skip to step 38** Login to the NOAM GUI as the ***guiadmin*** user: 

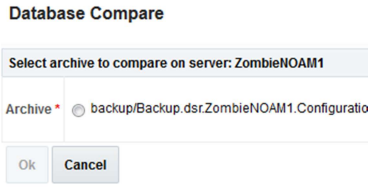
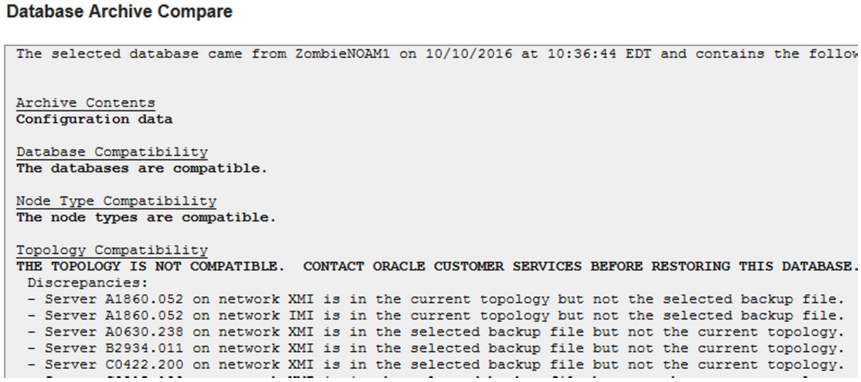
Procedure 3: Recovery Scenario 3

28 ☐	**NOAM GUI:** Upload the Backed up Database File	**DSR Only, if SDS, Skip to Step 32** Browse to **Main Menu->Status & Manage->Files**  Select the Active NOAM server. The following screen will appear:  Click on **Upload** as shown below and select the file *"NO Provisioning and Configuration:"* file backed up after initial installation and provisioning.  1. Click on **Browse** and locate the backup file 2. Check **This is a backup file** Box 3. Click on Open as shown below.  Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.

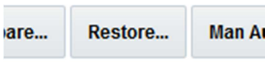
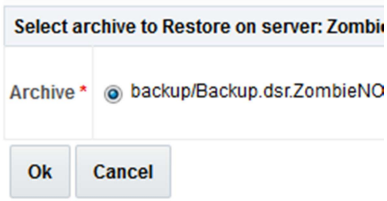
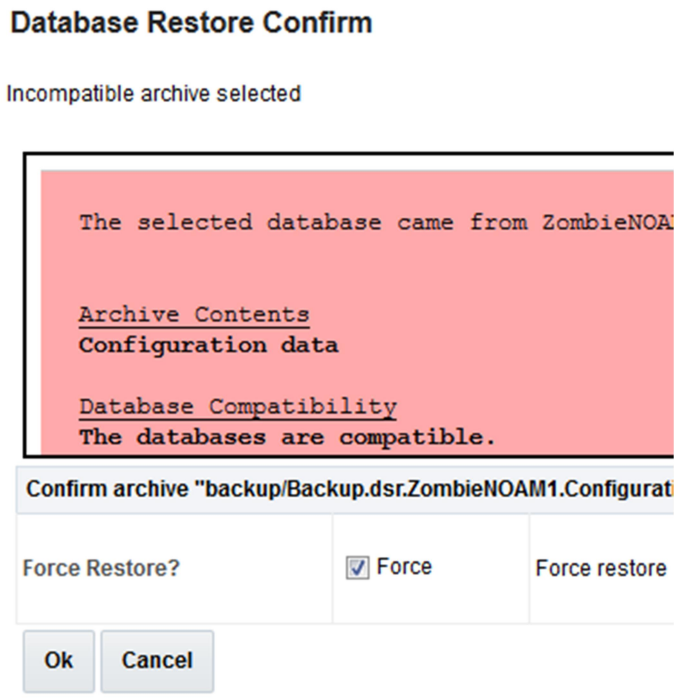
Procedure 3: Recovery Scenario 3

29 ☐	**NOAM GUI:** Disable Provisioning	**DSR Only, if SDS, Skip to Step 32** Click on **Main Menu->Status & Manage->Database**  Disable Provisioning by clicking on **Disable Provisioning** button at the bottom of the screen as shown below.  A confirmation window will appear, press **OK** to disable Provisioning. 

Procedure 3: Recovery Scenario 3

30 ☐	**NOAM GUI:** Verify the Archive Contents and Database Compatibility	**DSR Only, if SDS, Skip to Step 32** Select the **Active NOAM** server and click on the **Compare**.  The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 28** of this procedure.  **Verify** that the output window matches the screen below. **Note:** You will get a database mismatch regarding the Topology Compatibility and possibly User compatibility (due to authentication) These warnings are expected. If these are the only mismatches, proceed, otherwise stop and contact Appendix K. My Oracle Support (MOS) and ask for assistance.  **Note:** Archive Contents and Database Compatibilities must be the following: **Archive Contents:** Configuration data **Database Compatibility:** The databases are compatible. **Note:** The following is expected Output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one NOAM: **Topology Compatibility** THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID. **Note:** We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility. If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.

Procedure 3: Recovery Scenario 3

31 ☐	**ACTIVE NOAM:** Restore the Database	**DSR Only, if SDS, Skip to Step 32** From **Main Menu->Status & Manage->Database** Select the **Active NOAM** server, and click on **Restore** as shown below.  The following screen will be displayed. Select the proper back up provisioning and configuration file.  Click **OK** Button. The following confirmation screen will be displayed. If you get errors related to the warnings highlighted in the previous step, that is expected. If no other errors are displayed, select the **Force** checkbox as shown above and Click **OK** to proceed with the DB restore.  **Note:** After the restore has started, the user will be logged out of XMI NO GUI since the restored Topology is old data.

Procedure 3: Recovery Scenario 3

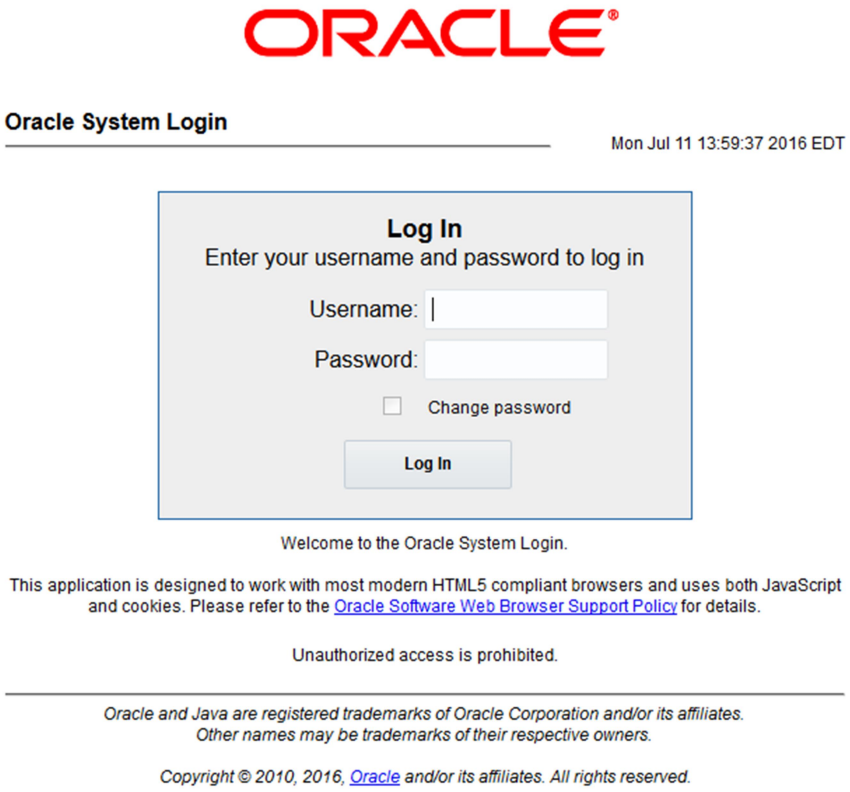
32 ☐	**SDS NOAM:** Transfer SDS Configuration and Provisioning backup Database Files	**SDS Only, if DSR, Skip this step**
		
		Using the IP of the recovered SDS NOAM, transfer the uncompressed backup database files to the */var/TKLC/db/filemgmt* directory
		
		Linux:
		
		3. From the command line of a Linux machine use the following command to copy the configuration backup file to the SDS NOAM guest:
		
		`# scp <path_to_configuration_db_file> admusr@<SDS_NOAM_IP>:/var/TKLC/db/filemgmt`
		
		4. From the command line of a Linux machine use the following command to copy the provisioning backup file to the SDS NOAM guest:
		
		`# scp < path_to_provisioning_db _file> admusr@<SDS_NOAM_IP>:/var/TKLC/db/filemgmt`
		
		Note: 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. Please refer to [9] procedure *Using WinSCP* to copy the backup image to the customer system.

33 ☐	**SDS NOAM:** Login	**SDS Only, if DSR, Skip this step** Establish an SSH session to the SDS active NOAM XMI IP address, login as ***admusr.***
34 ☐	**SDS NOAM:** Stop running applications	**SDS Only, if DSR, Skip this step** 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.

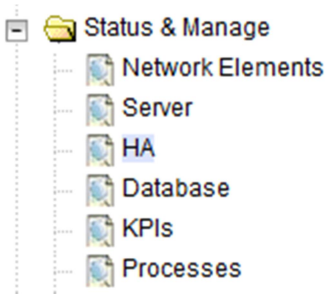
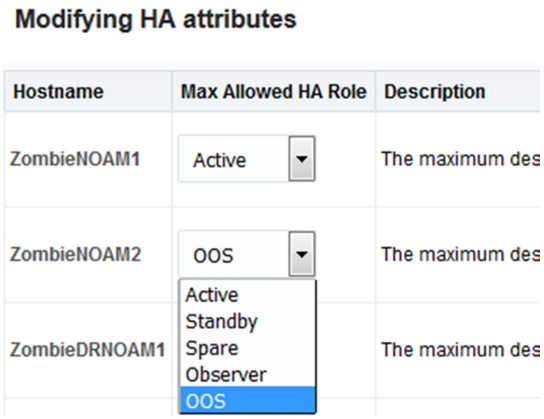
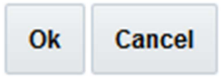
Procedure 3: Recovery Scenario 3

35 ☐	**SDS NOAM:** Stop running applications	**SDS Only, if DSR, Skip this step** 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>`
36 ☐	**SDS NOAM:** Stop running applications	**SDS Only, if DSR, Skip this step** Restore the configuration DB by executing the following command: `$ sudo idb.restore -n -t /var/TKLC/db/filemgmt -v <full path to provisioning archive file name>`
37 ☐	**SDS NOAM:** Stop running applications	**SDS Only, if DSR, Skip this step** Start the SDS application by executing the following command: `$ sudo prod.start`

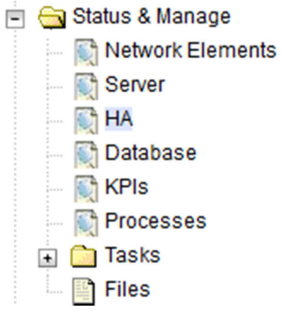
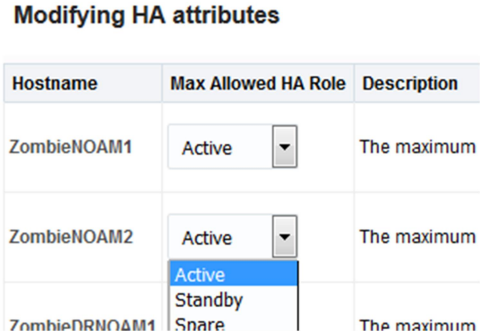
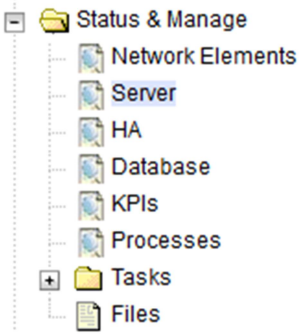
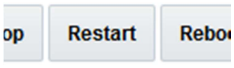
Procedure 3: Recovery Scenario 3

38 ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 
39 ☐	**NOAM VIP GUI:** Monitor and Confirm database restoral	Wait for **5-10 minutes** for the System to stabilize with the new topology: Monitor the Info tab for **"Success"**. This will indicate that the restore is complete and the system is stabilized. Following alarms **must** be ignored for NOAM and MP/DP Servers until all the Servers are configured: Alarms with Type Column as **"REPL"** , **"COLL", "HA"** (with mate NOAM), **"DB"** (about Provisioning Manually Disabled) **Note:** Do not pay attention to alarms until all the servers in the system are completely restored. **Note:** The Configuration and Maintenance information will be in the same state it was backed up during initial backup.

Procedure 3: Recovery Scenario 3

40 ☐	**Active NOAM:** Set Failed Servers to OOS	Navigate to **Main Menu -> Status & Manage -> HA**  Select **Edit**  Set the Max Allowed HA Role drop down box to **OOS** for the failed servers. Select **Ok** 
41 ☐	**NOAM VIP GUI:** Recover Standby NOAM	Install the second NOAM server: **DSR:** Execute procedure *"Configure the Second NOAM Server",* steps 1, 3-6 from reference [8] **SDS:** Execute procedure *"Configure the Second SDS NOAM Server",* steps 1, 3-6 from reference [8]
42 ☐	**Install NetBackup Client (Optional)**	If NetBackup is used execute procedure *"Install NetBackup Client (Optional)"* from reference [8]

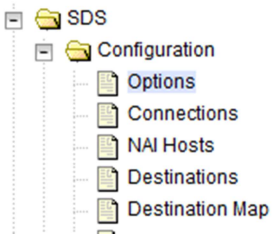
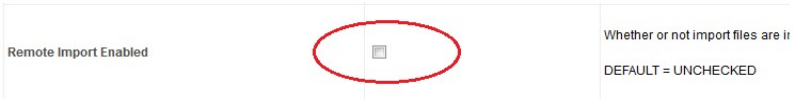
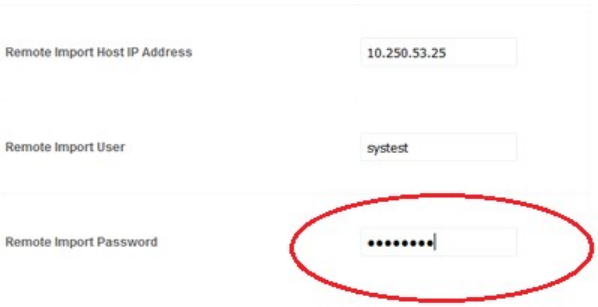
Procedure 3: Recovery Scenario 3

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

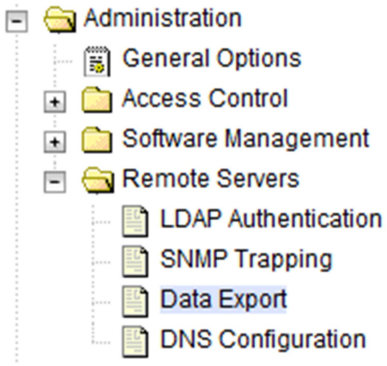
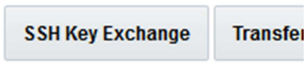
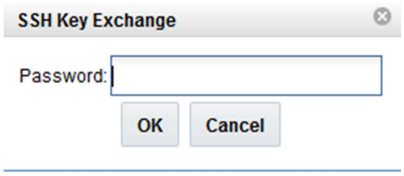
Procedure 3: Recovery Scenario 3

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

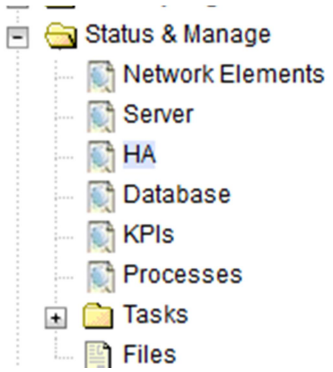
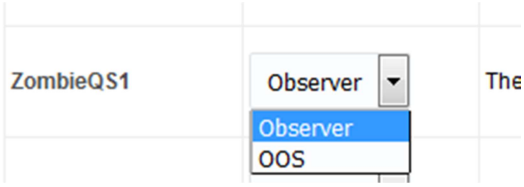
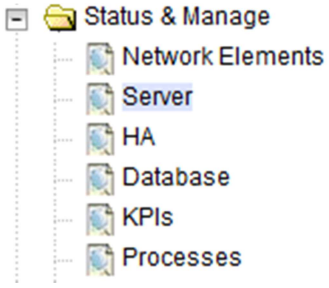
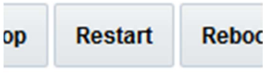
Procedure 3: Recovery Scenario 3

46 ☐	**NOAM VIP GUI:** Perform Keyexchange with Remote Import Server	**SDS Only, DSR Skip This Step** 7) Navigate to **Main Menu -> SDS -> Configuration -> Options**  8) Uncheck the **Remote Import Enabled Box**:  9) Click **Apply** **Note:** Re-navigate to **Main Menu -> SDS -> Configuration -> Options** to clear Success banner. 10) Re-Enter the **Remote Import Password**:  11) Click **Apply**  **Note:** Re-navigate to **Main Menu -> SDS -> Configuration -> Options** to clear Success banner. 12) Check the **Remote Import Enabled Box**: 

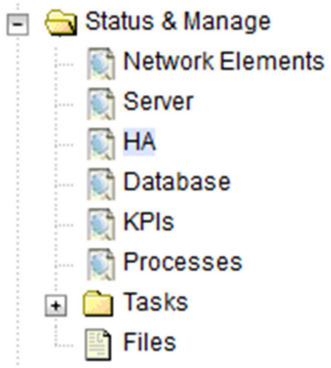
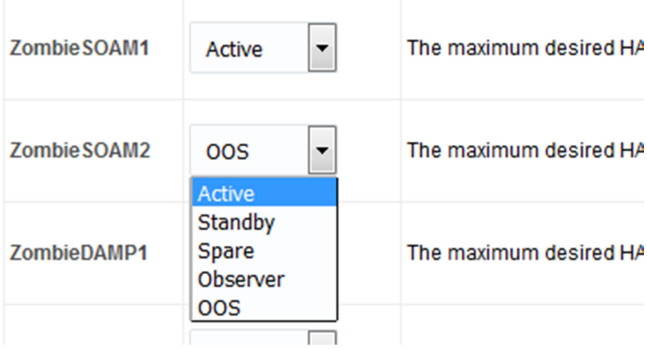
Procedure 3: Recovery Scenario 3

47 ☐	**NOAM VIP GUI:** Repeat for Remote Export Server	**SDS Only, DSR Skip This Step** Repeat **Step 35** for the remote Export Server
48 ☐	**NOAM VIP GUI:** Perform Keyexchange with Export Server	Navigate to **Main Menu -> Administration -> Remote Servers -> Data Export**  Click on **SSH Key Exchange** at the bottom of the screen  Enter the Password and press **OK** 
49 ☐	**NOAM VIP GUI:** Recover Query Servers	**SDS Only, DSR Skip This Step** Execute procedure *"Configuring SDS Query Servers",* steps 1, 4-7 from reference [8]

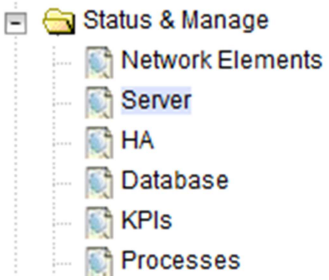
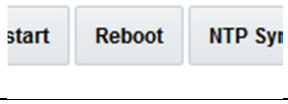
Procedure 3: Recovery Scenario 3

50 ☐	**SDS NOAM VIP GUI:** Set HA on Query Server	**SDS Only, DSR Skip This Step** Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Select the Query server, set it to **Observer**  Press **OK**
51 ☐	**SDS NOAM VIP GUI:** Restart SDS application	**SDS Only, DSR Skip This Step** Navigate to **Main Menu->Status & Manage->Server**  Select the recovered Query server and click on **Restart**. 

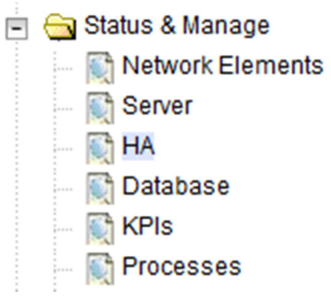
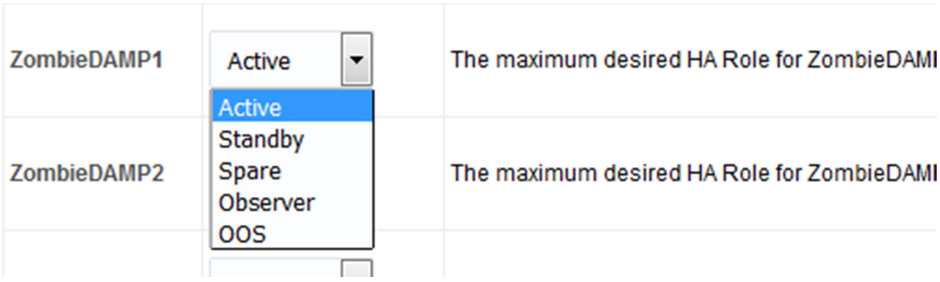
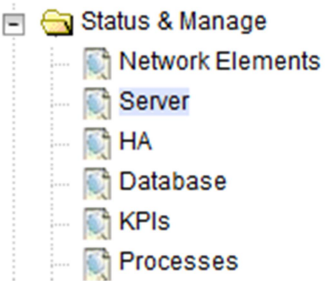
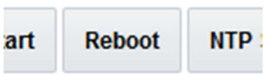
Procedure 3: Recovery Scenario 3

52 ☐	**NOAM VIP GUI:** Recover the Remaining SOAM Servers	Recover the **remaining** SOAM servers (**Standby, Spare**): Execute procedure *"Configure the SOAM Servers"*, steps 1-3, and 5-9, from reference [8] **Note:** If you are using NetBackup, also execute step 12. of procedure "*Configure the SOAM Servers"* from reference [8] **SDS:** Execute procedure *"Configure the SDS DP SOAM Servers"*, steps 1-3, and 5-8 from reference [8]
53 ☐	**NOAM VIP GUI:** Set HA on Standby SOAM	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen  Select the standby SOAM server, set it to **Active** Press **OK**

Procedure 3: Recovery Scenario 3

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

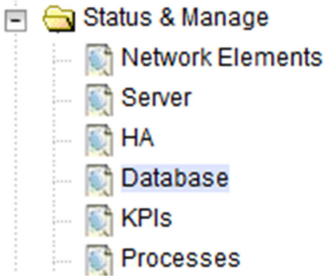
Procedure 3: Recovery Scenario 3

57 ☐	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen For each server whose Max Allowed HA Role is set to OOS, set it to **Active**  Press **OK**
58 ☐	**NOAM VIP GUI:** Restart DSR Application on recovered C-Level Servers.	Navigate to **Main Menu->Status & Manage->Server**  Select the recovered C-Level servers and click on **Restart**. 

Procedure 3: Recovery Scenario 3

59 ☐	**ACTIVE NOAM:** Perform key exchange between the active-NOAM and recovered servers.	Establish an SSH session to the Active NOAM, login as ***admusr.*** Execute the following command to perform a keyexchange from the active NOAM to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>` **Note:** If an export server is configured, perform this step.
60 ☐	**ACTIVE NOAM:** Activate Optional Features	**DSR Only, if SDS, Skip This Step** Establish an SSH session to the active NOAM, login as ***admusr.*** **Note For PCA Activation:** If you have PCA installed in the system being recovered, execute the procedure "*PCA Activation on Active NOAM server*" on recovered Active NOAM Server and procedure "*PCA Activation on Stand By SOAM server*" on recovered Standby SOAM from [6] to re-activate PCA. **Note:** If not all SOAM sites are recovered at this point, then you should repeat activation for each *new* SOAM site that comes online. **Note**: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature. Refer to **Section** 1.5 Optional Features to activate any features that were previously activated. **Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: *iload#31000{S/W Fault}*

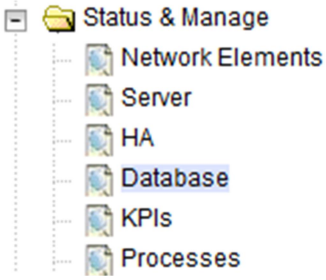
Procedure 3: Recovery Scenario 3

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

Procedure 3: Recovery Scenario 3

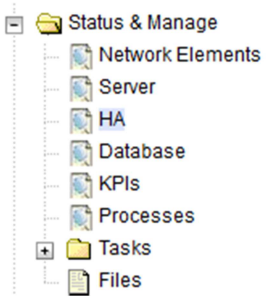
62 ☐	**ACTIVE NOAM:** Verify Replication Between Servers.	Login to the Active NOAM via SSH terminal as ***admusr***.
		
		Execute the following command:
		
		$ sudo irepstat –m
		
		Output like below shall be generated:
		
		`-- Policy 0 ActStb [DbReplication] ----------`
		`----------`
		`Oahu-DAMP-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.15%cpu 25B/s  A=me`
		`  CC To  Oahu-DAMP-2  Active  0  0.10  0.14%cpu 25B/s  A=me`
		`Oahu-DAMP-2 -- Stby`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.11%cpu 31B/s`
		`A=C3642.212`
		`  CC From Oahu-DAMP-1  Active  0  0.10 ^0.14 1.16%cpu 31B/s`
		`A=C3642.212`
		`Oahu-IPFE-1 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 24B/s`
		`A=C3642.212`
		`Oahu-IPFE-2 -- Active`
		`  BC From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 28B/s`
		`A=C3642.212`
		`Oahu-NOAM-1 -- Stby`
		`  AA From Oahu-NOAM-2  Active  0  0.25 ^0.03%cpu 23B/s`
		`Oahu-NOAM-2 -- Active`
		`  AA To  Oahu-NOAM-1  Active  0  0.25 1%R 0.04%cpu 61B/s`
		`  AB To  Oahu-SOAM-2  Active  0  0.50 1%R 0.05%cpu 75B/s`
		`Oahu-SOAM-1 -- Stby`
		`  BB From Oahu-SOAM-2  Active  0  0.50 ^0.03%cpu 27B/s`
		`Oahu-SOAM-2 -- Active`
		`  AB From Oahu-NOAM-2  Active  0  0.50 ^0.03%cpu 24B/s`
		`  BB To  Oahu-SOAM-1  Active  0  0.50 1%R 0.04%cpu 32B/s`
		`  BC To  Oahu-IPFE-1  Active  0  0.50 1%R 0.04%cpu 21B/s`
		`  BC To  Oahu-SS7MP-2 Active  0  0.50 1%R 0.04%cpu 21B/s`
		`irepstat ( 40 lines) (h)elp (m)erged`

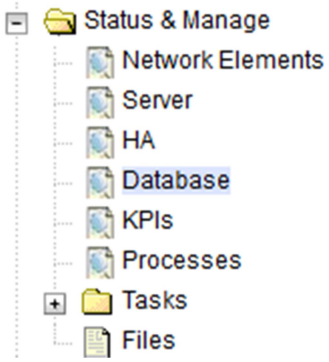
Procedure 3: Recovery Scenario 3

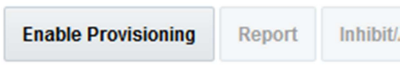
63 ☐	**NOAM VIP GUI:** Verify the Database states	Click on **Main Menu->Status and Manager->Database**  Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below:

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 3: Recovery Scenario 3

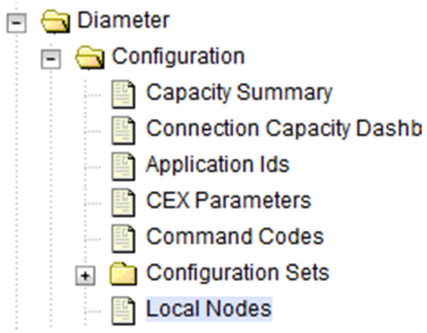
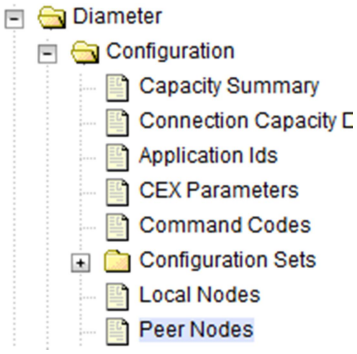
<table>
<tr>
<td>64
☐</td>
<td>NOAM VIP GUI:
Verify the HA Status</td>
<td>Click on Main Menu->Status and Manage->HA
 

Select the row for all of the servers
Verify that the “HA Role” is either “Active” or “Standby”.
<table>
<tr><th>Hostname</th><th>OAM HA Role</th><th>Application HA Role</th><th>Max Allowed HA Role</th></tr>
<tr><td>ZombieNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieDRNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieDRNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieSOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr>
<tr><td>ZombieSOAM2</td><td>Standby</td><td>N/A</td><td>Standby</td></tr>
</table>
</td>
</tr>
<tr>
<td>65
☐</td>
<td>NOAM GUI:
Enable Provisioning</td>
<td>Click on Main Menu->Status & Manage->Database
 

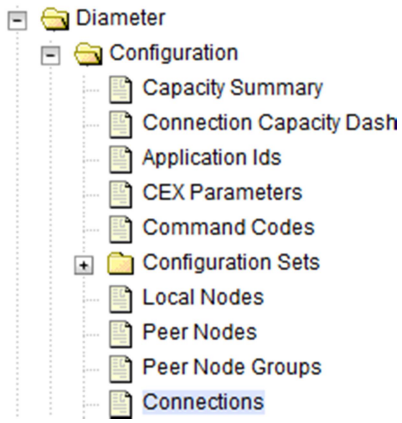
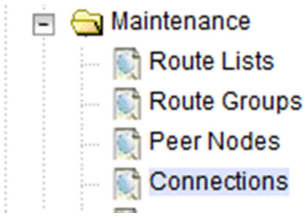
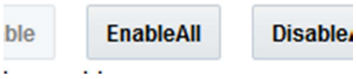
Enable Provisioning by clicking on Enable Provisioning button at the bottom of the screen as shown below.
 

A confirmation window will appear, press OK to enable Provisioning.</td>
</tr>
</table>

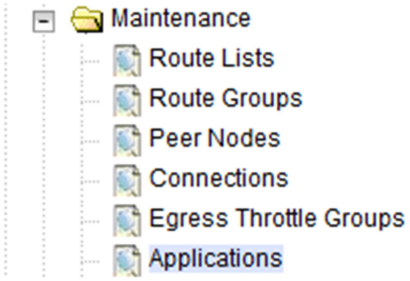
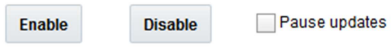
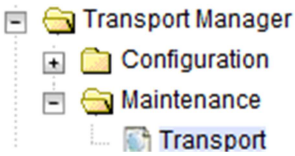
Procedure 3: Recovery Scenario 3

66 ☐	**SOAM VIP GUI:** Verify the Local Node Info (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Configuration->Local Node**  Verify that all the local nodes are shown.
67 ☐	**SOAM VIP GUI:** Verify the Peer Node Info (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.

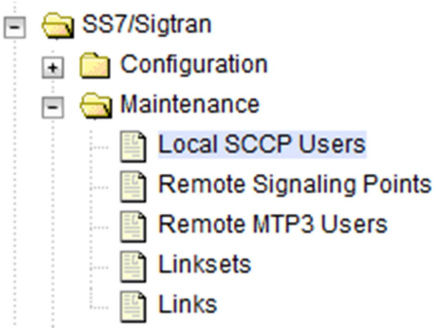
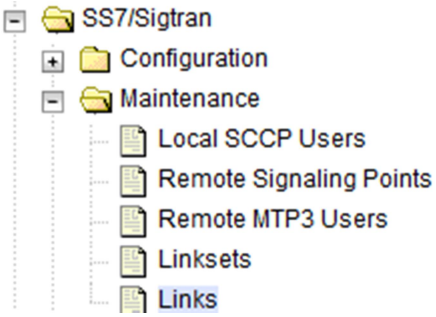
Procedure 3: Recovery Scenario 3

68 ☐	**SOAM VIP GUI:** Verify the Connections Info (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Configuration->Connections**  Verify that all the connections are shown.
69 ☐	**MP Servers:** Disable SCTP Auth Flag (DSR Only)	**DSR Only, SDS Skip This Step** For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [12] Execute this procedure on all Failed MP Servers.
70 ☐	**SOAM VIP GUI:** Enable Connections if needed (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Maintenance->Connections**  Select each connection and click on the **Enable** button. Alternatively you can enable all the connections by selecting the **EnableAll** button.  Verify that the Operational State is Available. **Note:** If a Disaster Recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution

Procedure 3: Recovery Scenario 3

71 ☐	**SOAM VIP GUI:** Enable Optional Features (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Select the optional feature application configured in **step 60** Click the **Enable** button. 
71 ☐	**SOAM VIP GUI:** Re-enable Transports if Needed (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Transport Manager -> Maintenance -> Transport**  Select each transport and click on the **Enable** button  Verify that the Operational Status for each transport is Up.

Procedure 3: Recovery Scenario 3

73 ☐	**SOAM VIP GUI:** Re-enable MAPIWF application if needed(DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users**  Click on the **Enable** button corresponding to MAPIWF Application Name.  Verify that the SSN Status is Enabled.
74 ☐	**SOAM VIP GUI:** Re-enable links if needed (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->SS7/Sigtran->Maintenance->Links**  Click on **Enable** button for each link.  Verify that the Operational Status for each link is Up.

Procedure 3: Recovery Scenario 3

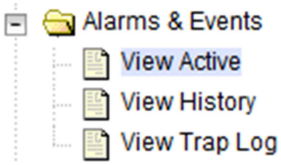
75 ☐	**NOAM VIP:** Verify all servers in Topology are accessible (RADIUS Only)	**If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)**
		Establish an SSH session to the NOAM VIP. Login as ***admusr.***
		Execute following commands to check if all the servers in the Topology are accessible :
		`$ ./usr/TKLC/dpi/bin/sharedKrevo –checkAccess`
		Output Example:
		`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 of the servers are not accessible, stop and contact Appendix K. My Oracle Support (MOS)

Procedure 3: Recovery Scenario 3

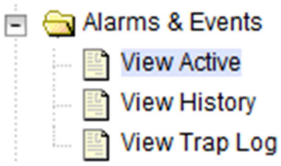
76 ☐	**SOAM VIP:** Copy key file to all the servers in Topology (RADIUS Only)	**If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)**
		
		Establish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

Procedure 3: Recovery Scenario 3

77 ☐	**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)**
		Establish an SSH session to any of the Active NOAM. Login as admusr.
		Execute following command to copy the key file to all the servers in the Topology :
		$ ./sharedKrevo –synchronize
		`[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.`
		$ ./sharedKrevo –updateData
		`[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'`

78 ☐	**SOAM VIP GUI:** Examine All Alarms	Navigate to **Main Menu->Alarms & Events->View Active**  Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix K. My Oracle Support (MOS)**.

Procedure 3: Recovery Scenario 3

79 ☐	**NOAM VIP GUI:** Examine All Alarms	Login to the NOAM VIP if not already logged in. Navigate to **Main Menu->Alarms & Events->View Active**  Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix K. My Oracle Support (MOS)**.
80 ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**. Database Backup to back up the Configuration databases:
81 ☐	**Recover IDIH** (If Configured)	If any components of IDIH were affected, refer to **Section 7.0** to perform the disaster recovery on IDIH.
82 ☐	**SNMP Workaround**	Refer to **Appendix H**. SNMP Configuration to configure SNMP as a workaround in the following cases: 1) If SNMP is not configured in DSR/SDS 2) If SNMP is already configured and **SNMPv3** is selected as enabled version

5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)

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

Recover **Standby NOAM** server by recovering 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.

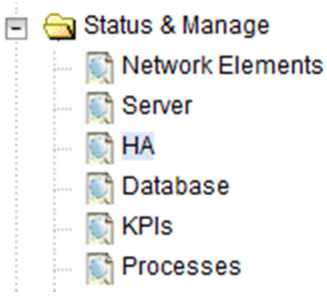
- Recover the base hardware.
- Recover the software.

Recover IDIH if necessary

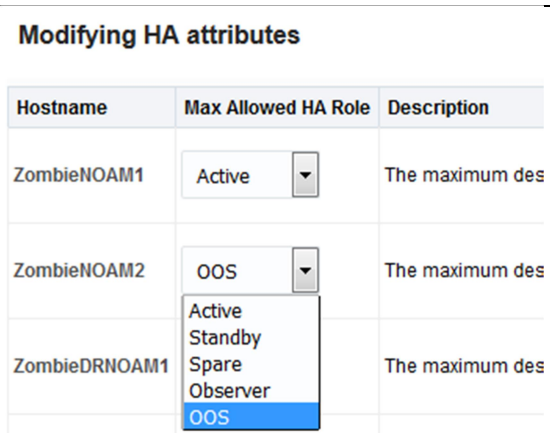
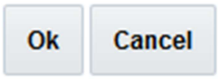
Procedure 4: Recovery Scenario 4

S T E P #	This procedure performs recovery if at least 1 NOAM server is intact and available and 1 SOAM server is intact and available. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Workarounds**	Refer to Appendix G. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure. Refer to **Appendix H**. SNMP Configuration to configure SNMP as a workaround in the following cases: 1) If SNMP is not configured in DSR/SDS 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 **Section 3.1** Required Materials
3. ☐	**NOAM VIP GUI:** Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:

Procedure 4: Recovery Scenario 4

		
4. ☐	**Active NOAM:** Set Failed Servers to OOS	Navigate to **Main Menu -> Status & Manage -> HA**  Select **Edit**

Procedure 4: Recovery Scenario 4

		 Set the Max Allowed HA Role drop down box to **OOS** for the failed servers. Select **Ok** 
5. ☐	**Replace Failed Equipment**	HW vendor to replace the failed equipment
6. ☐	**Recover PMAC TVOE Host (If Required):** 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:** *"Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings"* • **HP DL380 Gen9:** *"Configure HP Gen9 Server BIOS Settings"* 2. Verify and/or upgrade server firmware by executing procedure *"Upgrade Rack Mount Server Firmware"* from reference [8]
7. ☐	**Recover PMAC and PMAC TVOE Host:** Backup Available	**If the PMAC is located on the failed rack mount server(s), execute this step. Otherwise skip to step 10.** This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, **skip this step**. 1. Restore the TVOE backup by executing **Appendix E**. Restore TVOE Configuration from Backup Media 2. on **ALL** failed rack mount serversRestore the PMAC backup by executing **Appendix F**. Restore PMAC from Backup

Procedure 4: Recovery Scenario 4

		Proceed to Step 10
8. ☐	**Recover PMAC and PMAC TVOE Host:** Backup Not Available	**If the PMAC is located on the failed rack mount server(s), execute this step. Otherwise skip to step 10.** This step assumes that TVOE and PMAC backups Are NOT available, if the TVOE and PMAC have already been restored, **skip this step** 1. Execute section *"Install and Configure TVOE on First RMS (PMAC Host)"* from reference [8] 2. Execute section *"Install PMAC"* from reference [8] 3. Execute section *"Initialize the PMAC Application"* from reference [8] **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 sections *"Configure PMAC Server (NetBackup Only)"* and *"Add RMS to the PMAC Inventory"* from reference [8]
10. ☐	**Install/Configure Additional Rack Mount Servers**	**Note:** If TVOE backups are available refer Appendix E. Restore TVOE Configuration from Backup Media otherwise execute this below 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 procedure *"Install TVOE on Additional Rack Mount Servers"* from reference [8] 2. Execute *"Configure TVOE on Additional Rack Mount Servers"* from reference [8] 3. 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:** *"Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings"* • **HP DL380 Gen9:** *"Configure HP Gen9 Server BIOS Settings"*
11. ☐	**Determine VM Placement and Socket Pinning** (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only)	**HP DL380 GEN 8 SKIP THIS STEP** Determine the VM placement and Pinning for proper VM placement and pinning. Refer 12 for workbook reference

Procedure 4: Recovery Scenario 4

12. ☐	**Deploy Redundant PMAC (if required)**	Refer to procedure *"Deploy Redundant PMAC (Optional)"* to re-deploy and configure any redundant PMACs previously configured.
13. ☐	**PMAC: Determine if an fdconfig file exists from the initial deployment.**	Determine whether the fdconfig backup file exists: [admusr@melbourne-pmac-1 ~]$ ll /usr/TKLC/smac/etc/fdc/ Examine the results and verify whether the rms config file <hostname>.cfg exists Note: There may be multiple fdconfig backup files here with respect to each RMS. Select the respective one according to the RMS.
14. ☐	**If FDCONFIG backup file does NOT exist:**	**Execute this step ONLY If the fdconfig backup file does NOT exist:** If the fdconfig file does NOT exist : Create the needed file(s) by executing section "Virtual Machine/Network Fast Deployment" from reference [8] **WARNING:** It is very important to ensure the file(s) created only affect the TVOE server(s) and its 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** **[If fdc backup file exists]:** **Load ISOs into PMAC if not done already**	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:** If the DSR, SDS, and TPD ISOs are NOT loaded in to the PMAC: Execute procedures 14 of section "Virtual Machine/Network Fast Deployment" from reference [8] If already loaded into PMAC, skip this step.
16. ☐	**PMAC** **[If fdc backup file exists]:** Edit/Update Configuration File	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:** **Edit the fdconfig file to include only the required/failed servers.** **Note:** Comment out configuration items that are not needed. **Note:** It is recommended that a separate configuration file be created for **EACH** rack mount server being deployed. Note:Cabinet ID in the config file needs to match the cabinet already defined in PM&C" The following items are mandatory: • siteName

Procedure 4: Recovery Scenario 4

		• 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) • SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured) • SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured) • SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured) • SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured) **Note:** Refer to **Appendix R: VM Automation Profile Values** for DSR and SDS profile values with the configuration file from reference [8] Note: Comment out SDS and DSR profile items if corresponding products are not used. **Note: [Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/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] **Note:** The VM names should not be modified in the .cfg file. The names are fixed and will be prefixed in the siteName. **Note:** The VM locations should not be changed from their 'RMSx' format. Each RMS should correspond with a separate Rack Mount Server. **WARNING**: It is very important to ensure the file(s) created only affect the TVOE server(s) and its 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** **[If fdc backup file exists]:** Copy the located backedup fdc file to the RMS directory	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:** Copy the located fdconfig backup file to the RMS directory: `$ cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file> /usr/TKLC/smac/etc/RMS/`
18.	**PMAC[If fdc backup file exists**	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:**

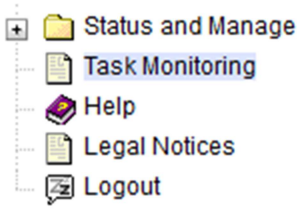
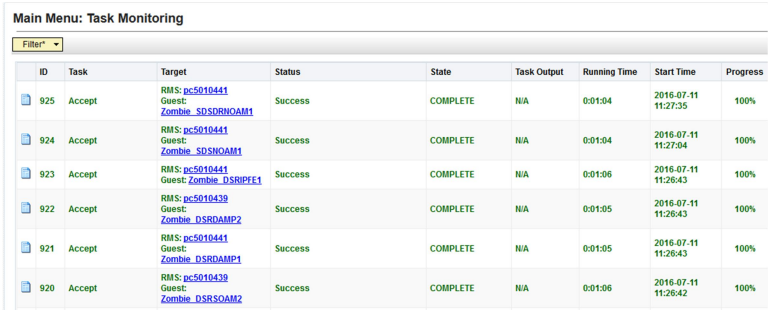
Procedure 4: Recovery Scenario 4

☐	**]:**
	
	Execute the config.sh script
		Execute config.sh against the modified back up config file defined above:
		
		Note: If the below command is executed on multiple cfg files, it will overwrite the existing xml file. It is recommended to rename the xml file before running the below command again.
		$ sudo ./config.sh <config file>
		
		Sample 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]$`

19. ☐	**PMAC** **[If fdc backup file exists]:**	**<u>Execute this step ONLY If the fdconfig backup file exists and located at step 13:</u>** With the file generated from the config.sh script, execute the following command to start fast deployment:

Procedure 4: Recovery Scenario 4

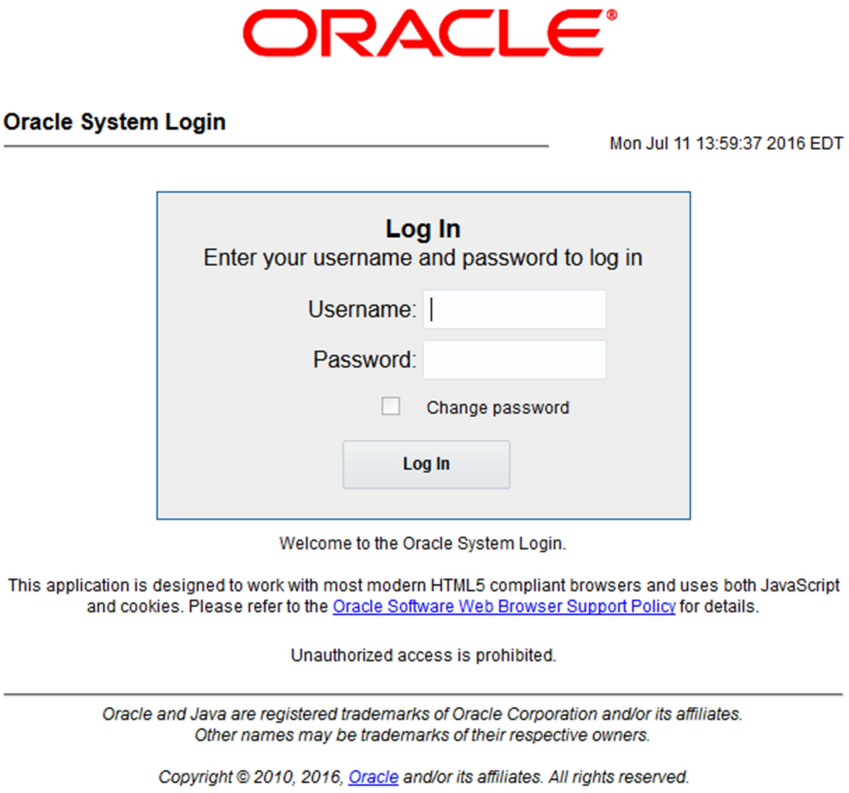
	Execute Fast Deployment	`$ screen`
		
		`$ sudo fdconfig config --file=<fd_config.xml>`
		
		Note: This is a long duration command. If the screen command was run prior to executing the fdconfig, perform a *"screen -dr"* to resume the screen session in the event of a terminal timeout etc.

20. ☐	**PMAC GUI** **[If fdc backup file exists]:** Monitor the Configuration	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:** If not already done so, establish a GUI session on the PMAC server. Navigate to **Main Menu -> Task Monitoring**  Monitor the configuration to completion:  **Note:** Should a failure occur with fdconfig, logs can be accessed in /var/TKLC/log/fdconfig/fdconfig.log [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 ----------

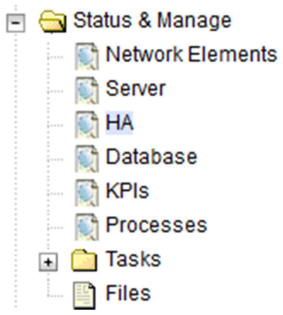
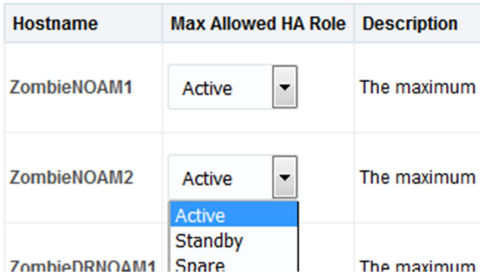
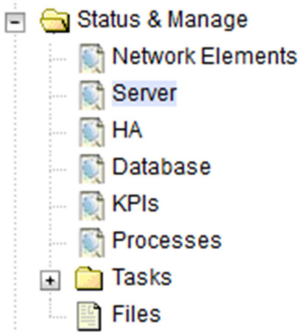
Procedure 4: Recovery Scenario 4

		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 Run Below command to restart the fdconfig after a failure has occurred and has been resolved: `$ sudo fdconfig restart --file=deploy_melbourne_20170329T202458_701b.fdcdb`
21. ☐	**PMAC** **[If fdc backup file exists]:** Repeat for each Rack mount server configuration file	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:** Repeat **steps 13-20** for each rack mount server/configuration file located at step **13**, if required.
22. ☐	**PMAC** **[If fdc backup file exists]:** Backup FDC file	**Execute this step ONLY If the fdconfig backup file exists and located at step 13:** Create the fdc directory so that the fdc file is backed up by PMAC: Issue the following commands: Copy the updated fdc file to the fdc backup directory: **`$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> /usr/TKLC/smac/etc/fdc/`** Change permissions: **`$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/<fdc_file>`**

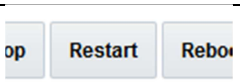
Procedure 4: Recovery Scenario 4

23. ☐	**Perform CPU Pinning**	Configure VM CPU socket pinning on each TVOE host to optimize performance by executing procedure *"CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only)"* from reference [8]
24. ☐	**NOAM VIP GUI:** Login	**If the failed server(s) are NOT OAM type, skip to step 34** Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 
25. ☐	**NOAM VIP GUI:** Recover Standby NOAM (If needed)	Install the second NOAM server if needed: **DSR:** Execute procedure *"Configure the Second NOAM Server"*, steps 1, 3-6 from reference [8] **SDS:** Execute procedure *"Configure the Second SDS NOAM Server"*, steps 1, 3-6 from reference [8]

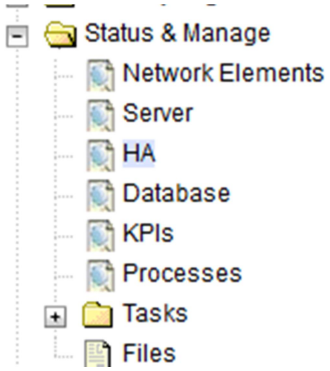
Procedure 4: Recovery Scenario 4

26. ☐	**Install NetBackup Client (Optional)**	If NetBackup is used execute procedure *"Install NetBackup Client (Optional)"* from reference [8]
27. ☐	**NOAM VIP GUI:** Set HA on Standby NOAM	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Select the standby NOAM server, set it to **Active** **Modifying HA attributes**  Press **OK**
28. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered standby NOAM server and click on **Restart**.

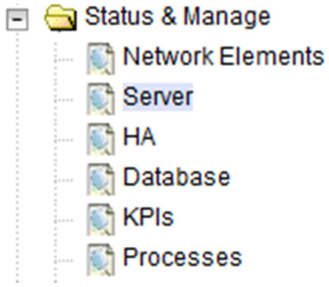
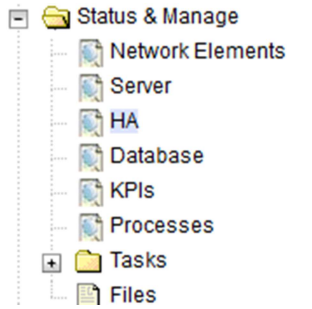
Procedure 4: Recovery Scenario 4

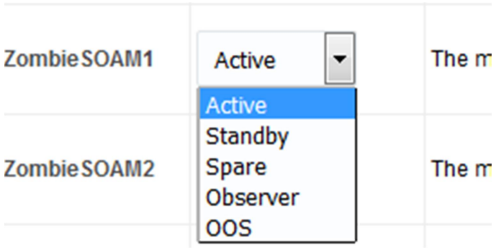
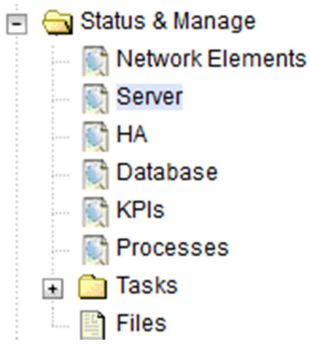
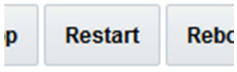
29. ☐	**Active NOAM:** Correct the RecognizedAuthority table	Establish an SSH session to the active NOAM, login as ***admusr***.
		
		Execute the following command:
		
		`$ sudo top.setPrimary`
		`- Using my cluster: A1789`
		`- New Primary Timestamp: 11/09/15 20:21:43.418`
		`- Updating A1789.022: 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

30. ☐	**NOAM VIP GUI:** Recover Query Servers	**SDS Only, DSR Skip This Step** Execute procedure *"Configuring SDS Query Servers",* steps 1, 4-7 from reference [8]
31. ☐	**SDS NOAM VIP GUI:** Set HA on Query Server	**SDS Only, DSR Skip This Step** Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Select the Query server, set it to **Observer**  Press **OK**
32.	**SDS NOAM VIP GUI:** Restart SDS	**SDS Only, DSR Skip This Step**

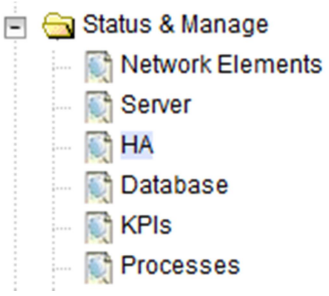
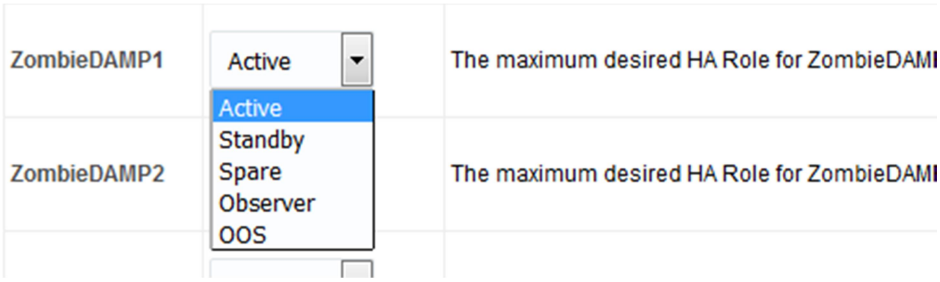
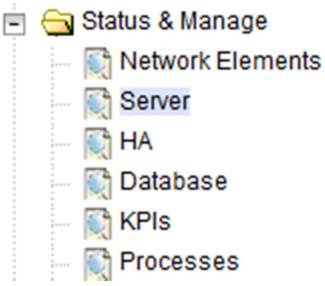
Procedure 4: Recovery Scenario 4

☐	application	Navigate to **Main Menu->Status & Manage->Server**  Select the recovered Query server and click on **Restart**. 
33. ☐	**NOAM VIP GUI:** Recover SOAM Servers	Recover the SOAM servers (**Standby, Spare**-*Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only*) **DSR:** Execute procedure *"Configure the SOAM Servers"*, steps 1-3, and 5-9 from reference [8] **Note:** If you are using NetBackup, also execute step 12 of procedure *"Configure the SOAM Servers"* from reference [8]. **SDS:** Execute procedure *"Configure the SDS DP SOAM Servers"*, steps 1-3, and 5-8 from reference [8]
34. ☐	**NOAM VIP GUI:** Set HA on Standby SOAM	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen

Procedure 4: Recovery Scenario 4

		Select the SOAM server, set it to **Active**  Press **OK**
35. ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered SOAM server and click on **Restart**. 
36. ☐	**(PCA Only) Activate PCA Feature**	If you have PCA installed in the system being recovered, execute the procedure "*PCA Activation on Stand By NOAM network*" on recovered StandBy NOAM Server and procedure "*PCA Activation on Stand By SOAM network*" on recovered StandBy SOAM Server from [7] to re-activate PCA.
37. ☐	**NOAM VIP GUI:** Recover the C-Level Server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs	Recover C-Level Servers: **DSR:** Execute procedure *"Configure the MP Servers"*, Steps 1, 9-13 from reference [8] **Note:** Execute steps 14-16 of *"Configure the MP Servers"*, from reference [8] if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.

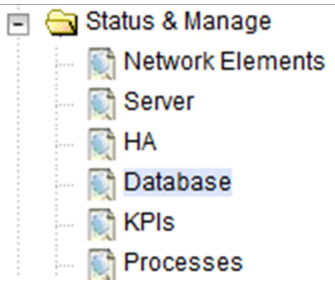
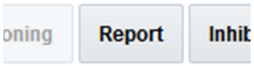
Procedure 4: Recovery Scenario 4

		SDS (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only): Execute procedure *"Configure the SDS DP Servers"*, Steps 1, 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	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen For each server whose Max Allowed HA Role is set to OOS, set it to **Active**  Press **OK**
39. ☐	**NOAM VIP GUI:** Restart DSR Application on recovered C-Level Servers.	Navigate to **Main Menu->Status & Manage->Server**  Select the recovered C-Level servers and click on **Restart**.

Procedure 4: Recovery Scenario 4

		
40. ☐	**ACTIVE NOAM:** Perform key exchange between the active-NOAM and recovered servers.	Establish an SSH session to the Active NOAM, login as ***admusr.*** Execute the following command to perform a keyexchange from the active NOAM to each recovered server: `$ keyexchange admusr@<Recovered Server Hostname>` **Note:** If an export server is configured, perform this step.
41. ☐	**ACTIVE NOAM:** Activate Optional Features	**DSR Only, if SDS, Skip This Step** Establish an SSH session to the active NOAM, login as ***admusr.*** **Note For PCA Activation:** If you have PCA installed in the system being recovered, execute the procedure "*PCA Activation on Stand By NOAM* server" on recovered StandBy NOAM Server and procedure "*PCA Activation on Stand By SOAM server*" on recovered StandBy SOAM Server from [6] to re-activate PCA. **Note:** If not all SOAM sites are recovered at this point, then you should repeat activation for each *new* SOAM site that comes online. **Note**: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature. Refer to **Section** 1.5 Optional **Features** to activate any features that were previously activated. **Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: *iload#31000{S/W Fault}*
42. ☐	**MP Servers:** Disable SCTP Auth Flag (DSR Only)	**DSR Only, SDS Skip This Step** For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [8] Execute this procedure on all Failed MP Servers.
43. ☐	**NOAM VIP GUI:** Fetch and Store the database Report for	Navigate to **Main Menu -> Status & Manage -> Database**

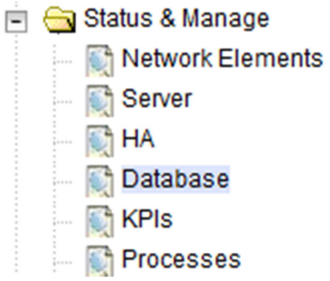
Procedure 4: Recovery Scenario 4

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

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

Procedure 4: Recovery Scenario 4

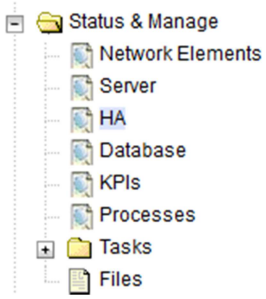
		``
		Oahu-DAMP-1 -- Active
		  BC From Oahu-SOAM-2 Active 0 0.50 ^0.15%cpu 25B/s A=me
		  CC To Oahu-DAMP-2 Active 0 0.10 0.14%cpu 25B/s A=me
		Oahu-DAMP-2 -- Stby
		  BC From Oahu-SOAM-2 Active 0 0.50 ^0.11%cpu 31B/s
		A=C3642.212
		  CC From Oahu-DAMP-1 Active 0 0.10 ^0.14 1.16%cpu 31B/s
		A=C3642.212
		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
		``

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

Procedure 4: Recovery Scenario 4

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

46. ☐	**NOAM VIP GUI:** Verify the HA Status	Click on **Main Menu->Status and Manage->HA**



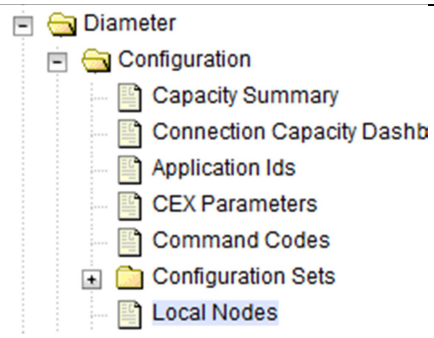
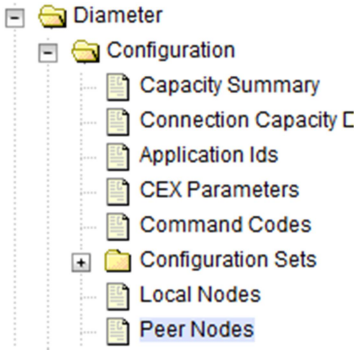
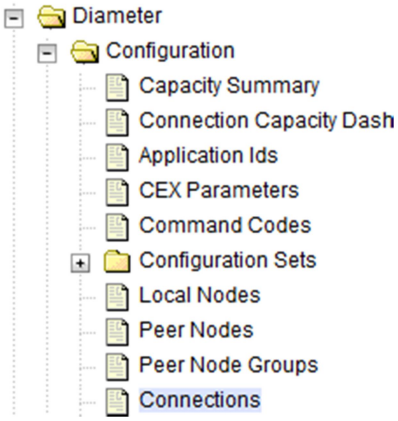
Select the row for all of the servers

Verify that the “HA Role” is either “Active” or “Standby”.

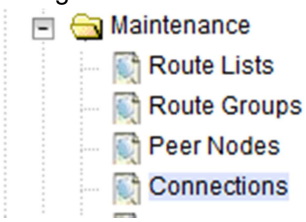
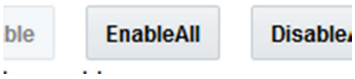
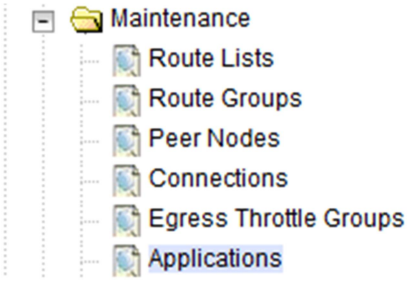
Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role
ZombieNOAM1	Active	N/A	Active
ZombieNOAM2	Standby	N/A	Active
ZombieDRNOAM1	Active	N/A	Active
ZombieDRNOAM2	Standby	N/A	Active
ZombieSOAM1	Active	N/A	Active
ZombieSOAM2	Standby	N/A	Standby

47. ☐	**SOAM VIP GUI:** Verify the Local Node Info (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Configuration->Local Node**

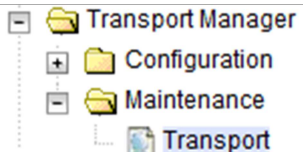
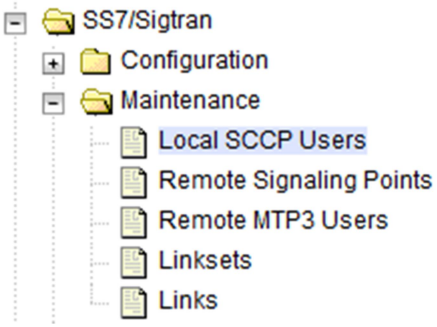
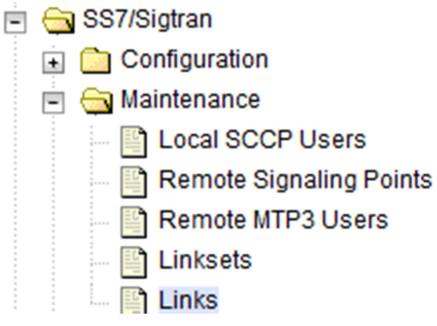
Procedure 4: Recovery Scenario 4

		 Verify that all the local nodes are shown.
48. ☐	**SOAM VIP GUI:** Verify the Peer Node Info (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.
49. ☐	**SOAM VIP GUI:** Verify the Connections Info (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Configuration->Connections** 

Procedure 4: Recovery Scenario 4

		Verify that all the connections are shown.
50. ☐	**SOAM VIP GUI:** Enable Connections if needed (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Diameter->Maintenance->Connections**  Select each connection and click on the **Enable** button. Alternatively you can enable all the connections by selecting the **EnableAll** button.  Verify that the Operational State is Available. **Note:** If a Disaster Recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution
51. ☐	**SOAM VIP GUI:** Enable Optional Features (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Select the optional feature application configured in **step 60** Click the **Enable** button. 
52. ☐	**SOAM VIP GUI:** Re-enable Transports if Needed (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->Transport Manager -> Maintenance -> Transport**

Procedure 4: Recovery Scenario 4

		 Select each transport and click on the **Enable** button  Verify that the Operational Status for each transport is Up.
53. ☐	**SOAM VIP GUI:** Re-enable MAPIWF application if needed(DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users**  Click on the **Enable** button corresponding to MAPIWF Application Name.  Verify that the SSN Status is Enabled.
54. ☐	**SOAM VIP GUI:** Re-enable links if needed (DSR Only)	**DSR Only, SDS Skip This Step** Navigate to **Main Menu->SS7/Sigtran->Maintenance->Links**  Click on **Enable** button for each link.

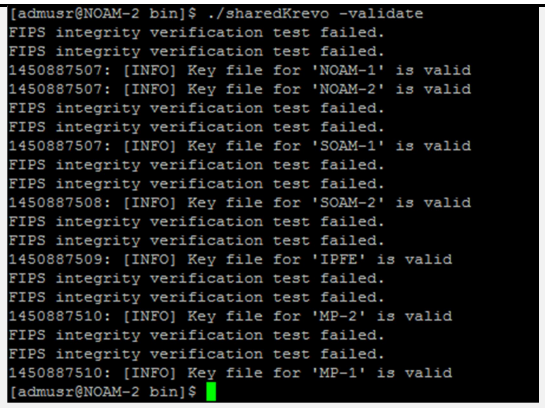
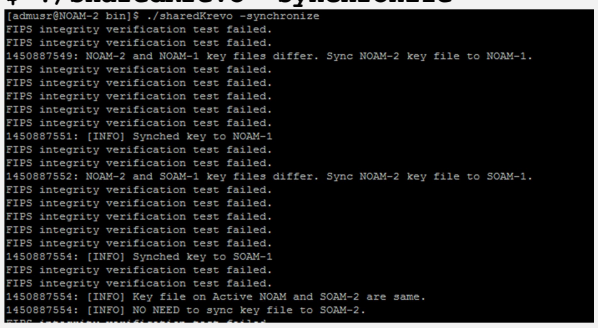
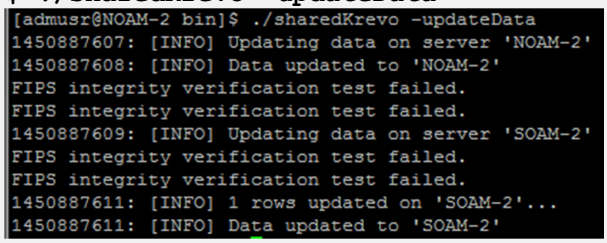
Procedure 4: Recovery Scenario 4

		Enable Disable Verify that the Operational Status for each link is Up.

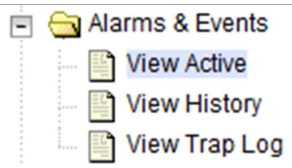
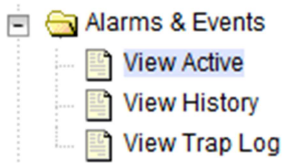
55.
☐
	NOAM VIP: Verify all servers in Topology are accessible (RADIUS Only)	**If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)**
		
		Establish an SSH session to the NOAM VIP. Login as ***admusr.***
		
		Execute following commands to check if all the servers in the Topology are accessible :
		
		`$ cd /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo –checkAccess`
		
		Example Output:
		
		`[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.`
		`FIPS integrity verification test failed.`
		`1450723086: [INFO] 'MP-1' is accessible.`
		`[admusr@NOAM-2 bin]$`
		
		Note: If any of the servers are not accessible, stop and contact Appendix K. My Oracle Support (MOS)

56. ☐	**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)** Execute following commands to check if existing Key file on Active NOAM server is valid : `$ ./sharedKrevo –validate`

Procedure 4: Recovery Scenario 4

		 If output of above command shows that existing key file is not valid then contact Appendix K. My Oracle Support (MOS) Execute following command to copy the key file to all the servers in the Topology : **$ ./sharedKrevo –synchronize**  **$ ./sharedKrevo –updateData** 
57. ☐	**SOAM VIP GUI:** Examine All Alarms	Navigate to **Main Menu->Alarms & Events->View Active**

Procedure 4: Recovery Scenario 4

		 Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix K. My Oracle Support (MOS)**.
58. ☐	**NOAM VIP GUI:** Examine All Alarms	Login to the NOAM VIP if not already logged in. Navigate to **Main Menu->Alarms & Events->View Active**  Examine all active alarms and refer to the on-line help on how to address them. If needed contact **Appendix K. My Oracle Support (MOS)**.

59. ☐	**Restart oampAgent if Needed**	Note: If alarm "10012: The responder for a monitored table failed to respond to a table change" is raised, the oampAgent needs to be restarted.
		Establish an SSH session to each server that has the alarm.
		Login ***admusr***
		Execute the following commands:
		`$ sudo pm.set off oampAgent`
		`$ sudo pm.set on oampAgent`

60. ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**. Database Backup to back up the Configuration databases:
61. ☐	**Recover IDIH** (If Configured)	If any components of IDIH were affected, refer to **Section 7.0** to perform the disaster recovery on IDIH.

5.1.5 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 procedures' detailed steps are in **Procedure 5**. The major activities are summarized as follows:

Switch DR NOAM from secondary to primary

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

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

If applicable, recover any failed SOAM and MP/DP 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/DP 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, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1 ☐	**Workarounds**	Refer to Appendix G. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure. Refer to **Appendix H**. SNMP Configuration to configure SNMP as a workaround in the following cases: 1) If SNMP is not configured in DSR/SDS 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 **Section 3.1** Required Materials**.**
3 ☐	**Switch DR NOAM to Primary**	Refer Document DSR / SDS 8.x NOAM Failover User's Guide, E85595 [13]

Procedure 5: Recovery Scenario 5

4
☐
	Recover System	If **ALL** SOAM servers have failed, execute Procedure 2
		
		If **ALL** NOAM servers have failed, execute the following steps:
		
		1) Procedure 4: *Steps 4-14*
		
		2) Perform a 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 prompted 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, and retry the keyexchange commands.
		
		3) Use the PMAC GUI to determine the control network IP address of the recovered VMs. From the PMAC GUI, navigate to **Main Menu -> Software -> Software Inventroy**
		
		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 prompted 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, and retry the keyexchange commands.
		
		4) Procedure 4: *15-19 (To be performed for each NOAM))*

Procedure 5: Recovery Scenario 5

5 ☐	**Perform Key exchange between Active NOAM and Recovered NOAMs**	Perform a keyexchange between the newly active NOAM and the recovered NOAM servers: From a terminal window connection on the active NOAM as the ***admusr*** user, exchange SSH keys for ***admusr*** between the active NOAM and the recovered NOAM servers using the keyexchange utility, using the host names of the recovered NOAMs. When prompted for the password, enter the password for the ***admusr*** user of the recovered NOAM servers. `$ keyexchange admusr@<Recovered_NOAM Hostname>`
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	**DSR Only, if SDS, Skip This Step** **Map-Diameter Interworking (MAP-IWF) and/or Policy and Charging Application (PCA) Only** Activate the features Map-Diameter Interworking (MAP-IWF) and Policy and Charging Application (PCA) as follows: For **PCA**: 1. Establish SSH sessions to the all the recovered NOAM servers and login as admusr. Refer [7] and execute procedure “PCA Activation on Standby NOAM server” on all recovered NOAM Servers to re-activate PCA. For **MAP-IWF:** ***1.*** Establish SSH session to the recovered active NOAM, login as ***admusr.*** Refer [5] to activate Map-Diameter Interworking (MAP-IWF) **Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored: *iload#31000{S/W Fault}* **Note**: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.

Procedure 5: Recovery Scenario 5

8
☐
	DR-NOAM VIP:
	Copy key file to recovered NOAM servers in Topology (RADIUS Only)
		DSR Only, if SDS, Skip This 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)
		
		Establish an SSH session to any of the Active DR NOAM which is intact and operational. Login as ***admusr***.
		
		Execute following commands to check if existing Key file on Active DR NOAM server is valid :
		
		`$ cd /usr/TKLC/dpi/bin/`
		
		`$ ./sharedKrevo –validate`
		
		Note: If errors are present, stop and contact **Appendix K. My Oracle Support (MOS)**
		
		If key file is valid, Execute following commands to copy Key file from Active DR NOAM server to recovered NOAMs :
		
		`$ ./sharedKrevo -copyKey –destServer <First NOAM>`
		`$ ./sharedKrevo -copyKey –destServer <Second NOAM>`

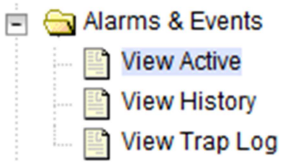
9
☐
	Primary NOAM:
	Modify DSR OAM process
		Establish an SSH session to the primary NOAM, login as ***admusr***.
		
		Execute the following commands:
		
		Retrieve the cluster ID of the recovered NOAM:
		`$ sudo iqt -fClusterID TopologyMapping where "NodeID='<DR_NOAM_Host_Name>'"`
		`Server_ID NodeID ClusterID`
		`1 Oahu-DSR-NOAM-2 A1055`
		
		Execute the following 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 Document DSR / SDS 8.x NOAM Failover User's Guide, E85595 [13]

Procedure 5: Recovery Scenario 5

11 ☐	**NOAM VIP:** Verify all servers in Topology are accessible (RADIUS Only)	**DSR Only, if SDS, Skip This 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)
		
		Establish an SSH session to the NOAM VIP. Login as ***admusr.***
		
		Execute following commands to check if all the servers in the Topology are accessible :
		
		`$ cd /usr/TKLC/dsr/bin/`
		`$ ./sharedKrevo -checkAccess`
		
		Note: If any of the servers are not accessible, stop and contact Appendix K. My Oracle Support (MOS)

12 ☐	**NOAM VIP:** Copy key file to all the servers in Topology (RADIUS Only)	**DSR Only, if SDS, Skip This Step**
		
		Establish an SSH session to the Active NOAM, login as ***admusr***.
		
		Execute following command to copy the key file to all the servers in the Topology :
		
		`$ ./sharedKrevo -synchronize`
		`$ ./sharedKrevo -updateData`
		
		Note: If errors are present, stop and contact Appendix K. My Oracle Support (MOS)

13 ☐	**Recovered Servers:** Verify Alarms	Navigate to **Main Menu -> Alarms & Events -> View Active**  Verify the recovered servers are not contributing to any active alarms (Replication, Topology misconfiguration, database impairments, NTP, etc.)
14 ☐	**Recover IDIH** (If Configured)	If any components of IDIH were affected, refer to **Section 7.0** to perform the disaster recovery on IDIH.

5.1.6 Recovery Scenario 6 (Database Recovery)

5.1.6.1 Recovery Scenario 6: Case 1

For a partial outage with

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

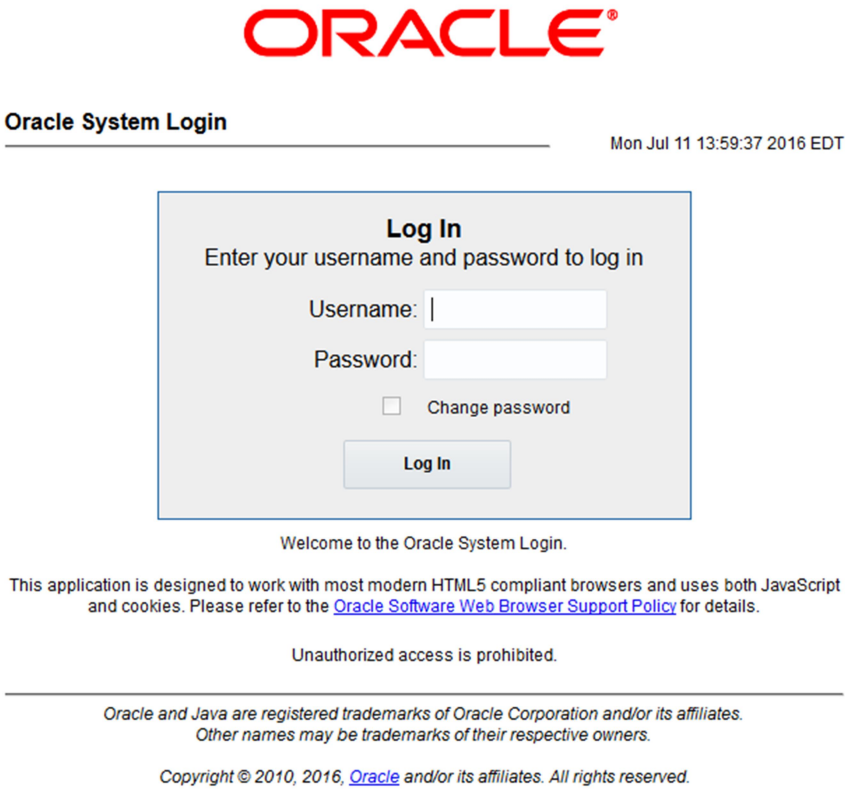
Note: During recovery, the corrupted Database will get replaced by the sever Runtime backup. Any configuration done after taking the backup will not be visible post recovery.

Note: 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.

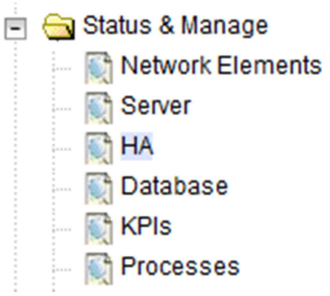
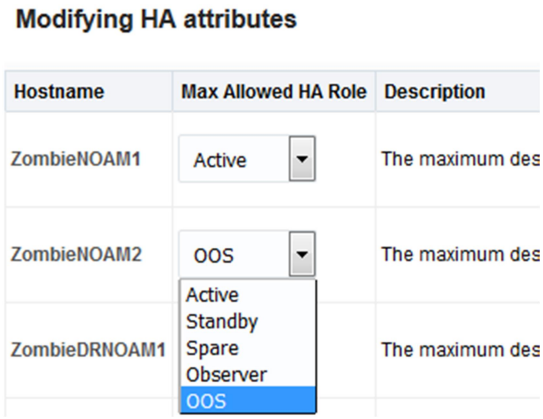
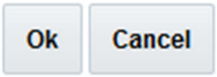
Procedure 6: Recovery Scenario 6 (Case 1)

S T E P #	This procedure performs recovery if database is corrupted in the system Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1 ☐	**Workarounds**	Refer to Appendix G. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.

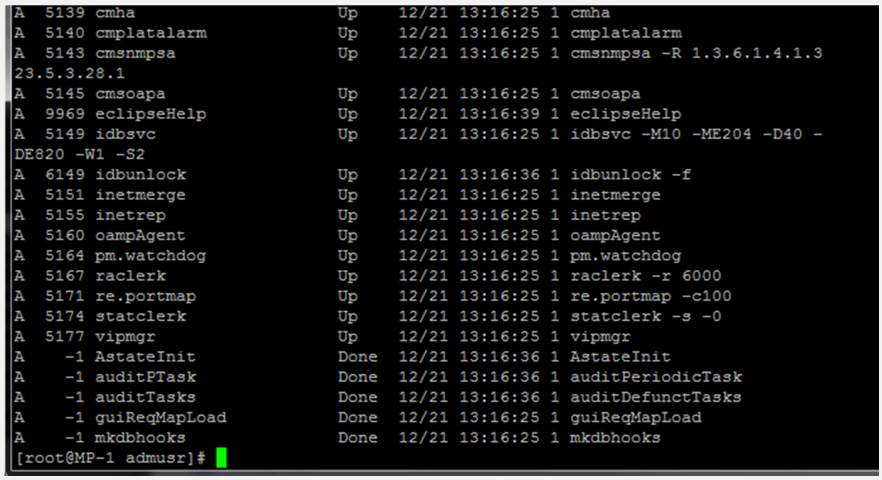
Procedure 6: Recovery Scenario 6 (Case 1)

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

Procedure 6: Recovery Scenario 6 (Case 1)

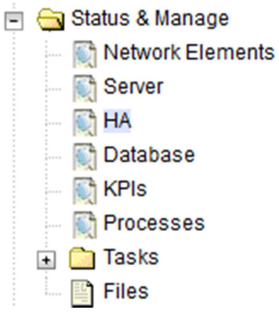
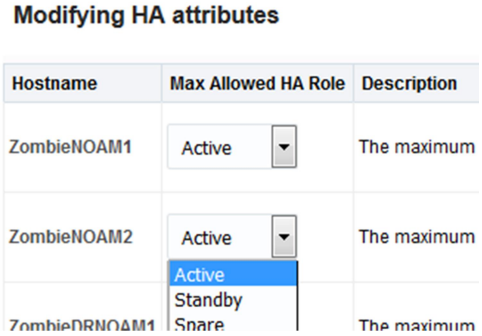
3 ☐	**Active NOAM:** Set Failed Servers to OOS	Navigate to **Main Menu -> Status & Manage -> HA**  Select **Edit**  Set the Max Allowed HA Role drop down box to **OOS** for the failed servers. Select **Ok** 
4 ☐	**Server Being Recovered:** Login	Establish an SSH session to the server in question. Login as ***admusr***
5 ☐	**Server Being Recovered:** Change runlevel to 3	Execute the following command to bring the system to runlevel 3. `$ sudo init 3`
6 ☐	**Server Being Recovered:** Recover System	Execute the following command and follow the instructions appearing the console prompt `$ sudo /usr/TKLC/appworks/sbin/backout_restore`
7 ☐	**Server Being Recovered:** Change runlevel to 4	Execute the following command to bring the system back to runlevel 4. `$ sudo init 6`

Procedure 6: Recovery Scenario 6 (Case 1)

8 ☐	**Server Being Recovered:** Verify the server	Execute the following command to verify if 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 1.3.6.1.4.1.3
23.5.3.28.1
A  5145 cmsoapa                 Up    12/21 13:16:25 1 cmsoapa
A  9969 eclipseHelp             Up    12/21 13:16:39 1 eclipseHelp
A  5149 idbsvc                  Up    12/21 13:16:25 1 idbsvc -M10 -ME204 -D40 -
DE820 -W1 -S2
A  6149 idbunlock               Up    12/21 13:16:36 1 idbunlock -f
A  5151 inetmerge               Up    12/21 13:16:25 1 inetmerge
A  5155 inetrep                 Up    12/21 13:16:25 1 inetrep
A  5160 oampAgent               Up    12/21 13:16:25 1 oampAgent
A  5164 pm.watchdog             Up    12/21 13:16:25 1 pm.watchdog
A  5167 raclerk                 Up    12/21 13:16:25 1 raclerk -r 6000
A  5171 re.portmap              Up    12/21 13:16:25 1 re.portmap -c100
A  5174 statclerk               Up    12/21 13:16:25 1 statclerk -s -0
A  5177 vipmgr                  Up    12/21 13:16:25 1 vipmgr
A    -1 AstateInit              Done  12/21 13:16:36 1 AstateInit
A    -1 auditPTask              Done  12/21 13:16:36 1 auditPeriodicTask
A    -1 auditTasks              Done  12/21 13:16:36 1 auditDefunctTasks
A    -1 guiReqMapLoad           Done  12/21 13:16:25 1 guiReqMapLoad
A    -1 mkdbhooks               Done  12/21 13:16:25 1 mkdbhooks
[root@MP-1 admusr]#
```

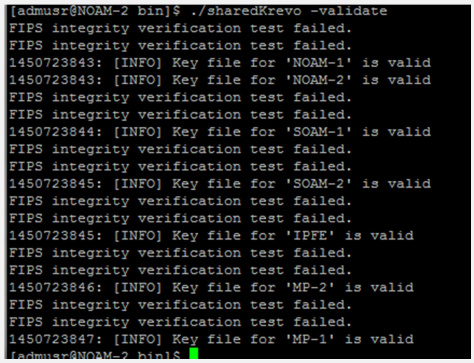
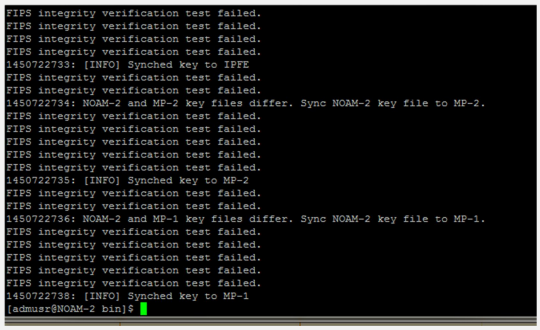
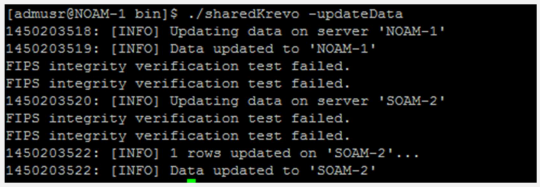
Procedure 6: Recovery Scenario 6 (Case 1)

9 ☐	**NOAM VIP GUI:** Set Failed Servers to Active	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Select the failed server, set it to **Active**  Press **OK**

Procedure 6: Recovery Scenario 6 (Case 1)

10 ☐	**NOAM VIP:** Verify all servers in Topology are accessible (RADIUS Only)	**DSR Only, if SDS, Skip This 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)
		
		Establish an SSH session to the NOAM VIP. Login as ***admusr.***
		
		Execute following commands to check if all the servers in the Topology are accessible :
		
		`$ cd /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo -checkAccess`
		
		`[admusr@NOAM-2 bin]$ ./sharedKrevo -checkAccess`
		`FIPS integrity verification test failed.`
		`1450723797: [INFO] 'NOAM-1' is accessible.`
		`FIPS integrity verification test failed.`
		`1450723797: [INFO] 'SOAM-1' is accessible.`
		`FIPS integrity verification test failed.`
		`1450723797: [INFO] 'SOAM-2' is accessible.`
		`FIPS integrity verification test failed.`
		`1450723798: [INFO] 'IPFE' is accessible.`
		`FIPS integrity verification test failed.`
		`1450723798: [INFO] 'MP-2' is accessible.`
		`FIPS integrity verification test failed.`
		`1450723798: [INFO] 'MP-1' is accessible.`
		`[admusr@NOAM-2 bin]$`

Procedure 6: Recovery Scenario 6 (Case 1)

11 ☐	**NOAM VIP:** Copy key file to all the servers in Topology (RADIUS Only)	**DSR Only, if SDS, Skip This 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)** Execute following commands to check if existing Key file on Active NOAM (The NOAM which is intact and was not recovered) server is valid : **$ ./sharedKrevo -validate**  [admusr@NOAM-2 bin]$ ./sharedKrevo -validate FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723843: [INFO] Key file for 'NOAM-1' is valid 1450723843: [INFO] Key file for 'NOAM-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723844: [INFO] Key file for 'SOAM-1' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723845: [INFO] Key file for 'SOAM-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723845: [INFO] Key file for 'IPFE' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723846: [INFO] Key file for 'MP-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723847: [INFO] Key file for 'MP-1' is valid [admusr@NOAM-2 bin]$ If output of above command shows that the existing key file is not valid, contact Appendix K. My Oracle Support (MOS) Execute following command to copy the key file to all the servers in the Topology : **$ ./sharedKrevo -synchronize**  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**  [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 are present, stop and contact Appendix K. My Oracle Support (MOS)

Procedure 6: Recovery Scenario 6 (Case 1)

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

5.1.6.2 Recovery Scenario 6: Case 2

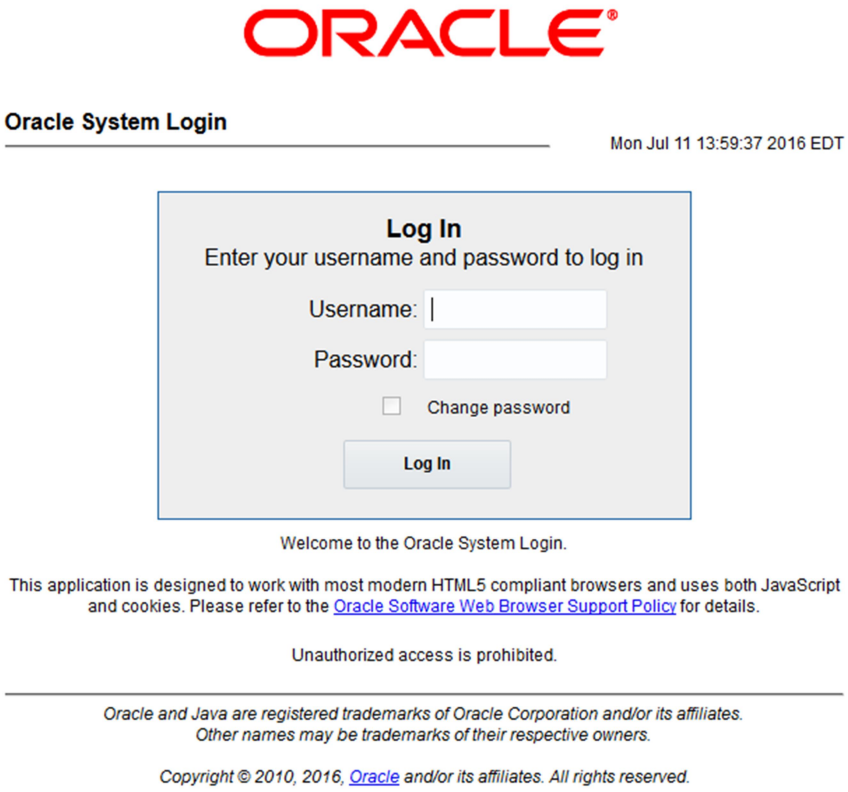
For a partial outage with

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

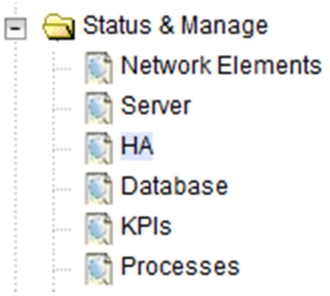
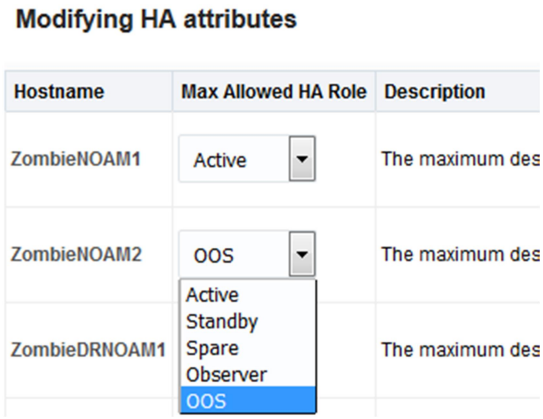
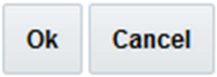
Procedure 7: Recovery Scenario 6 (Case 2)

S T E P #	This procedure performs recovery if database got corrupted in the system and system is in the state to get replicated Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1 ☐	**Workarounds**	Refer to Appendix G. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.

Procedure 7: Recovery Scenario 6 (Case 2)

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

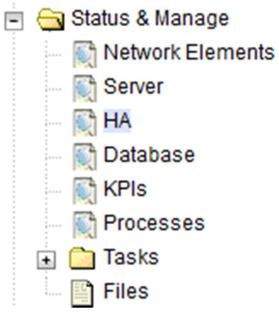
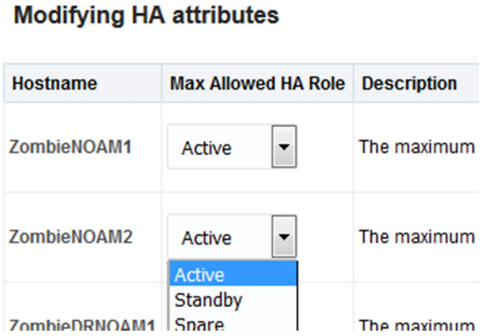
Procedure 7: Recovery Scenario 6 (Case 2)

3 ☐	**Active NOAM:** Set Failed Servers to OOS	Navigate to **Main Menu -> Status & Manage -> HA**  Select **Edit**  Set the Max Allowed HA Role drop down box to **OOS** for the failed servers. Select **Ok** 
4 ☐	**Server in Question:** Login	Establish an SSH session to the server in question. Login as ***admusr***

5 ☐	**Server in Question:** Take Server out of Service	Execute the following command to take the server out of service.
		`$ sudo bash -l`
		`$ sudo prod.clobber`

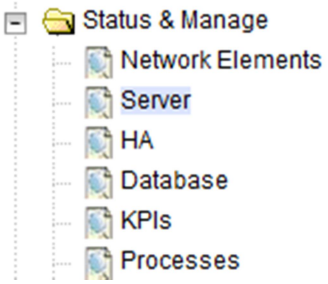
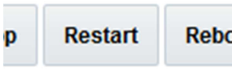
6 ☐	**Server in Question:** Take Server to DbUp State and Start the Application	Execute the following commands to take the server to Dbup and start the DSR application:
		`$ sudo bash -l`
		`$ sudo prod.start`

Procedure 7: Recovery Scenario 6 (Case 2)

7 ☐	**NOAM VIP GUI:** Set Failed Servers to Active	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen Select the failed server, set it to **Active**  Press **OK**

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

Procedure 7: Recovery Scenario 6 (Case 2)

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

10
☐
	NOAM VIP:
	Verify all servers in Topology are accessible (RADIUS Only)
		DSR Only, if SDS, Skip This 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)
		Establish an SSH session to the NOAM VIP. Login as ***admusr.***
		Execute following commands to check if all the servers in the Topology are accessible :
		`$ cd /usr/TKLC/dpi/bin/`
		`$ ./sharedKrevo -checkAccess`

Procedure 7: Recovery Scenario 6 (Case 2)

10 ☐	**NOAM VIP:** Copy key file to all the servers in Topology (RADIUS Only)	**DSR Only, if SDS, Skip This 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)
		
		Execute following commands to 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`
		
		If output of above command shows that the existing key file is not valid, contact Appendix K. My Oracle Support (MOS)
		
		Execute following command to copy the key file to all the servers in the Topology :
		
		`$ ./sharedKrevo -synchronize`
		
		`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`
		
		`[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 are present, stop and contact Appendix K. My Oracle Support (MOS)

Procedure 7: Recovery Scenario 6 (Case 2)

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

6.0 Resolving User Credential Issues after Database Restore

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

6.1 Restoring a Deleted User

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

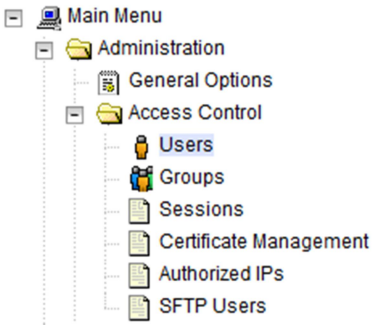
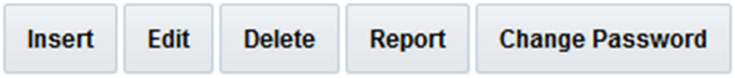
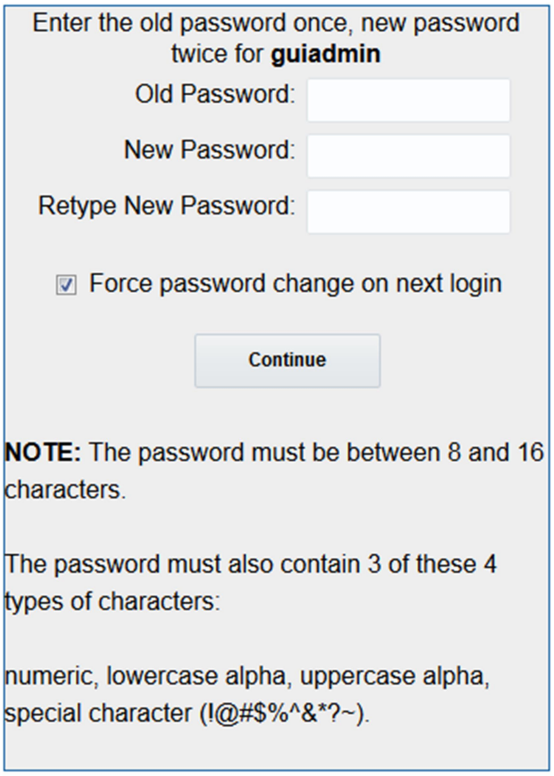
These users were removed prior to creation of the backup and archive file. They will be reintroduced by system restoration of that file.

6.2 Keeping a Restored user

Procedure 8: Keep Restored User

S T E P #		
	Perform this procedure to keep users that will be restored by system restoration. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1 ☐	**Before Restoration:** Notify Affected Users Before Restoration	Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.
2 ☐	**After Restoration:** Login to the NOAM VIP	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

Procedure 8: Keep Restored User

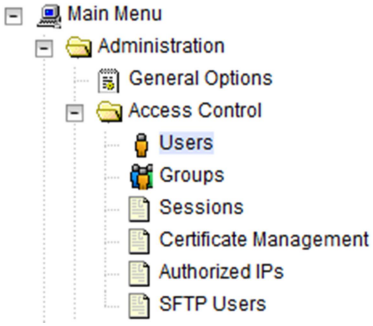
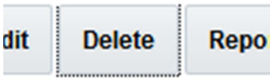
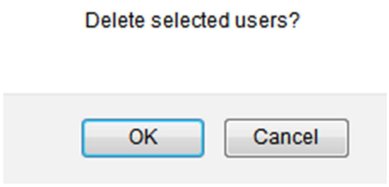
3 ☐	**After Restoration:** Reset User Passwords	Navigate to **Administration -> Access Control -> Users**  Select the user Click the **Change Password** button  Enter a new password  Click the **Continue** button

6.3 Removing a Restored User

Procedure 9: Remove the Restored User

S T E P #		
	Perform this procedure to remove users that will be restored by system restoration Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1 ☐	**After Restoration:** Login to the NOAM VIP	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

Procedure 9: Remove the Restored User

2 ☐	**After Restoration:** Delete User	Navigate to **Administration -> Access Control -> Users**  Select the user Click the **Delete** button   Click the **OK** button to confirm.

6.4 Restoring a Modified User

These users have had a password change prior to creation of the backup and archive file. The will be reverted by system restoration of that file.

```
- The password for user 'testuser' differs between the selected backup file
and the current database.
```

Before Restoration:

Verify that you have access to a user with administrator permissions that is not affected.

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

After Restoration:

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

6.5 Restoring an Archive that does not contain a Current User

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

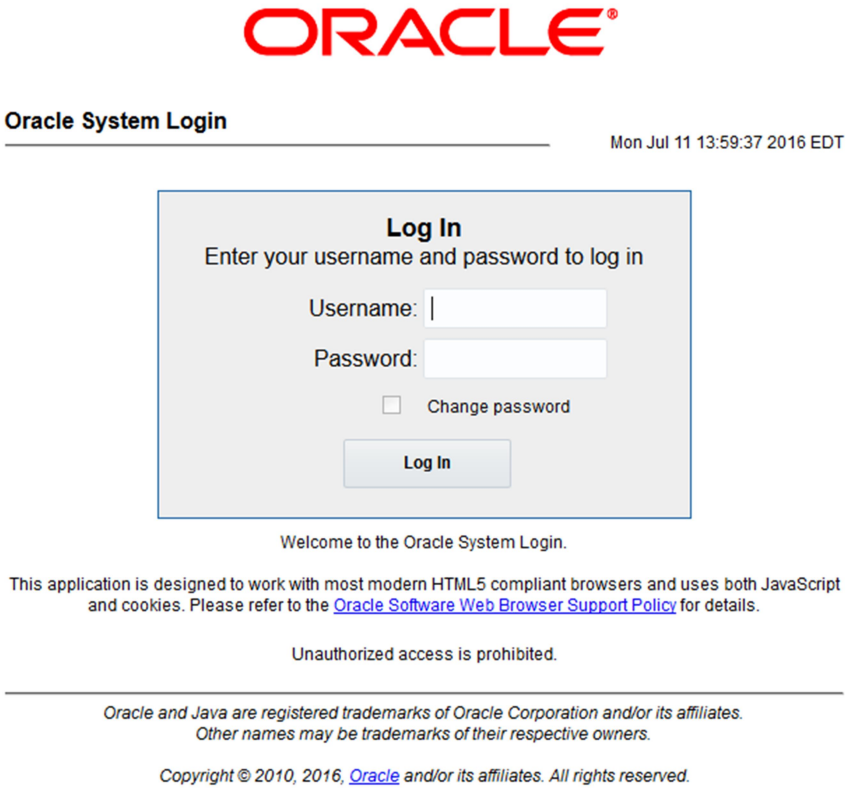
```
- User 'testuser' exists in current database but not in the selected backup
file.
```

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

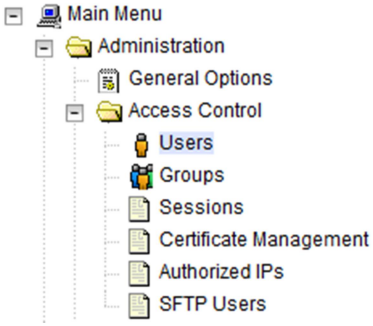
Procedure 10: Restoring an Archive that does not Contain a Current User

S T E P #	Perform this procedure to remove users that will be restored by system restoration Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K. 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.

Procedure 10: Restoring an Archive that does not Contain a Current User

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

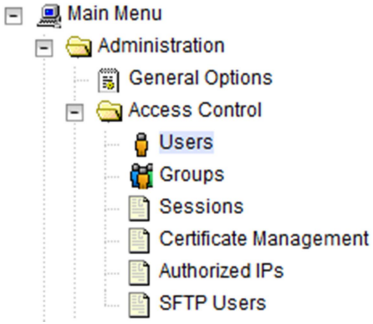
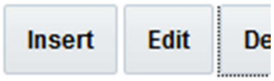
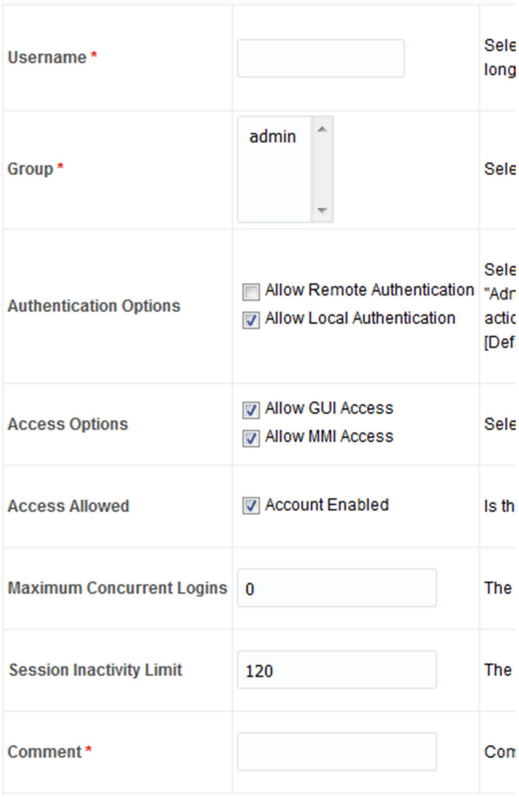
Procedure 10: Restoring an Archive that does not Contain a Current User

3 ☐	**Before Restoration:** Record user settings	Navigate to **Administration -> Access Control -> Users**  Under each affected user, record the following: • Username, • Account status • Remote Auth • Local Auth • Concurrent Logins Allowed • Inactivity Limit • Comment • Groups

Procedure 10: Restoring an Archive that does not Contain a Current User

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

Procedure 10: Restoring an Archive that does not Contain a Current User

5 ☐	**After Restoration:** Recreate affected user	Navigate to **Administration -> Access Control -> Users**  Click **Insert**  Recreate the user using the data collected in **Step 3.** **Adding new user**  Click **Ok**

Procedure 10: Restoring 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.

7.0 IDIH Disaster Recovery

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

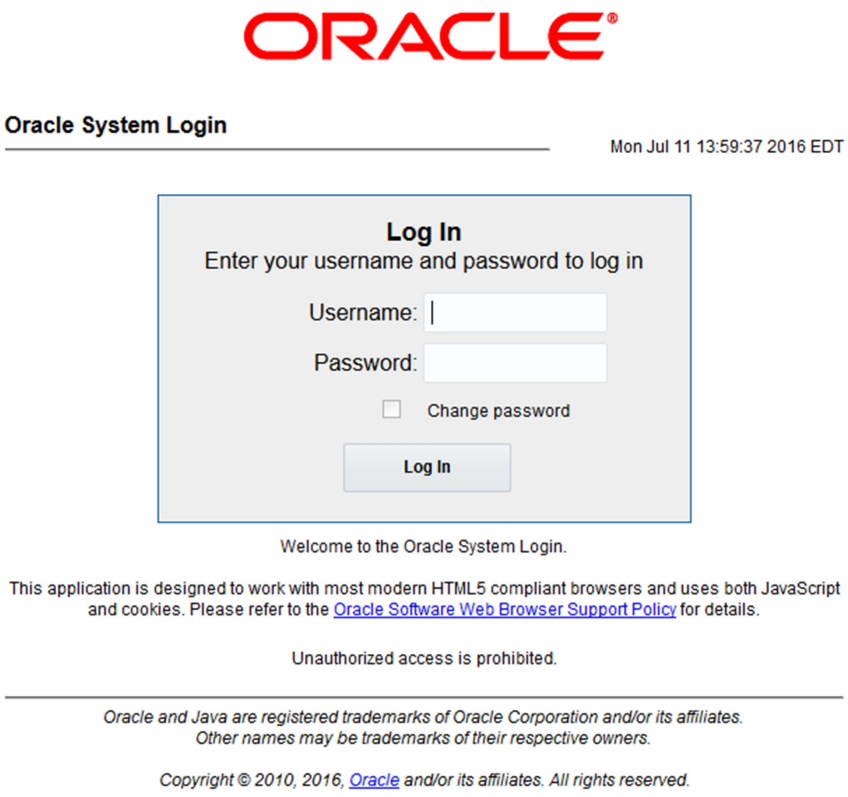
Note: the fdconfig xml file for disaster recovery is exactly the same as the one for upgrade and this file should have been created during the latest upgrade or fresh installation. In case the file is not found, make a copy of the fdconfig.xml file for fresh installation with “-upgrade” between the hostname 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>
```

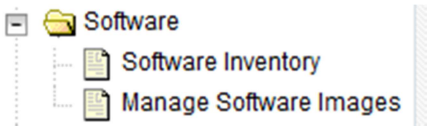
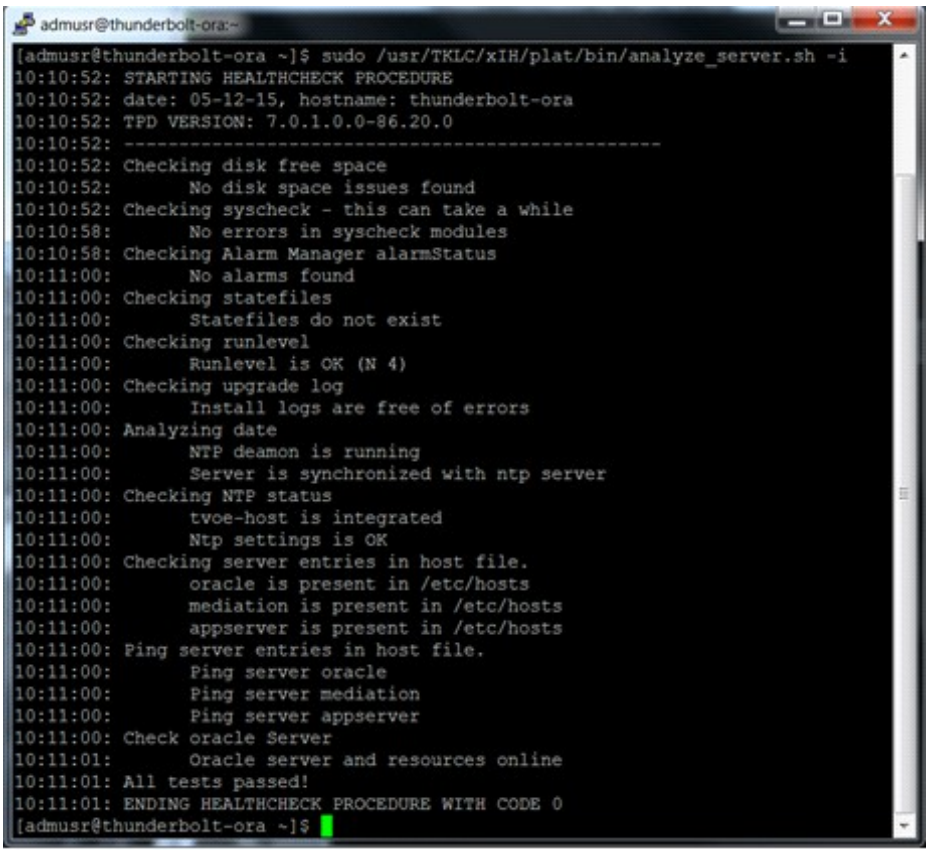
Disaster Recovery Scenarios:

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

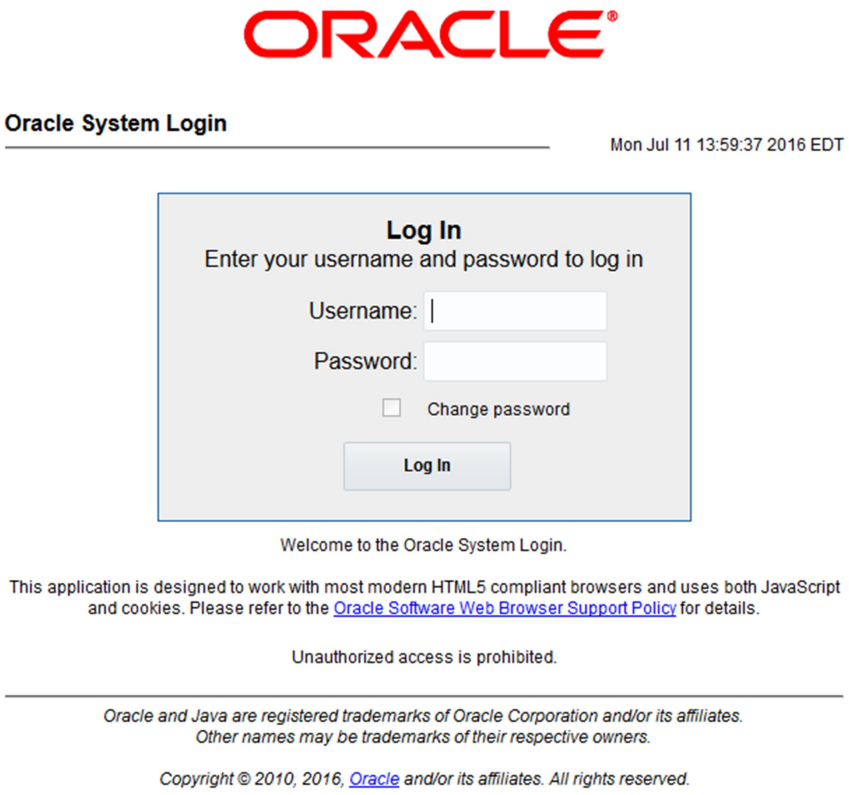
Procedure 11: IDIH Disaster Recovery Preparation

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, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1 ☐	**PMAC GUI:** Login	Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` Login as ***pmacadmin*** user: 

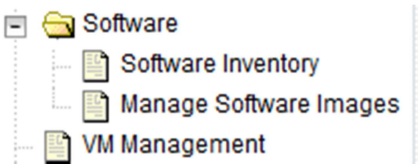
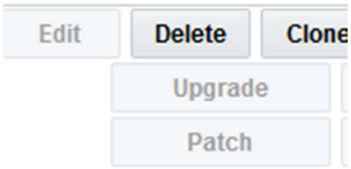
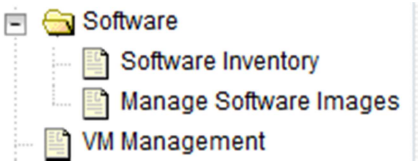
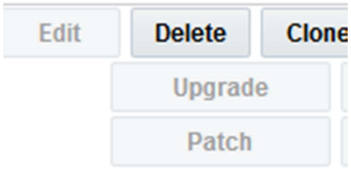
Procedure 11: IDIH Disaster Recovery Preparation

2 ☐	**PMAC GUI:** Verify necessary IDIH images are available	Navigate to **Main Menu -> Software -> Manage Software Images**  Verify the current IDIH **TVOE**, **TPD**, **Oracle**, **Application** and **Mediation** images are listed. 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 please follow the instructions from reference [8].
3 ☐	**Oracle Guest:** Login	Establish an SSH session to the Oracle guest, login as ***admusr***.
4 ☐	**Oracle Guest:** Perform Database Health check	Execute the following command to perform a database health check: `$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i` Output: 

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

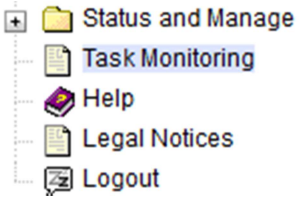
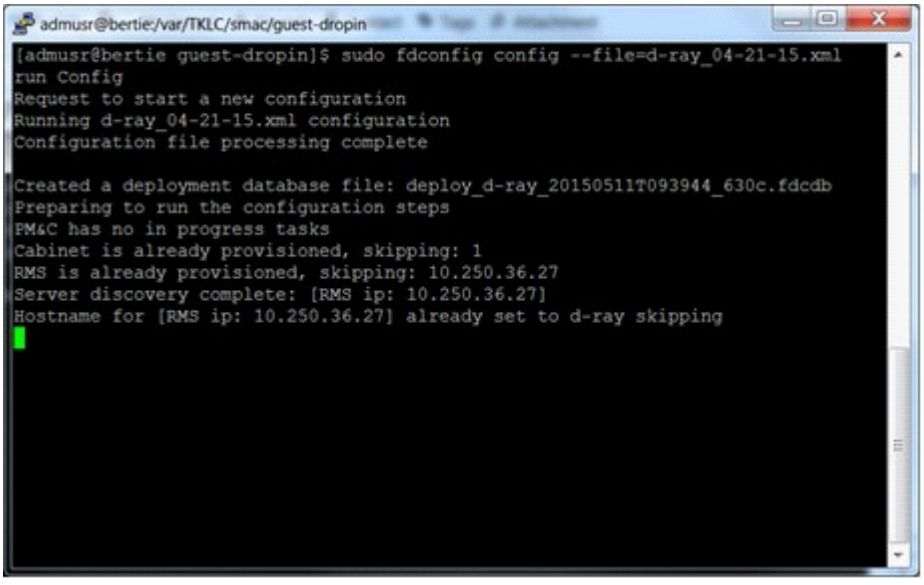
S T E P #	This procedure performs disaster recovery for the IDIH by re-installing the mediation and application servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1 ☐	**PMAC GUI:** Login	Open web browser and enter: `http://<PMAC_Mgmt_Network_IP>` Login as ***pmacadmin*** user: 

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

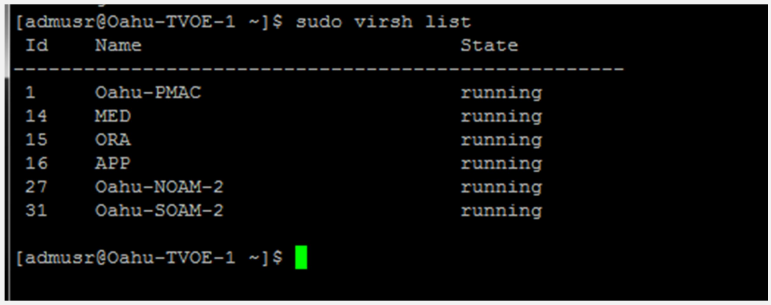
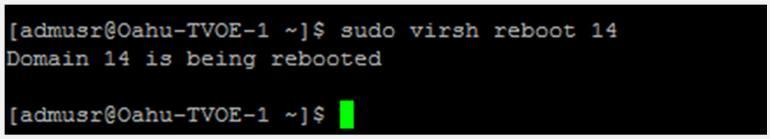
2 ☐	**Remove existing Application Server**	Navigate to **Main Menu -> VM Management**  Select the application guest, Click on the **Delete** button. 
3 ☐	**Remove existing Mediation Server**	Navigate to **Main Menu -> VM Management**  Select the Mediation guest, Click on the **Delete** button. 
4 ☐	**PMAC:** Establish SSH session and Login	Establish an SSH session to the PMAC, login as ***admusr***.

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

5 ☐	**PMAC:** Re-install the Mediation and Application Servers	Execute the following command (Enter your upgrade file) :
		`$ cd /var/TKLC/smac/guest-dropin`
		`$ sudo fdconfig config --file=<hostname-upgrade_xx-xx-xx>.xml`
		 
		Warning: If you run the fdconfig without "upgrade" in the XML filename, the database will be destroyed and you will lose all of the existing data.

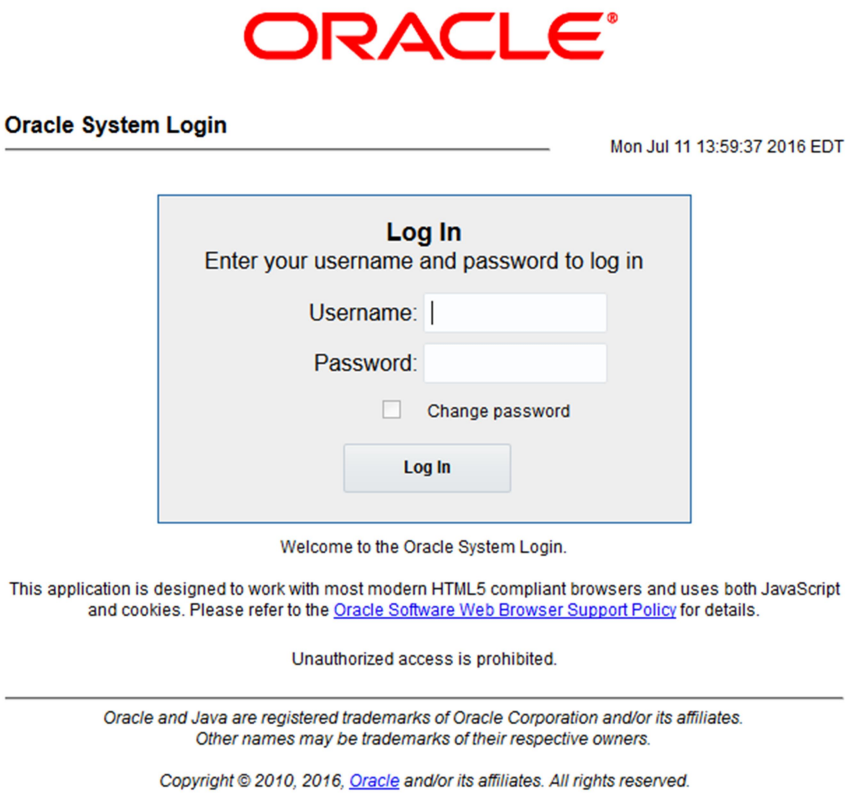
6 ☐	**PMAC GUI:** Monitor the Configuration	If not already done so, establish a GUI session on the PMAC server. Navigate to **Main Menu -> Task Monitoring**  Monitor the IDIH configuration to completion. Alternatively, you can monitor the fdconfig status through the command line after executing the fdconfig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

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

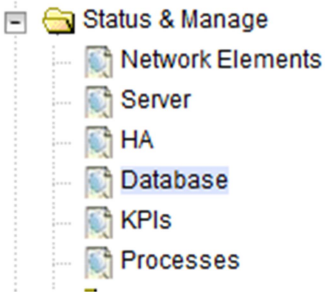
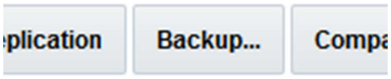
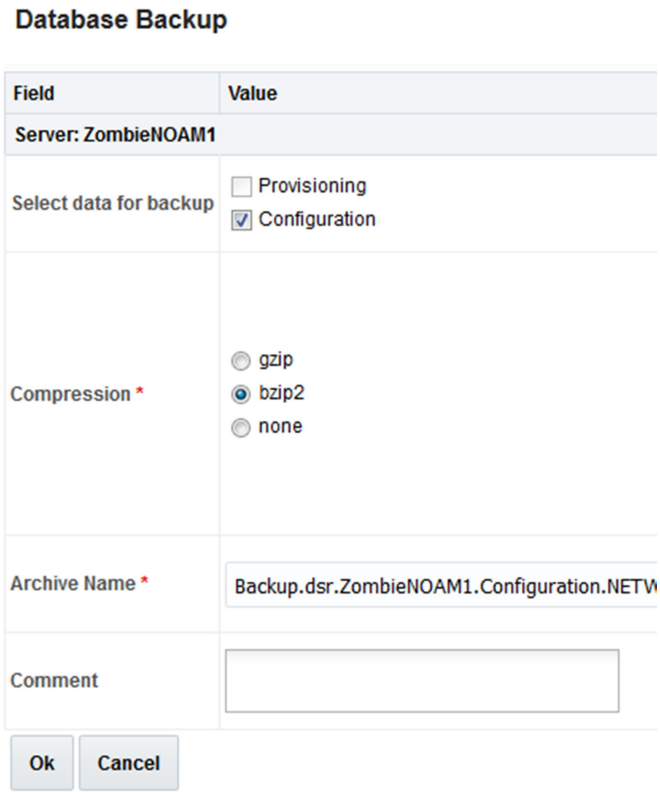
7 ☐	**Perform CPU Pinning**	Configure VM CPU socket pinning on each TVOE host to optimize performance by executing procedure *"CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only)" steps 1-3* from reference [8] Establish an SSH session to the TVOE host of the recovered VM, login as **admusr**. Perform the following command to list the current VMs configured: **$ sudo virsh list**  Reboot the recovered VM by executing the following command: **$ sudo virsh reboot <virsh ID>**  Repeat for each recovered VM

Appendix A. Database Backup

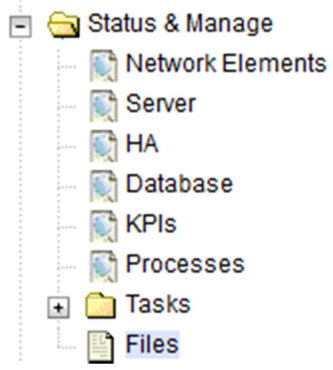
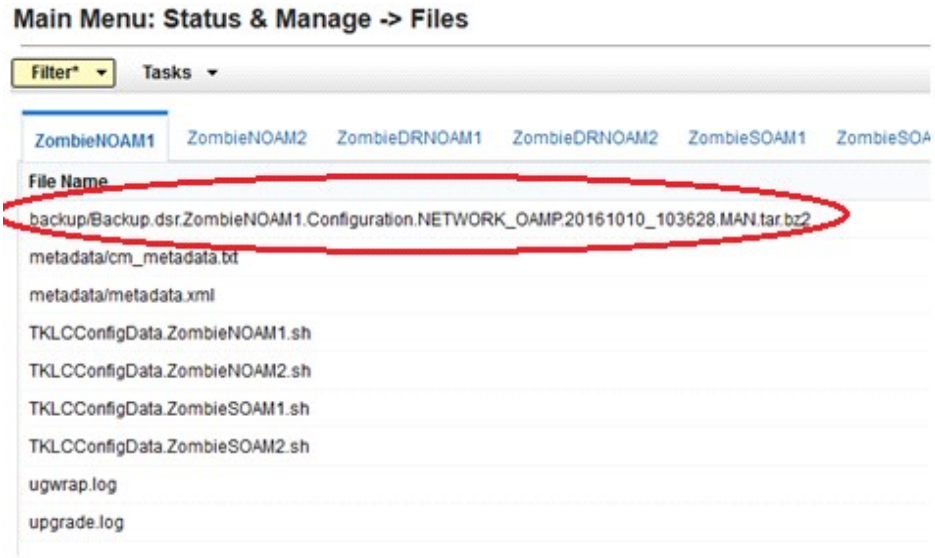
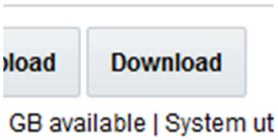
Procedure 13: Database Backup

S T E P #		
	The intent of this procedure is to back up the provision and configuration information from an NOAM or SOAM server after the disaster recovery is complete **Note:** SOAM database on SDS is not required. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1 ☐	**NOAM/SOAM VIP:** Login	Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server. Open the web browser and enter a URL of: `http://<Primary_NOAM/SOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

Procedure 13: Database Backup

2 ☐	**NOAM/SOAM VIP:** Backup Configuration Data for the System	Navigate to **Main Menu -> Status & Manage -> Database**  Select the Active NOAM Server and Click on **Backup** button  Make sure that the checkboxes next to “Configuration” is checked.  Enter a filename for the backup and press **OK**

Procedure 13: Database Backup

3 ☐	**NOAM/SOAM VIP:** Verify the backup file existence.	Navigate to **Main Menu -> Status & Manage -> Files**   Select the Active NOAM or SOAM tab. The files on this server will be displayed. Verify the existence of the backup file.
4 ☐	**NOAM/SOAM VIP:** Download the file to a local machine.	From the previous step, choose the backup file. Select the **Download** button  Select **OK** to confirm the download.

Procedure 13: Database Backup

5 ☐	**Upload the Image to Secure Location**	Transfer the backed up image saved in the previous step to a secure location where the Server Backup files are fetched in case of system disaster recovery.
6 ☐	**Backup Active SOAM**	Repeat **Steps 2 through 5** to back up the Active SOAM

7 ☐	**Take Secured backup of key file (RADIUS Only)**	**DSR Only, if SDS, Skip This 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)
		
		Login to ssh shell of Active NOAM server using user admusr
		
		Take secure backup of updated key file "RADIUS shared secret encryption key" for disaster scenarios.
		
		Execute following command to encrypt the key file before being backed up to secure customer setup :
		
		`$ ./sharedKrevo -encr`
		
		Execute following command to 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: Access to backed up key file must be strictly controlled by the operator. If the operator wishes to further encrypt this key file using operator specified encryption techniques, the operator is recommended to do so, however the operator shall be 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. Recovering/Replacing Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 8 Only)

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

Procedure 14: Recovering a Failed Aggregation Switch (Cisco 4948E/4948E-F)- HP DL380 Only

S T E P #		
	The intent of this procedure is to recover a failed Aggregation (4948E / 4948E-F) Switch. Prerequisites for this procedure are: • A copy of the networking xml configuration files • A copy of HP Misc Firmware DVD or ISO • IP address and hostname of the failed switch • Rack Mount position of the failed switch Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1 ☐	**Recover failed Aggregation Switches:** Cisco 4948E/4948E-F	Login to the PMAC via SSH as ***admusr*** Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell: `sudo ssh-keygen -R <4948_switch_ip>` **Note:** You will need a copy of the HP Misc Firmware DVD or ISO *(or firmware file obtained from the appropriate hardware vendor)* and of the original networking xml files custom for this installation. These will either be stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD. **Note: Copy switch appropriate init file and use it for respective switch:** 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'. *After creating the init file Refer to procedure "Replace a failed 4948/4948E/4948E-F switch (PM&C Installed) (netConfig)" to replace a failed Aggregation switch. - Refer [2] for the applicable platform configuration reference.* The templates can be found by the following method: From the PMAC CLI 1. `df | grep –I DSR` Sample output:

Procedure 14: Recovering a Failed Aggregation Switch (Cisco 4948E/4948E-F)- HP DL380 Only

```
/var/TKLC/smac/image/repository/DSR-
8.0.0.0.0_80.19.0-x86_64.iso
1118514  1118514         0 100%
/usr/TKLC/smac/html/TPD/DSR-8.0.0.0.0_80.19.0-x86_64
/var/TKLC/smac/image/repository/DSR-
8.0.0.0.0_80.20.0-x86_64.iso
1118372  1118372         0 100%
/usr/TKLC/smac/html/TPD/DSR-8.0.0.0.0_80.20.0-x86_64
/var/TKLC/smac/image/repository/DSR-
8.0.0.0.0_80.22.1-x86_64.iso
1117976  1117976         0 100%
/usr/TKLC/smac/html/TPD/DSR-8.0.0.0.0_80.22.1-x86_64
```

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

3. **cd usr/TKLC/smac/html/TPD/<DSR Release dir>/upgrade/overlay/**

   Example:
   cd /usr/TKLC/smac/html/TPD/DSR-8.0.0.0.0_80.22.1-x86_64/upgrade/overlay/

4. Locate the DSR_NetConfig_Templates.zip

   1. Example:

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

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

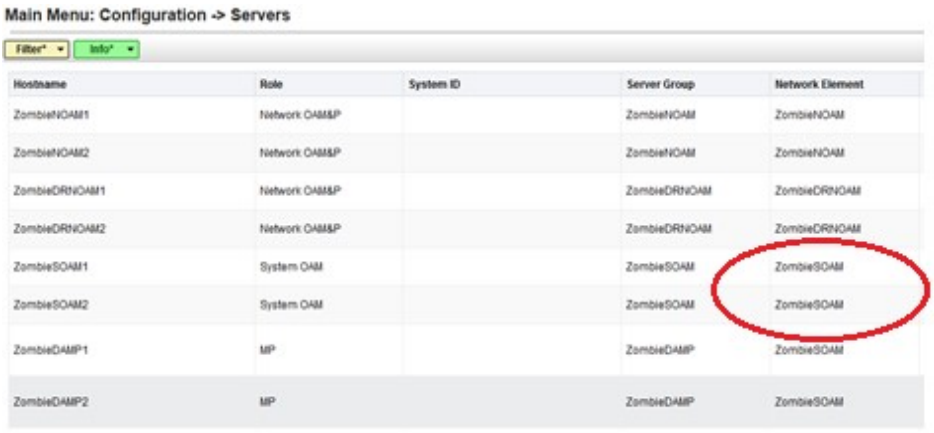
Procedure 14: Recovering a Failed Aggregation Switch (Cisco 4948E/4948E-F)- HP DL380 Only

		Example: **$ unzip DSR_NetConfig_Templates.zip** 6. Edit the desired file with site specific details. The existing file from original deployment "**/usr/TKLC/smac/etc/switch/xml**" can be used as a reference. 7. Copy the new init file to the "**/usr/TKLC/smac/etc/switch/xml**" dir. Example: **$ cp <switch_xml_file> /usr/TKLC/smac/etc/switch/xml/**

-

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

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

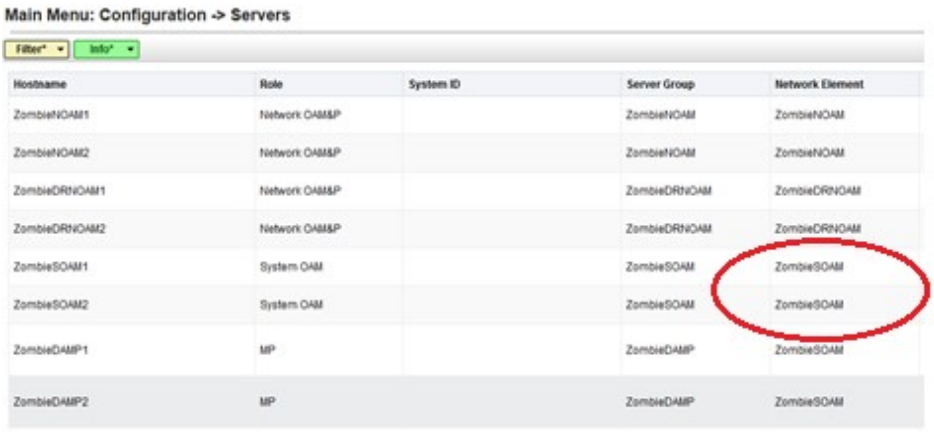
S T E P #		
	The intent of this procedure is to inhibit A and B level replication on all C Level servers of this site Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1 ☐	**Active NOAM:** Login	Login to the Active NOAM server via SSH as ***admusr***.
2 ☐	**Active NOAM:** Inhibit replication on all C level Servers	Execute the following command: `$ for i in $(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<SOAM Site_NE name of the site>'"); do iset -finhibitRepPlans='A B' NodeInfo where "nodeName='$i'"; done` **Note:** SOAM Site_NE name of the site can be found out by logging into the Active NOAM GUI and going to **Configuration->Server Groups** screen. Please see the screenshot below for more details. E.g. if ServerSO1 belongs to the site which is being recovered then siteId will be SO_HPC03. 

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

3 ☐	**Active NOAM:** Verify Replication has been Inhibited.	After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP/DP is disabled. Verification of replication inhibition on MP/DPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP/DP servers for the selected site e.g. Site SO_HPC03 shall be set as 'A B': Perform the following command: **$ iqt NodeInfo** Expected output: nodeId nodeName hostName nodeCapability inhibitRepPlans siteId excludeTables A1386.099 NO1 NO1 Active NO_HPC03 B1754.109 SO1 SO1 Active SO_HPC03 C2254.131 MP2 MP2 Active A B SO_HPC03 C2254.233 MP1 MP1 Active A B SO_HPC03

Appendix 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 #		
	The intent of this procedure is to Un-inhibit A and B level replication on all C Level servers of this site Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1 ☐	**Active NOAM:** Login	Login to the Active NOAM server via SSH as ***admusr*** user.
2 ☐	**Active NOAM:** Un-Inhibit replication on all C level Servers	Execute the following command: `$ for i in $(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<SOAM_Site_NE_namee>'"); do iset -finhibitRepPlans='' NodeInfo where "nodeName='$i'"; done` **Note:** SOAM Site NE name of the site can be found out by logging into the Active NOAM GUI and going to **Configuration->Server Groups** screen. Please see the screenshot below for more details. E.g. if ServerSO1 belongs to the site which is being recovered then siteId will be SO_HPC03. 

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

3 ☐	**Active NOAM:** Verify Replication has been un-Inhibited.	After executing above steps to un-inhibit replication on MP/DP(s), no alarms on GUI would be raised informing that replication on MP/DP is disabled. Verification of replication un-inhibition on MP/DPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP/DP servers for the selected site e.g. Site SO_HPC03 shall be set as 'A B': Perform the following command: **$ sudo iqt NodeInfo** Expected output: nodeId nodeName hostName nodeCapability inhibitRepPlans siteId excludeTables A1386.099 NO1 NO1 Active NO_HPC03 B1754.109 SO1 SO1 Active SO_HPC03 C2254.131 MP2 MP2 Active SO_HPC03 C2254.233 MP1 MP1 Active SO_HPC03

Appendix E. Restore TVOE Configuration from Backup Media

Procedure 17: 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, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1 ☐	**Install TVOE Application**	• If the PMAC is **NOT** hosted on the failed rack mount server, follow procedure *"Install TVOE on Additional Rack Mount Servers"* from reference [8] • If the PMAC is hosted on the failed rack mount server, follow procedure *"Install and Configure TVOE on First RMS (PMAC Host)"* 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 procedures *"Gather and Prepare Configuration files"* and *"First RMS Configuration steps 1-4, 22-23"* **Note:** The IP address that is configured on the TVOE must be one that will be accessible via the network of the machine that currently holds 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 execute this step, otherwise skip this step** 1. Execute Appendix "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 will be in */var/TKLC/bkp/* on the TVOE server.

Procedure 17: Restore TVOE Configuration from Backup Media

4 ☐	**Transfer TVOE Backup ISO image to the TVOE host**	**Restoring 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 the following command to copy the backup ISO image to the TVOE host:
		
		`# scp <path_to_image> tvoexfer@<TVOE_IP>:backup/`
		
		Note: where **<path_to_image>** is the path to the backup ISO image on the local system and **<TVOE_IP>** is the TVOE IP address.
		
		Note: If the IP is an IPv4 address then **<TVOE_IP>** will be a normal dot-decimal notation (e.g. "10.240.6.170").
		
		Note: If the IP is an IPv6 link local address then **<TVOE_IP>** will be need to be scoped such as "[fe80::21e:bff:fe76:5e1c%control]" where *control* is the name of the interface on the machine that is initiating the transfer and it must be on the same link as the interface on 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 backup directory within the tvoexfer user's home directory. Please refer to [9] procedure *Using WinSCP* to copy the backup image to the customer system.

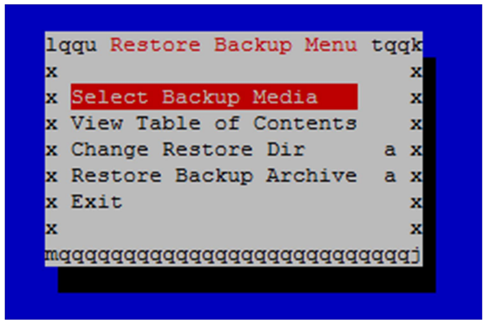
5 ☐	**TVOE Server:** Login	Establish an SSH session to the TVOE server, login as ***admusr*.**

Procedure 17: Restore TVOE Configuration from Backup Media

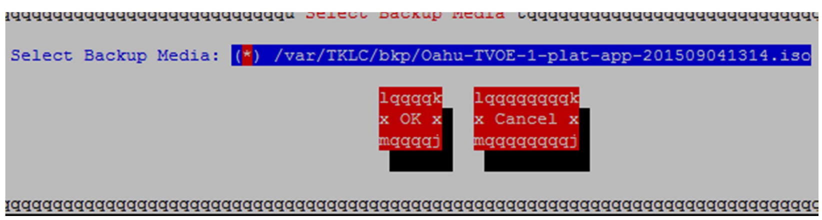
6 ☐	**Restore TVOE Backup ISO image**	Restore the TVOE backup ISO by executing the following:

```
$ sudo  su – platcfg
```

Navigate to **Maintenance -> Backup and Restore -> Restore Platform -> Select Backup Media**

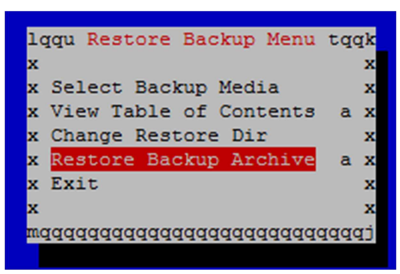


Select the desired archive:

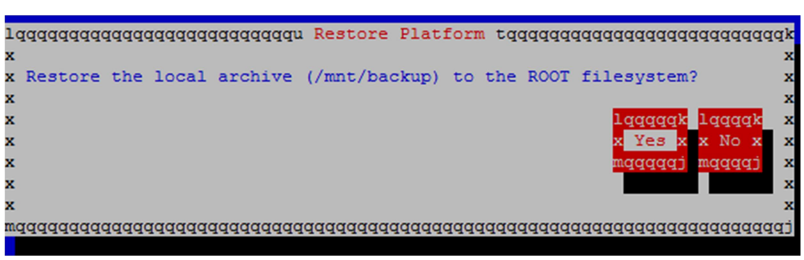


Select **OK**

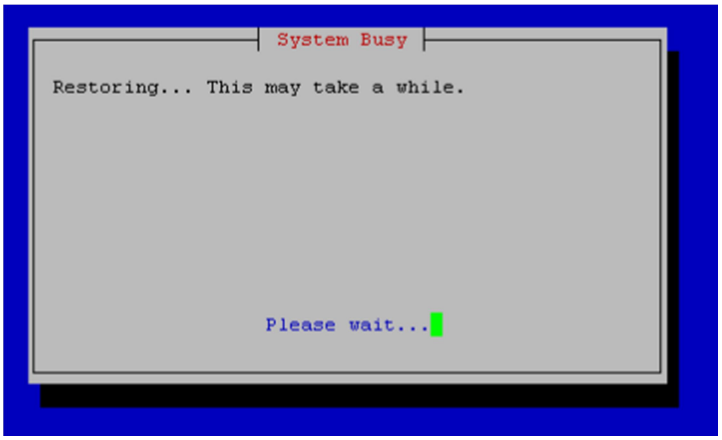
Select **Restore Backup Archive**



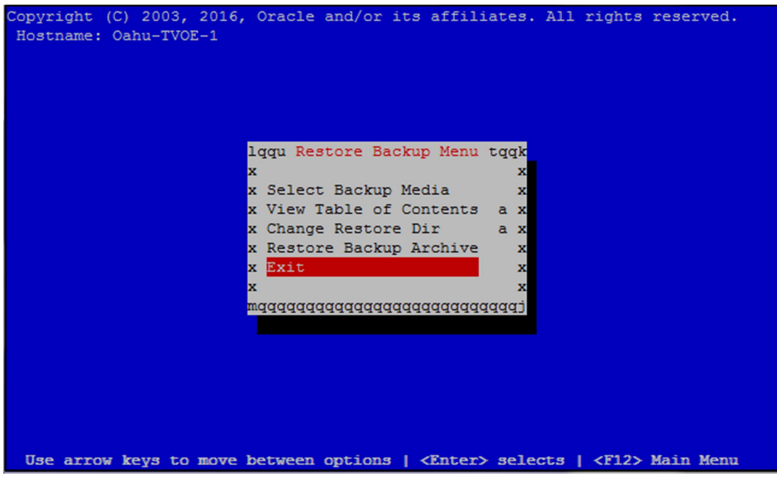
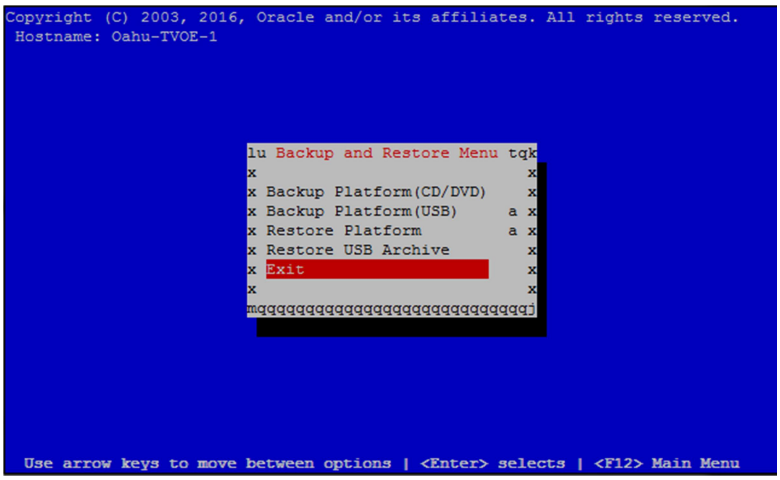
Confirm restore:



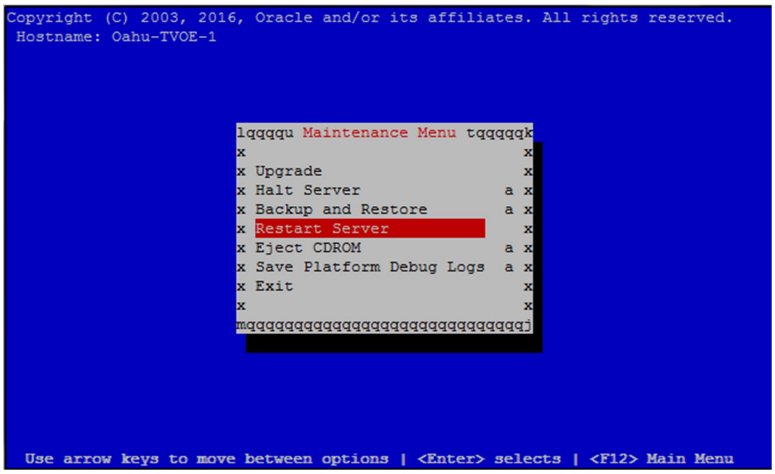
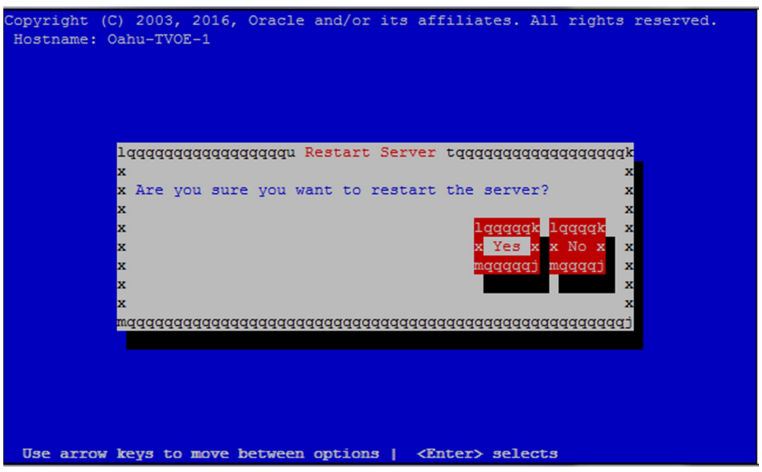
Procedure 17: Restore TVOE Configuration from Backup Media

7 ☐	**Monitor TVOE Backup process**	Wait for the restore to complete.  **Note:** This will typically take less than 5 minutes Restore complete: 

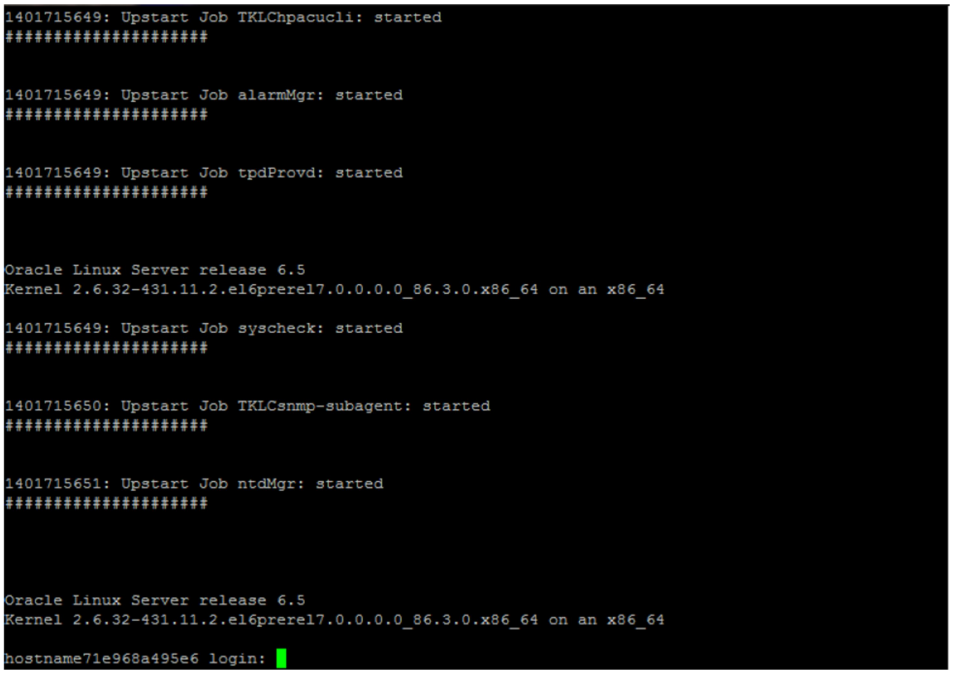
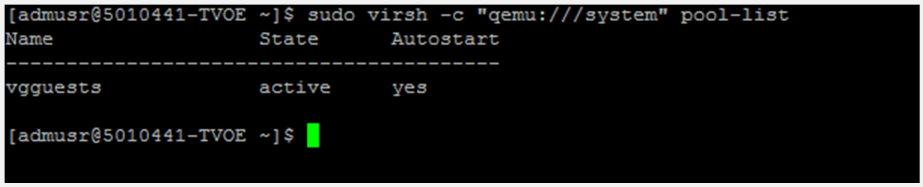
Procedure 17: Restore TVOE Configuration from Backup Media

8 ☐	**TVOE Server:** Exit Restore Backup Menu	Exit the Restore Backup Menu  

Procedure 17: Restore TVOE Configuration from Backup Media

9 ☐	**TVOE Server:** Restart	Restart the TVOE server  Select **Yes** to Restart  Confirm Restart 

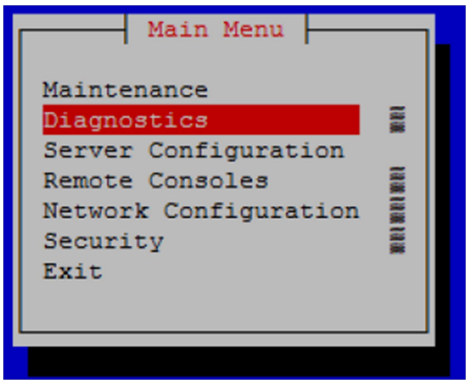
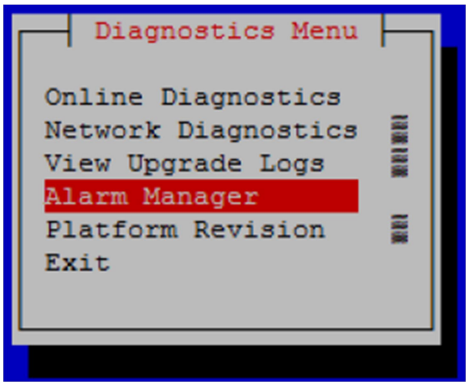
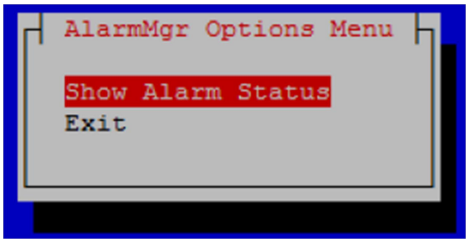
Procedure 17: Restore TVOE Configuration from Backup Media

10 ☐	**TVOE Server:** Wait for restart to successfully complete.	
11 ☐	**TVOE Server:** Verify storage pools are active	Login as admusr. Execute the following command to 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 **Appendix K. My Oracle Support (MOS)**

Procedure 17: Restore TVOE Configuration from Backup Media

12 ☐	**TVOE Server:** Enable HIDS (Optional)	**Note:** Enabling HIDS is optional. This step should be skipped if HIDS is not required to be enabled. When enabling HIDS, the baseline should be updated as well so the restored files aren't incorrectly reported as being tampered with. The following commands should be run 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 17: Restore TVOE Configuration from Backup Media

13 ☐	**TVOE Server:** Verify Alarms	Execute the following to verify alarms: `$ sudo su - platcfg` Select Diagnostics  Select Alarm Manager  Select Show Alarm Status  If any failures are reported, contact **Appendix K. My Oracle Support (MOS)**

Procedure 17: Restore TVOE Configuration from Backup Media

14 ☐	**TVOE (Optional):** Delete the files from /var/TKLC/upgrade	**If the original DSR release is pre 8.0 & performing *Network Fast Deployment* from** [8], execute the below step: After the TVOE configuration is restored, delete the following scripts/supporting files which are copied to /var/TKLC/upgrade/ folder from the DSR ISO: tuned_tvoe.tar irqtune.sh cpuset.py FDCONFIG will re-create these fles with necessary permissions.

Appendix F. Restore PMAC from Backup

Procedure 18: Restore PMAC from Backup Media

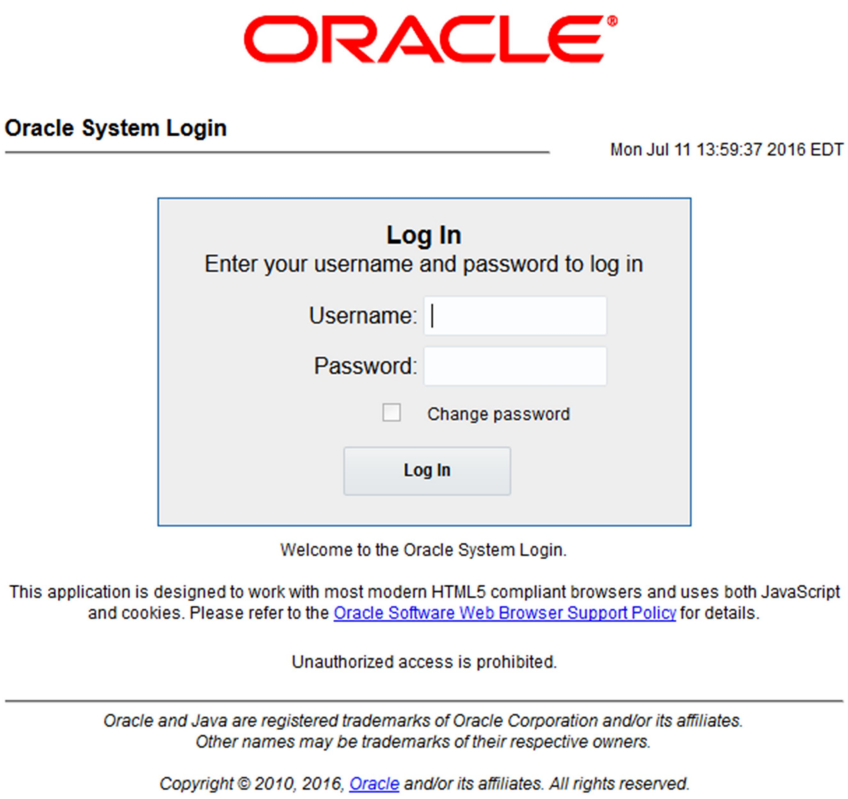
S T E P #	This procedure provides steps to restore the PMAC application configuration from backup media. **Prerequisite:** TVOE management server has been restored. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K. My Oracle Support (MOS) and ask for assistance.	
1 ☐	**Deploy the PMAC Guest**	Execute section *"Install PMAC"* from reference [8]
2 ☐	**PMAC:** Login	Establish an SSH session to the PMAC server, login as ***admusr.***

3
☐
	Restore PMAC Backup image to the PMAC host	From the remote backup location, copy the backup file to the deployed PMAC. There are too many possible backup scenarios to cover them all here.
		
		The example below is a simple scp from a redundant PM&C backup location. If using IPv6 addresses, command requires shell escapes, e.g. admusr@[<ipV6addr>]:/<file>
		
		Note: Below scp command must be executed from the recovered PM&C and the backup file is to be 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 prior to the restoration of the data.

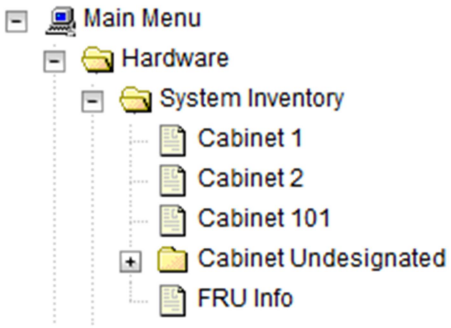
4 ☐	**PMAC:** Verify no Alarms are present	Verify no alarms are present by executing the following command: `$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus`

Procedure 18: Restore PMAC from Backup Media

5 ☐	**Restore the PMAC Data from Backup**	Restore the PMAC data from backup by executing the following command:
		`$ sudo /usr/TKLC/smac/bin/pmacadm restore`
		`PM&C Restore been successfully initiated as task ID 1`
		To check the status of the background task, issue the following command:
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		Note: The result will eventually display *PMAC Restore successful.*

6 ☐	**PMAC GUI:** Login	Open web browser and navigate to the PMAC GUI, Login as ***PMACadmin*** user: `https://<pmac_network_ip>` 

Procedure 18: Restore PMAC from Backup Media

7 ☐	**PMAC GUI:** Verify Restore Task completed	Navigate to **Task Monitoring** Verify the restore background task completed successfully. **Note:** After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior, ISO images will be added in the next step.
8 ☐	**PMAC GUI:** Verify System Inventory	Navigate to **Main Menu -> System Inventory**  Verify previously provisioned cabinets 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.`

Procedure 18: Restore PMAC from Backup Media

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/HP DL380 Gen 9 Only), and TPD ISOs to the PMAC Server"* from reference [8] for ALL ISO images as required.

Procedure 19: 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, contact Appendix K. My Oracle Support (MOS) and ask for assistance	
1 ☐	**Deploy the PMAC Guest**	Execute section *"Install PM&C"* from reference [9] **Note:** This procedure is for restoring from a NetBackup server, so specify the appropriate options when deploying PM&C for use with NetBackup.
2 ☐	**PMAC TVOE Host:** Login	Establish an SSH session to the PMAC TVOE Host, login as ***admusr.***

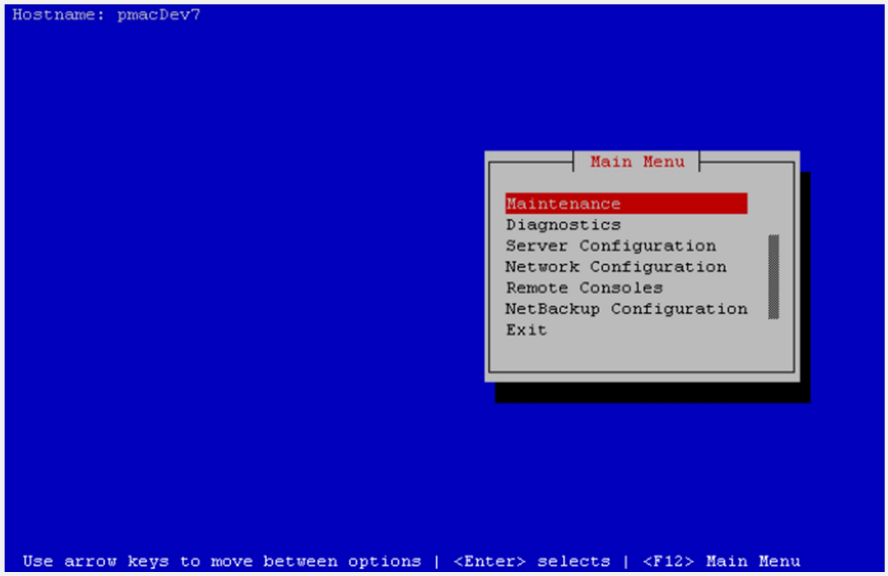
3
☐
	PMAC TVOE Host: Login to PMAC Guest Console	On the TVOE host, execute the following command:
		
		`$sudo virsh list`
		
		This will produce a listing of currently running virtual machines.
		
		`[admusr@Oahu-TVOE-1 ~]$ sudo virsh list`
		` Id    Name                           State`
		`----------------------------------------------------`
		` 1     Oahu-PMAC                      running`
		
		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:
		
		`$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 19: 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.	Run the following 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 19: Restore PMAC from Backup Server

6 ☐	**PMAC:** Verify the TPD platcfg backup menus are visible, then exit the TPD platcfg Utlility	Issue the following command to 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 by executing the following command:
		$ 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`

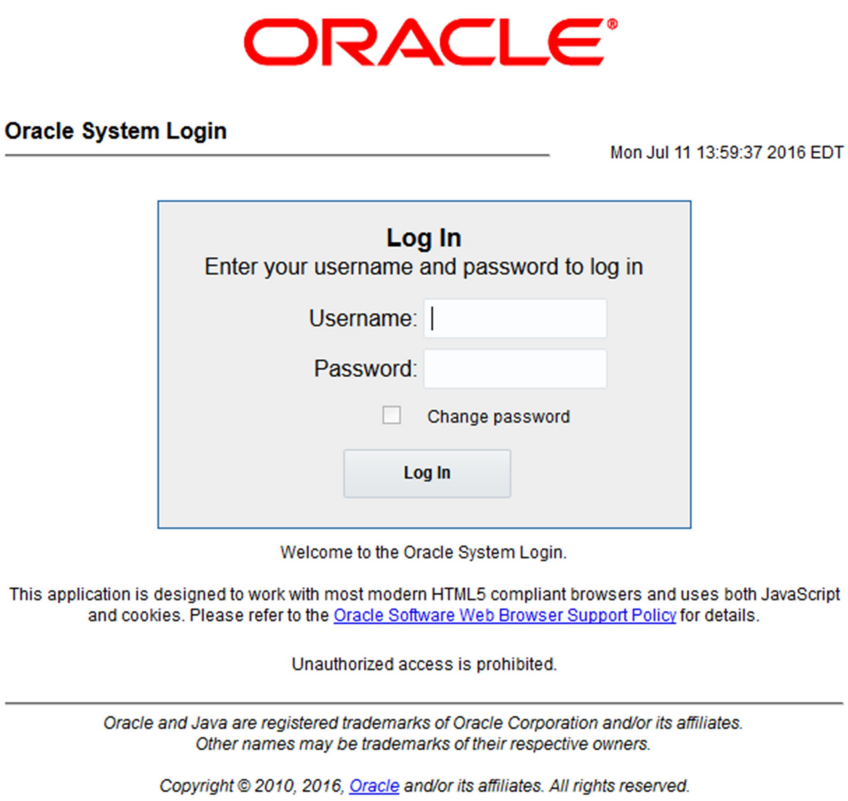
8 ☐	**PMAC:** Install backup utility client software on the PMAC Guest	Execute section *“PM&C NetBackup Client Installation and Configuration”* from [9] Start at step 4. **Note:** The *“Initialize PM&C Application”* and *“Configure PM&C application”* prereuistes can be igrnored.

Procedure 19: Restore PMAC from Backup Server

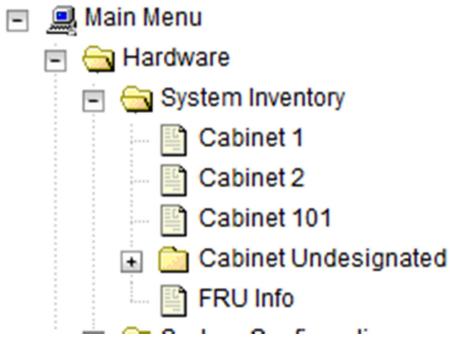
9 ☐	**Backup Server:** Verify appropriate PMAC backup exists.	This step will likely be executed by customer IT personnel. Log in to the Backup Server as the appropriate user, using the user password. Execute the appropriate commands to verify the PMAC backup exists for the desired date. **Note:** The actions and commands required to verify that the PM&C 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 choose 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 PM&C prior to the restoration of the data.
10 ☐	**Backup Server:** Verify appropriate PMAC backup exists.	This step will likely be executed by customer IT personnel. Log in to the Backup Server as the appropriate user, using the user password. Execute the appropriate commands to verify the PMAC backup exists for the desired date. Execute the appropriate commands to restore the PM&C Management Server backup for the desired date. **Note:** The actions, and commands, required to verify the PM&C 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 by executing the following command: `$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus`

12 ☐	**Restore the PMAC Data from Backup**	Restore the PMAC data from backup by executing the following command:
		
		`$ sudo /usr/TKLC/smac/bin/pmacadm restore`
		
		`PM&C Restore been successfully initiated as task ID 1`
		
		To check the status of the background task, issue the following command:
		
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		
		Note: The result will eventually display *PMAC Restore successful.*

Procedure 19: Restore PMAC from Backup Server

13 ☐	**PMAC GUI:** Login	Open web browser and navigate to the PMAC GUI, Login as ***PMACadmin*** user: `https://<pmac_network_ip>` 
14 ☐	**PMAC GUI:** Verify Restore Task completed	Navigate to **Task Monitoring** 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 will be added in the next step.

Procedure 19: Restore PMAC from Backup Server

15 ☐	**PMAC GUI:** Verify System Inventory	Navigate to **Main Menu -> System Inventory**  Verify previously provisioned enclosures are present

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

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

Appendix G. Workarounds for Issues not fixed in this Release

Issue	Associated PR	Workaround

Inetsync alarms after performing disaster recovery	222828	Restart the Inetsync service on all affected servers using the following commands:
		`$ pm.set off inetsync`
		`$ pm.set on inetsync`

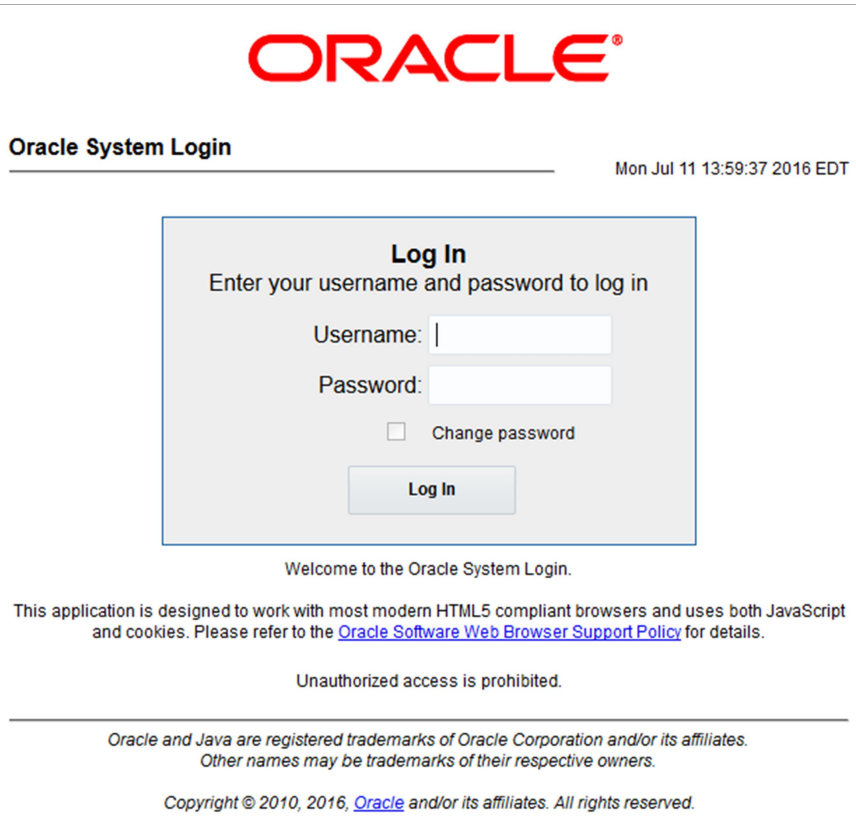
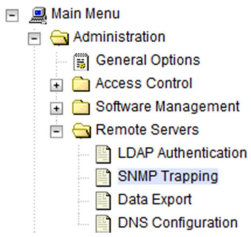
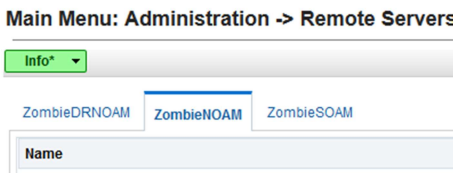
DSR Only: Restore Database from the active SOAM server will fail if the spare SOAM is in another network and is unreachable		While restoring the database from the recovered SOAM GUI, if the spare SOAM is in another network and is unreachable, the database restore will fail. **Workaround** - If the spare 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), kill the hung ping processes and the restore will proceed.

Appendix H. SNMP Configuration

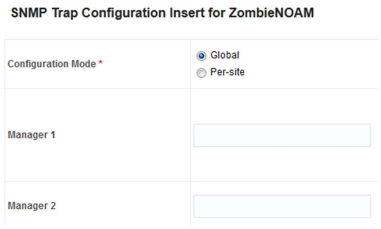
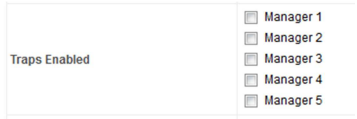
Procedure 20: SNMP Configuration

S T E P #	This workaround procedure will provide the steps to configure SNMP with **'SNMPv2c and SNMPv3'** as the enabled versions for SNMP Traps configuration, as PMAC does not support SNMPv3. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix K. My Oracle Support (MOS), and ask for assistance.	
1 ☐	**(Workaround)** **PRIMARY NOAM VIP GUI:** Login	**NOTE:** This workaround step should be performed only in any of 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, as PMAC does not support SNMPv3.** Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user:

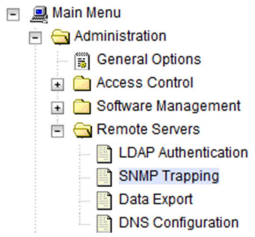
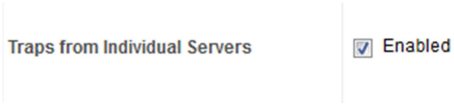
Procedure 20: SNMP Configuration

		
2 ☐	**NOAM VIP GUI:** Configure System-Wide SNMP Trap Receiver(s)	Navigate to **Main Menu -> Administration -> Remote Servers -> SNMP Trapping**  Select the Server Group tab for SNMP trap configuration:  Fill in the IP address or hostname of the Network Management Station (NMS) you

Procedure 20: SNMP Configuration

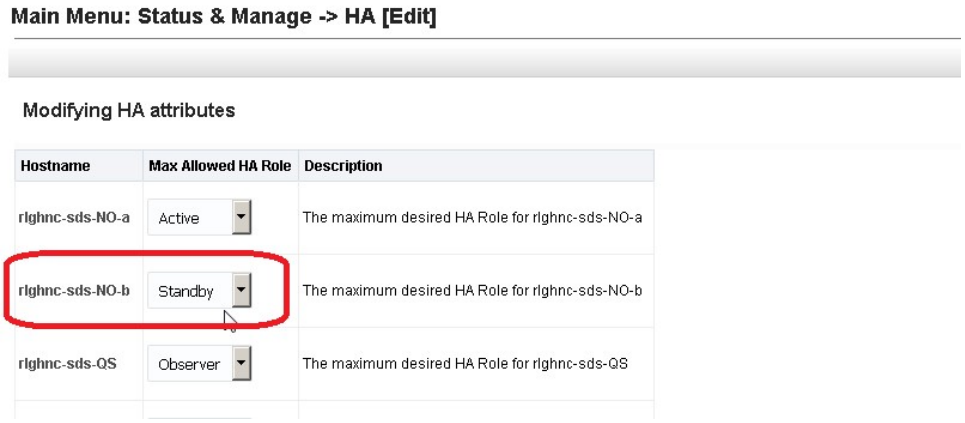
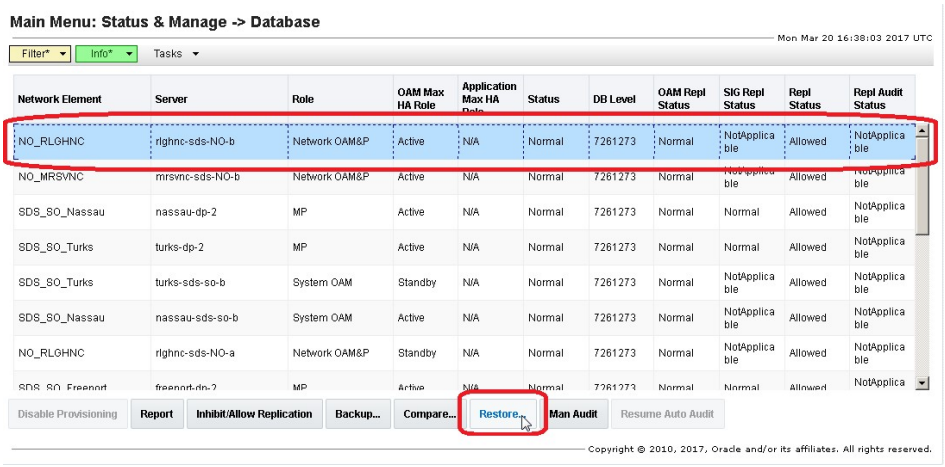
		wish to forward traps to. This IP should be reachable from the NOAMP's "XMI" network. (If already configured SNMP with **SNMPv3** as enabled version, another server needs to be configured here) Continue to fill in additional secondary, tertiary, etc. Manager IPs in the corresponding slots if desired.  Set the Enabled Versions as **SNMPv2c and SNMPv3**:  Check Traps Enabled boxes for the Manager servers being configured:  Enter the **SNMP Community Name**:  Leave all other fields at their default values. Press **OK**
3 ☐	**NOAMP VIP:** Enable Traps from Individual Servers **(**Optional)	**Note**: By default SNMP traps from MPs are aggregated and then displayed at the active NOAMP. If instead, you wish for every server to send its own traps directly to the NMS, then execute this procedure. This procedure requires that all servers, including MPs, have an XMI interface on which the customer SNMP Target server (NMS) is reachable. Navigate to **Main Menu -> Administration -> Remote Servers -> SNMP Trapping**

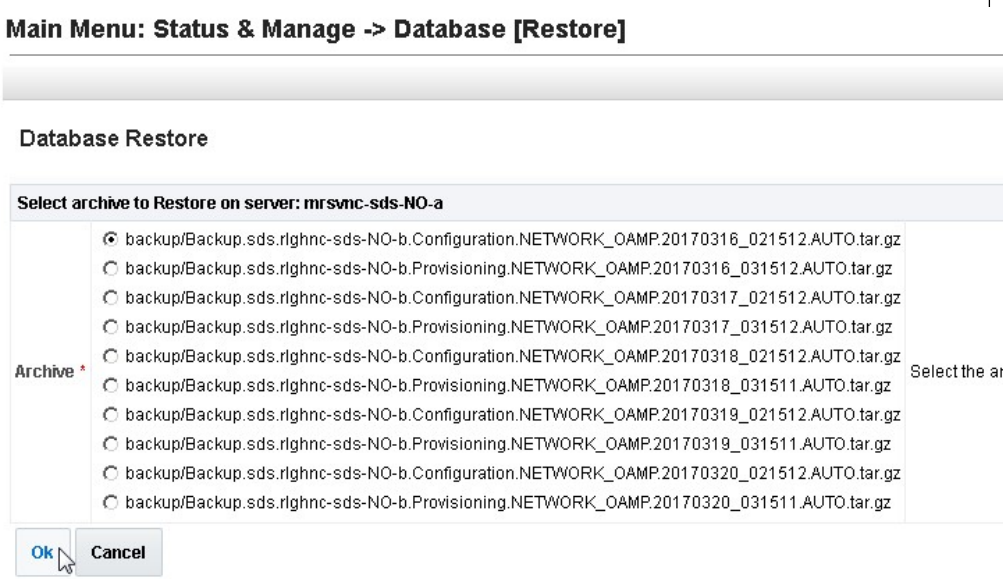
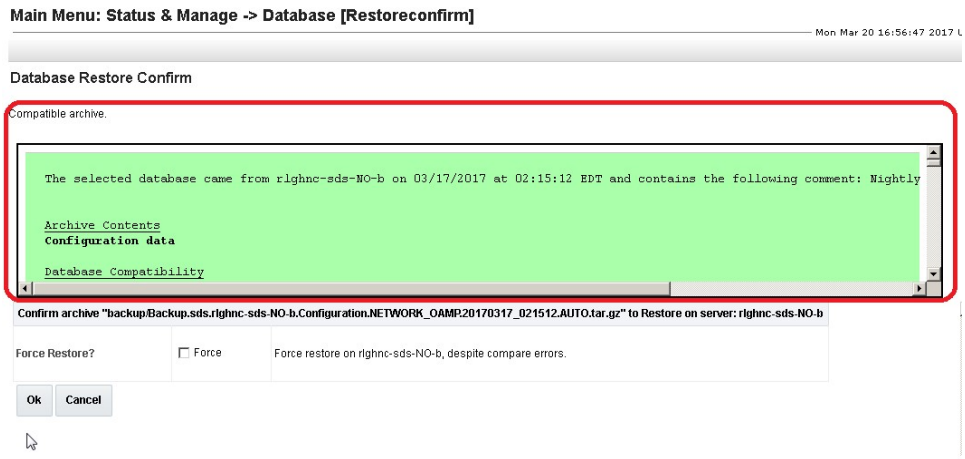
Procedure 20: SNMP Configuration

		 Make sure the checkbox next to **Enabled** is checked, if not, check it as shown below  Then click on **Apply** and verify that the data is committed.
4 ☐	**PMAC:** Update the TVOE Host SNMP Community String	Establish an SSH session to the PMAC, login as ***admusr***. Execute the following command to update the TVOE host community string: `$ sudo pmaccli setCommStr --accessType=rw --commStr=<site specific value>` **Note:** When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest on the PMAC control network will be updated. All those servers that match the existing Site Specific Community String will not be updated again until the string name is changed.

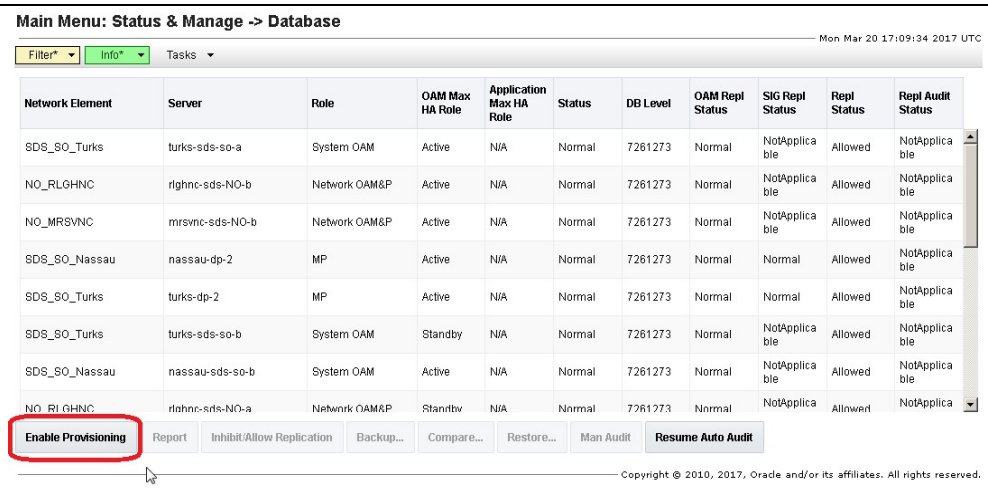
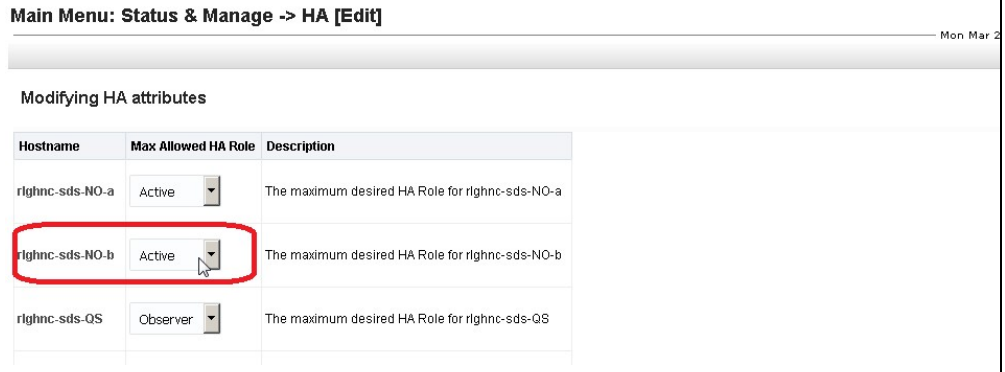
Appendix I. Restore Provisioning Database

S T E P #	This procedure will provide the steps to restore 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, contact Appendix K. My Oracle Support (MOS), and ask for assistance.

1 ☐	**Primary SDS NOAM GUI :**Log into 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 **Main Menu: Status & Manage-> HA** 2. Click on **"Edit"** 3. Move the newly recovered standby server to forced standby. 
3 ☐	**Primary SDS NOAM GUI :**Restore Provisioning data	1. Navigate to **Main Menu: Status & Manage -> Database** 2. Select Select Active NOAM and click the Restore button.  3. Select Provisioning backup file from the list (which was previously placed in /var/TKLC/db/filemgmt/backup directory in Step 5 of Section 2.6.2) and click the OK button. **Note: Must use a Provisioning only backup file. Combined backup files containing Configuration & Provisioning data will cause catastrophic**

		issues which could lead to complete re-installation.  4. Verify Compatibility and select Ok to restore. 
4 ☐	**Primary SDS NOAM GUI :**Wait for the restore to begin	Wait 60 seconds for the restore to begin.
5 ☐	**Primary SDS NOAM GUI :**Track Progress of Restore	Monitor the "Info" tab under the **[Status & Manage --> Database]** screen and look for the following message: Note: - Restore on <Active_NO_hostname> status MAINT_IN_PROGRESS.
6	**Primary SDS**	Continue to monitor the "Info" tab under the **[Status & Manage --> Database]**

☐	**NOAM GUI :**Wait for the restore to complete	screen until the following message is received: Success: - Restore on rlghnc-sds-NO-b status MAINT_CMD_SUCCESS. Success NOTE: The “Info" tab may require manual refresh to see updated status. To refresh the "Info" tab, re-select **[Status & Manage --> Database]** from the Main Menu, then reselect the "Info" tab.
7 ☐	**Primary SDS NOAM GUI :**Uninhibit servers	Uninhibit All servers in the following staggered arrangement: 1. Uninhibit Active NOAM. 2. Refresh/monitor the [Status & Manage --> Database] screen until a valid "DB Level" appears for the Active NOAM. 3. Uninhibit Standby NOAM / Query Server. 4. Refresh/monitor the [Status & Manage --> Database] screen until a valid "DB Level" appears for the Standby NOAM / Query Server. 5. Uninhibit Active SOAMs. 6. Refresh/monitor the [Status & Manage --> Database] screen until a valid "DB Level" appears for the Active SOAMs. 7. Uninhibit Standby SOAMs / DPs. 8. Refresh/monitor the [Status & Manage --> Database] screen until a valid "DB Level" appears for the Standby SOAMs / DPs.
8 ☐	Recover Pdbrelay (IF NEEDED)	Verify whether PDB Relay is Enabled by following the instructions in Appendix J. Recover PDB Relay
9 ☐	**Primary SDS NOAM GUI :**Enable Provisioning	Navigate to: [**Status & Manage --> Database**] and click “Enable Provisioning”

		
10 ☐	**Primary SDS NOAM GUI :**Remove NO from forced standby.	1. Navigate to **Main Menu: Status & Manage -> HA** , 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

S T E P	This procedure will provide the steps to re-establish 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, contact Appendix K. 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	Uncheck PDB Relay Enabled checkbox under the **[SDS --> Configuration --> Options]** screen and Apply the change.
3 ☐	**NOAM VIP console**: Emergency Restart (Start from Beginning of Cmd Log)	Execute following commad on console: `$ iset -fvalue=0 ProvOptions where "var='pdbRelayMsgLogTimeStamp'"`
4 ☐	**NOAM VIP GUI:** Enable pdbrelay	Recheck PDB Relay Enabled checkbox under the **[SDS --> Configuration --> Options]** screen and Apply the change.

Appendix K. My Oracle Support (MOS)

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

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

When calling, there are multiple layers of menus selections. Make the selections in the sequence shown below on the Support telephone menu:

1. For the first set of menu options, select 2, “New Service Request”. You will hear another set of menu options.

2. In this set of menu options, select 3, “Hardware, Networking and Solaris Operating System Support”. A third set of menu options begins.

3. In the third set of options, select 2, “Non-technical issue”. Then you will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.