Oracle® Communications

Diameter Signaling Router

RMS Productization Disaster Recovery Guide

Release 5.0/6.0/7.0/7.1

E57521 Revision 02

July 2015

ORACLE

Oracle Communications Diameter Signaling Router RMS Productization Disaster Recovery Procedure, Release 5.0/6.0/7.0/7.1

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

1.0 Introduction

1.1 Purpose and Scope

This document is a guide to describe procedures used to execute disaster recovery for DSR 5.0/6.0/7.0/7.1 RMS Productization 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 5.0/6.0/7.0/7.1. 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, and PMAC. As of DSR 7.1, IDIH content is included in this document (**Section 7.0**). For DSR 5.0, 6.0, and 7.0, refer to **Table 6**: IDIH Disaster Recovery Reference Table.

Note that this document only covers the disaster recovery scenarios of DSR RMS Productization deployments. For all other DSR deployments, refer to [9] for 3-tier deployments, and refer to [10] for 2-tier deployments.

1.2 References

[1] TPD Initial Product Manufacture, E54521
[2] PM&C 5.x Disaster Recovery Guide, 909-2283-001
[3] PM&C 5.7/6.0 Disaster Recovery Guide, E54388
[4] DSR RMS Productization Installation Guide, 909-2255-001
[5] DSR 6.0/7.0/7.1 RMS Productization Installation Guide, E55235
[6] IDIH 5.x Installation/Upgrade Procedure, 909-2232-002
[7] DSR RBAR Feature Activation Procedure, E58665
[8] DSR MAP-Diameter IWF Feature Activation Procedure, E58666
[9] DSR 5.0/6.0/7.0/7.1 3-Tier Disaster Recovery Procedure, E57520
[10] DSR 2-Tier Disaster Recovery Procedure, 909-2225-001
[11] IDIH 6.0/7.0 Disaster Recovery Guide, E56375
[12] IDIH 6.0/7.0 Installation/Upgrade Procedure, E56571
[13] Platform 6.7/7.0 Configuration Procedure Reference, E54386

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
IDIH	Integrated Diameter Intelligence Hub

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

Table 3 Optional Features

Feature	Document
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation Procedure, E58665
Map-Diameter Interworking (MAP-IWF) – DSR 6.0+	DSR MAP-Diameter IWF Feature Activation Procedure, E58666

2.0 General Description

The DSR RMS Productization disaster recovery procedure falls into three 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 core RMS servers failed • All expansion Servers failed
Recovery of a failed core RMS server with one core RMS server intact	• 1 core RMS server with all its VMs intact • 1 core RMS server failed (including all its VMs) • 1 or more expansion server failed (including all its VMs)
Recovery of failed expansion RMS server with the core RMS server intact	• All core RMS servers with all VMs intact • 1 or more expansion RMS server failed (including all its VMs)
Recovery of one or more server with corrupt databases that cannot be restored via replication from the active parent node.	

Note: Core RMS server refers to server hosting NOAM, SOAMs, PMAC DAMP, and IPFE. In DSR 6.0 scaling of the DA MPs is introduced for rack-mount server configurations by adding additional expansion server VMs running as DA MPs and SS7-MPs (optional)

Note: For Disaster Recovery of the Aggregation switches refer to **Appendix B**. Recovering/Replacing Failed.

Note: For Disaster Recovery of the PMAC Server, refer to **Table 5**: PMAC Disaster Recovery Reference Table.

Note: As of DSR 7.1, IDIH content is included in this document **Section 7.0**. For DSR 5.0, 6.0, and 7.0, refer to **Table 6**: IDIH Disaster Recovery Reference Table.

2.1 Complete Outage (All Servers)

This is the worst case scenario where all RMS servers 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.

For DSR 6.0/7.0/7.1, this case will also cover the recovery of the expansion servers.

2.2 Partial Outage with one RMS Intact

This case assumes that one RMS Server and all its VMs are intact. The servers that failed are recovered using base recovery of hardware and software. VMs are created and setup. Replication will recover the database and configuration.

For DSR 6.x/7.0/7.1, this case will also cover the recovery of the expansion servers.

2.3 Partial Outage with Expansion Servers Outage

This case applicable to DSR 6.x/7.0/7.1 assumes that both core RMS Server and all its VMs are intact. The expansion servers that failed are recovered using base recovery of hardware and software. VMs are created and setup. Replication will recover the database and configuration.

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

1. One (1) target release Application Media, or a target-release ISO
2. One (1) ISO of TPD release, or later shipping baseline as per Oracle ECO
3. One (1) ISO of TVOE release, or later shipping baseline as per Oracle ECO
4. One (1) ISO of PMAC release, or later shipping baseline as per Oracle ECO
5. Firmware files as provided by Hardware vendor.
6. All applicable documents listed in **Section 3.1.1** Release Document Matrix.

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.

SUDO

DSR 6.x+ introduced a new non-root user ‘admusr’, as a non-root user, many commands (when run as admusr) now require the use of ‘sudo’.

3.1.1 Release Document Matrix

Table 4: DSR RMS Installation Reference Table

DSR Release	Reference
DSR 5.0	[4]
DSR 6.0	[5]
DSR 7.0	[5]
DSR 7.1	[5]

Table 5: PMAC Disaster Recovery Reference Table

DSR Release	Reference
DSR 5.0	[2]
DSR 6.0	[3]
DSR 7.0	[3]
DSR 7.1	[3]

Table 6: IDIH Disaster Recovery Reference Table

IDIH Release	Reference
IDIH 6.0	[11]
IDIH 7.0	[11]

Table 7: IDIH Installation Reference Table

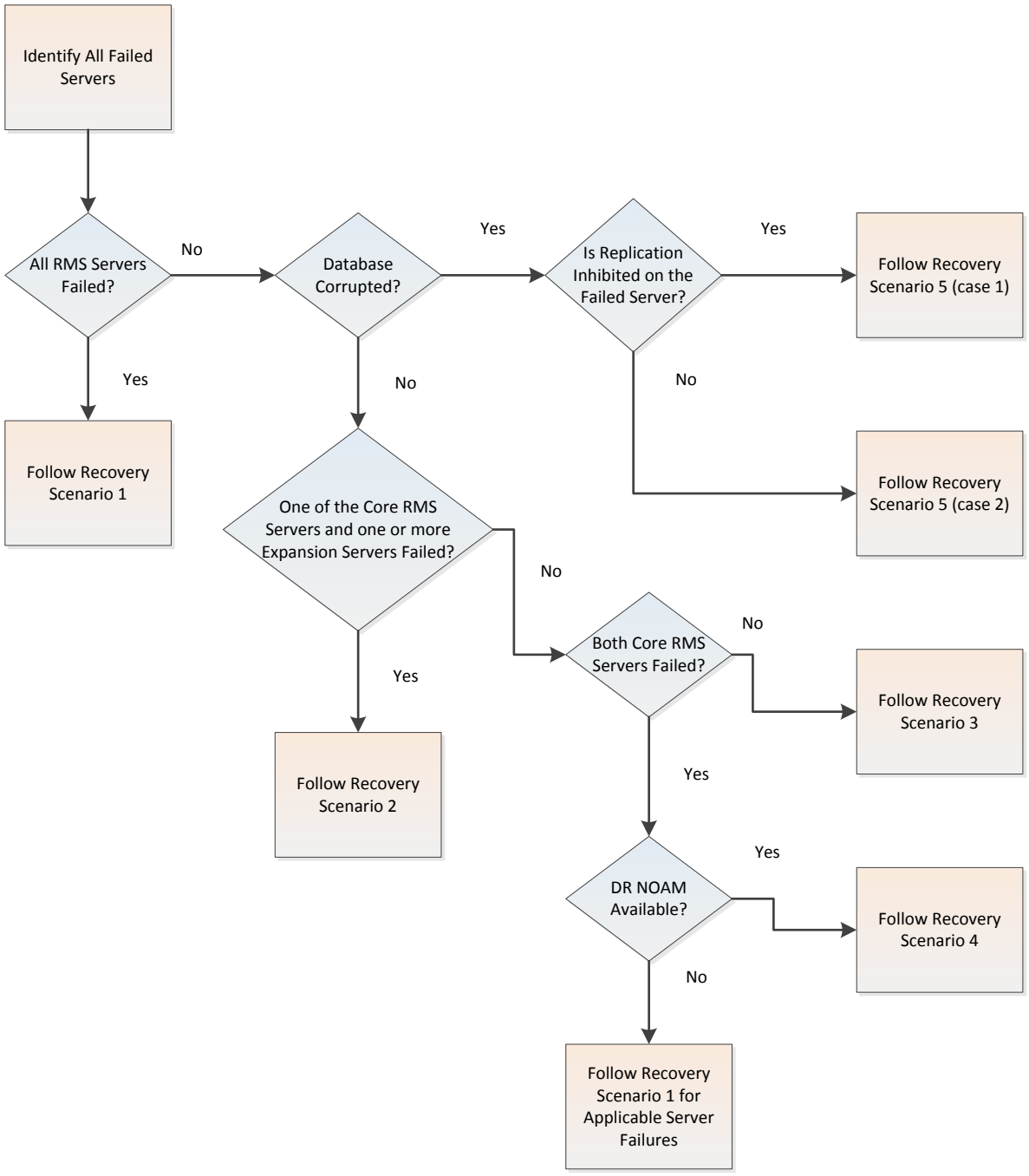
IDIH Release	Reference
IDIH 6.0	[12]
IDIH 7.0	[12]

3.2 Disaster Recovery Strategy

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

- 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**
- Read and review the content in this document.
- Gather required materials in **Section 3.1** Required Materials
- From the failure conditions, determine the Recovery Scenario and procedure to follow (using **Figure 1**: Determining Recovery Scenario and **Table 8** Recovery Scenarios
- Execute appropriate recovery procedures (listed in **Table 9**).

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 9** 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.

Note: Here Core RMS server refers to server hosting NOAM, SOAMs, PMAC (1st core RMS) and IPFE. In DSR 6.x/7.0/7.1, scaling of the DA MPs is introduced for rack-mount server configurations by adding additional VMs running as DA MPs and SS7-MPs (optional)

Table 8 Recovery Scenarios

Recovery Scenario	Failure Conditions	Section
1	**Both** core RMS Servers completely failed (All VMs unavailable). All expansion Servers completely failed (All VMs unavailable) **Note:** Presence of expansion servers is applicable on DSR 6.x and higher releases.	**Section 5.1.1** Recovery Scenario 1 (Complete Outage)
2	1 core RMS server is intact and available. 1 core RMS server failed. 1 or more expansion Servers failed Note: Presence of expansion servers is applicable on DSR 6.x and higher releases.	**Section 5.1.2** Recovery Scenario 2 (Partial Outage with one Core RMS Server Intact)
3	All Core RMS server with all its VMs intact 1 or more expansion Servers completely failed (All VMs unavailable) Note: Presence of expansion servers are applicable on DSR 6.x and higher releases	**Section 5.1.3** Recovery Scenario 3 (Partial Outage with one or more Expansion Servers Failed)
4	Both NOAM servers Failed DR NOAM is Available	**Section 5.1.4** Recovery Scenario 4 (Both NOAM servers Failed with DR NOAM Available)
5: Case 1	Server is intact Database gets corrupted on the server Replication is occurring to the server with corrupted database	**Section 5.1.5.1** Recovery Scenario 5: Case 1
5: Case 1	Server is intact Database gets corrupted on the server Latest Database backup of the corrupt server is NOT present Replication is inhibited (either	**Section 5.1.5.2** Recovery Scenario 5: Case 2

	manually or because of comcol upgrade barrier)	

5.0 Disaster Recovery Procedure

Call the My Oracle Support (MOS) at 1-888-367-8552 or 1-919-460-2150 (international) 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

Recovering Base Hardware:

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

5.1 Disaster Recovery Procedure

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

5.1.1 Recovery Scenario 1 (Complete 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 all SOAM and MP Guest.

- Recover the SOAM database.
- Reconfigure the Application

Restart processes and re-enable provisioning and replication.

Note: DR recovery actions on the IDIH may occur in parallel if necessary. These actions can/should be worked simultaneously; doing so would allow faster recovery of the complete solution. Refer to [11] for IDIH 5.0/6.0/7.0 disaster recovery and **Section 7.0** for DSR 7.1

Procedure 1: Recovery Scenario 1

S T E P #	This procedure performs recovery if all RMS servers are failed. 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 H. 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

Procedure 1: Recovery Scenario 1

3 ☐	**Recover Core RMS Servers**	Recover the failed core RMS servers: 1. Configure and verify the BIOS on the RMS. Execute procedure *"Configure the RMS Server BIOS Settings and Update Firmware"* – Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 2. Execute procedure *"Install TVOE on First RMS Server"* – Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 3. Execute procedure *"First RMS Configuration"* – Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 4. Recover the PMAC –Refer to **Table 5**: PMAC Disaster Recovery Reference Table for applicable PMAC Disaster Recovery Procedure. 5. Recover Failed Cisco 4948 Aggregation Switches if needed – Refer to **Appendix B**. Recovering/Replacing Failed Cisco 4948 Aggregation Switches 6. Execute procedure *"Install TVOE on Additional Rack Mount Servers"* – Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. **Note:** This step can also be done for expansion servers (as mentioned in step 4) if needed, to reduce recovery time. 7. **E**xecute procedure *"Configure TVOE on Additional Rack Mount Server"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 8. Execute procedure *"Load DSR and TPD ISO to the PMAC Server"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 9. Execute procedure *"Create NOAM Guest VMs"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 10. Execute procedure *"Create SOAM Guest VMs"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 11. Execute procedure *"Create MP Guest VMs"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 12. Execute procedure "Create IPFE Guest VMs" - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 13. IPM all the guests using procedure "Install the Software on Virtual Machines"- Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 14. If NetBackup was previously installed on the system, follow the Appendix *"Application NetBackup Client Installation Procedures"* - Refer to **Table 4**: DSR

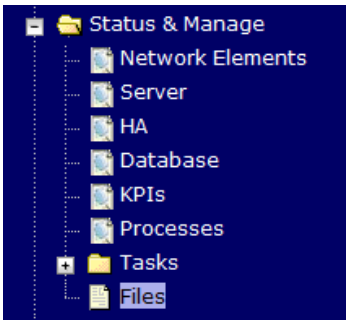
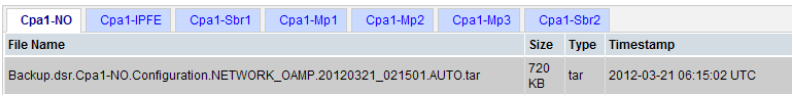
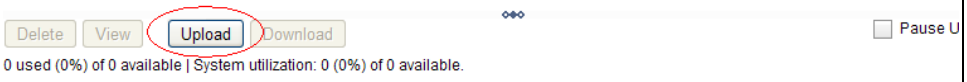
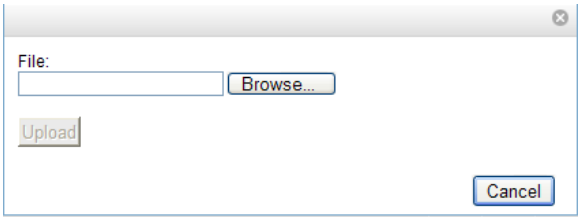
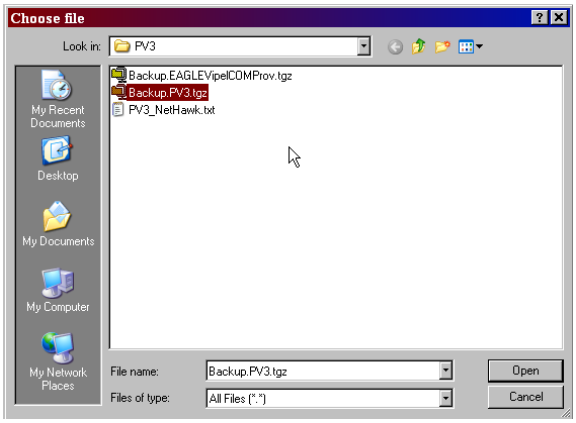
Procedure 1: Recovery Scenario 1

4 ☐	**Recover Expansion Servers**	Recover the failed expansion RMS servers (DSR 6.x and on): 1. Execute procedure *"Install TVOE on Additional Rack Mount Servers"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 2. Execute procedure *"Configure TVOE on Additional Rack Mount Servers"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 3. Execute procedure *"Create MP Guest VMs"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 4. IPM all the guests created in this step using procedure *"Install the Software on Virtual Machines"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure.
5 ☐	**Repeat for Remaining Failed Servers**	If necessary, repeat steps 4 for all remaining failed servers.
6 ☐	**Install NetBackup Client (Optional)**	If NetBackup is used execute procedure *"NetBackup Client Installation (Optional)"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure.
7 ☐	**Obtain Latest Database Backup and Network Configuration Data.**	Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. 1. Using procedures within your organization's process (ex. IT department recovery procedures), obtain the most recent backup of the DSR database backup file. 2. From required materials list in **Section 3.1** `Required Materials`; use NAPD documents and Network Element report (if available), to determine network configuration data.
8 ☐	**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) Configure the first NOAM server by executing procedure *"Configure the First NOAM NE and Server"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. Configure the NOAM server group by executing procedure *"Configure the NOAM Server Group"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure.

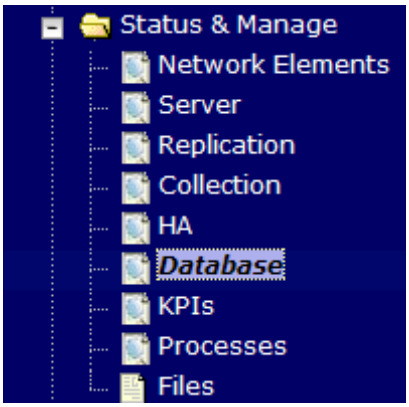
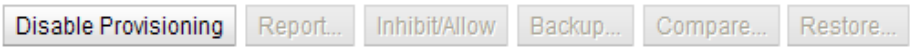
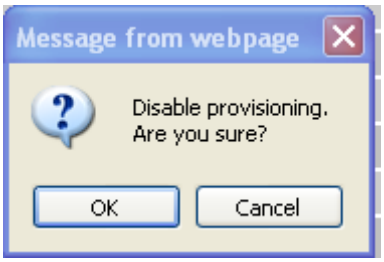
Procedure 1: Recovery Scenario 1

9 ☐	**NOAM GUI:** Login	Login to the NOAM GUI as the ***guiadmin*** user: 

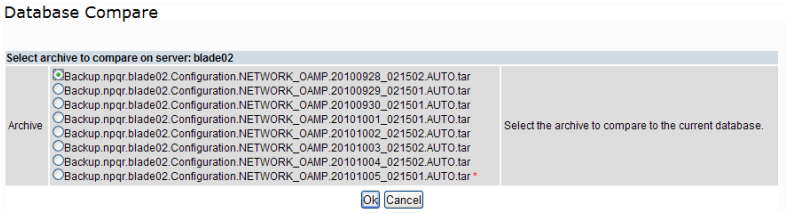
Procedure 1: Recovery Scenario 1

10 ☐	**NOAM GUI:** Upload the Backed up Database File	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.  Click on **Browse** and locate the backup file and 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.

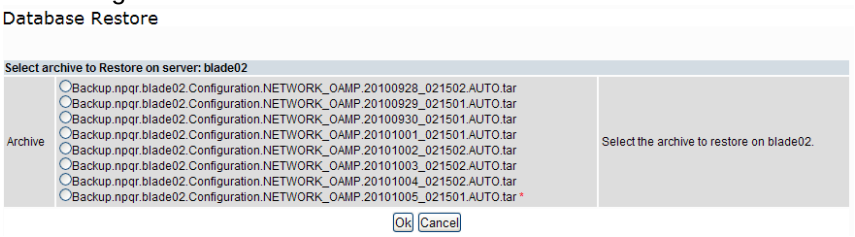
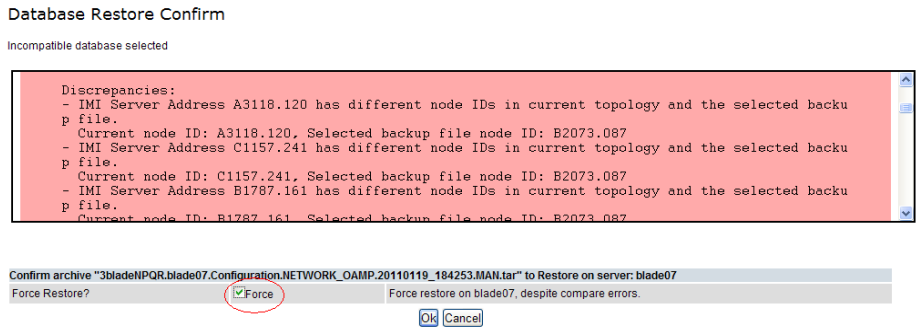
Procedure 1: Recovery Scenario 1

11 ☐	**NOAM GUI:** Disable Provisioning	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.  The message *"Warning Code 002"* will appear.

Procedure 1: Recovery Scenario 1

12 ☐	**NOAM GUI:** Verify the Archive Contents and Database Compatibility	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 10** of this procedure.  **Verify** that the output window matches the screen below. **Note:** You will get a database mismatch regarding the NodeIDs of the VMs. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix H. My Oracle Support (MOS)  **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.

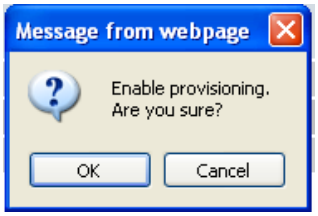
Procedure 1: Recovery Scenario 1

13 ☐	**ACTIVE NOAM:** Restore the Database	Click on **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 an error that the NodeIDs do not match. That is expected. If no other errors beside the NodeIDs 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 NOAM GUI since the restored Topology is old data.

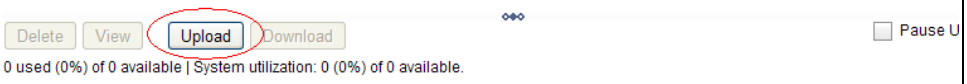
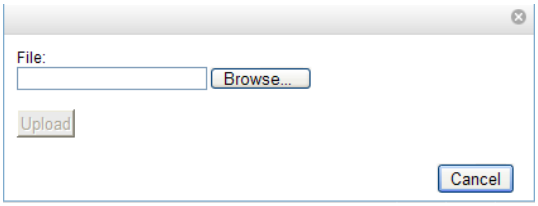
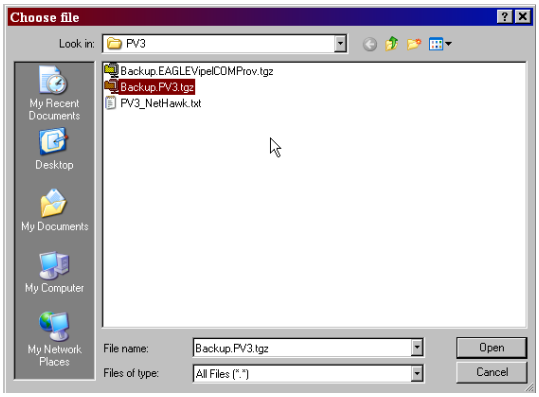
Procedure 1: Recovery Scenario 1

14 ☐	**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: 
15 ☐	**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 backup is complete and the system is stabilized. 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 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.
16 ☐	**ACTIVE NOAM:** Login	Login to the recovered Active NOAM via SSH terminal as ***root (5.0) or admusr(6.0+)*** user.

Procedure 1: Recovery Scenario 1

17 ☐	**ACTIVE NOAM:** Restore /etc/hosts/ File of the Active NOAM (DSR 5.0/6.0/7.0 ONLY)	**IF DSR 7.1 and Higher, SKIP THIS STEP** Execute the following command: `$ sudo AppWorks AppWorks_AppWorks updateServerAliases <NOAM Host Name>`
18 ☐	**NOAM VIP GUI:** Re-enable Provisioning	Navigate to **Main Menu->Status & Manage->Database**  Click on the **Enable Provisioning**. A pop-up window will appear to confirm as shown below, press **OK**. 
19 ☐	**NOAM VIP GUI:** Recover Standby NOAM	Install the second NOAM server by executing procedure *"Configure the Second NOAM Server"*, steps 1, 4, 5, and 6 - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. **Note:** Execute step 8 if Netbackup is used. If NetBackup is used, execute procedure *"NetBackup Client Installation"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. **Note:** If Topology or nodeId alarms are persistent after the database restore, refer to **Appendix G**. Workarounds for Issues not fixed in this Release
20 ☐	**NOAM VIP GUI:** Recover Active SOAM Server	Install the Active SOAM server by executing procedure *"Configure the SOAM Servers"*, steps 1-9. - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. **Note:** If you are using NetBackup, also execute step 11.

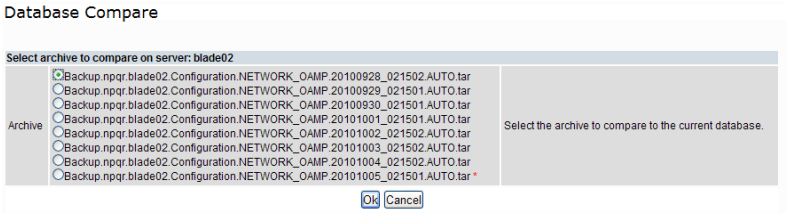
Procedure 1: Recovery Scenario 1

21 ☐	**NOAM VIP GUI:** Upload the backed up SOAM Database file	Navigate to **Main Menu->Status & Manage->Files** Select the Active SOAM server. 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.  Click on Browse and Locate the backup file and 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.

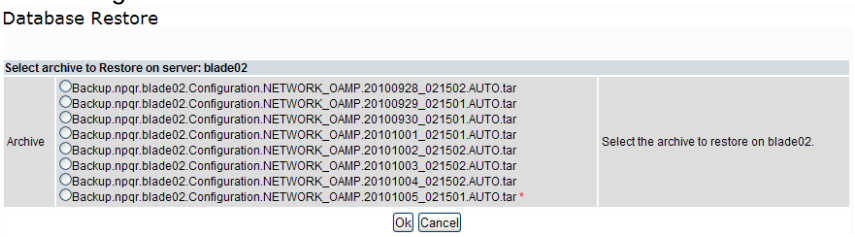
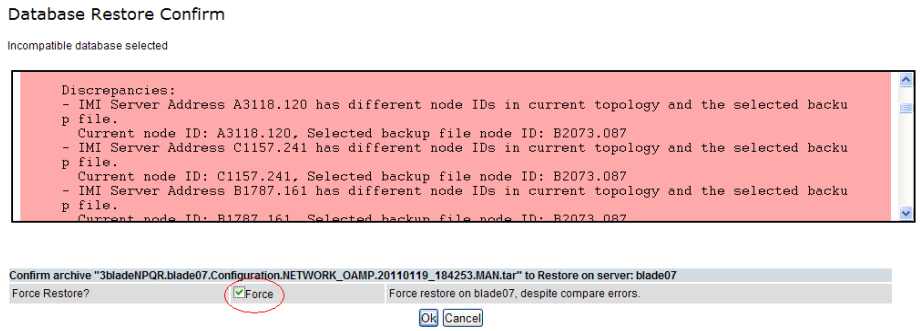
Procedure 1: Recovery Scenario 1

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

Procedure 1: Recovery Scenario 1

23 ☐	**Recovered SOAM GUI:** Verify the Archive Contents and Database Compatibility	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 22** of this procedure.  **Verify** that the output window matches the screen below. **Note:** You will get a database mismatch regarding the NodeIDs of the VMs. That is expected. If that is the only mismatch, proceed, otherwise stop and contact **Appendix H. My Oracle** Support (MOS)  **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.

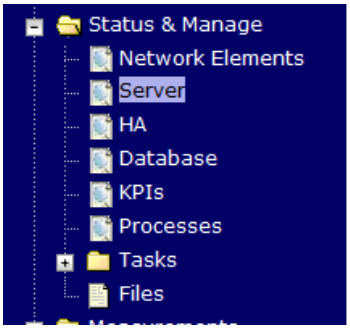
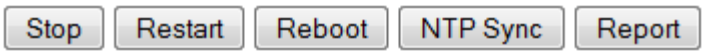
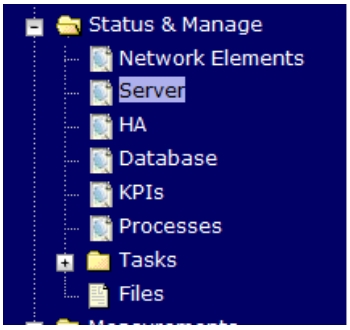
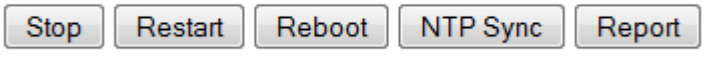
Procedure 1: Recovery Scenario 1

24 ☐	**Recovered SOAM GUI:** Restore the Database	Click on **Main Menu->Status & Manage->Database** 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 that the NodeIDs do not match. That is expected. If no other errors beside the NodeIDs 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.
25 ☐	**Recovered SOAM GUI**: Monitor and Confirm database restoral	Wait for **5-10 minutes** for the System to stabilize with the new topology: Monitor the Info tab for **"Success"**. This will indicate that the backup 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.

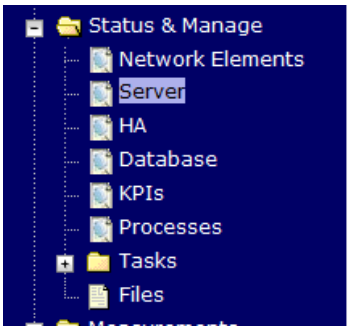
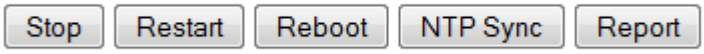
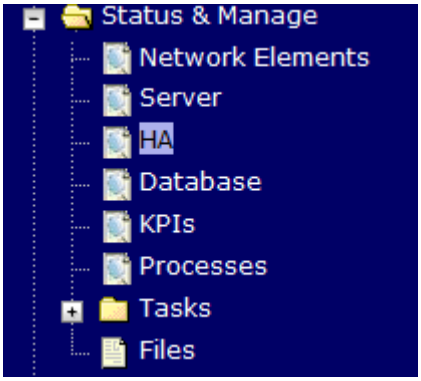
Procedure 1: Recovery Scenario 1

26 ☐	**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: 
27 ☐	**NOAM VIP GUI:** Recover the standby SOAM Server	Recover the **standby** SOAM server by repeating the following steps for each SOAM server: 1. Install the remaining SOAM servers by executing reference Procedure *"Configure the SOAM Servers"*, steps 1, 5, 6, 7, 8, and 9. - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. **Note:** Execute step 11 as well if NetBackup is used. 2. If you are using Netbackup, execute procedure *"NetBackup Client Installation"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure..

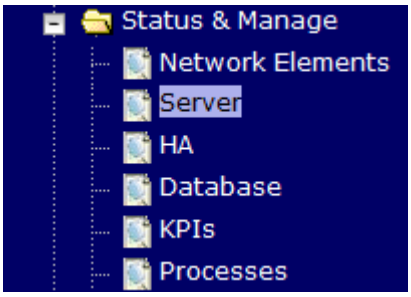
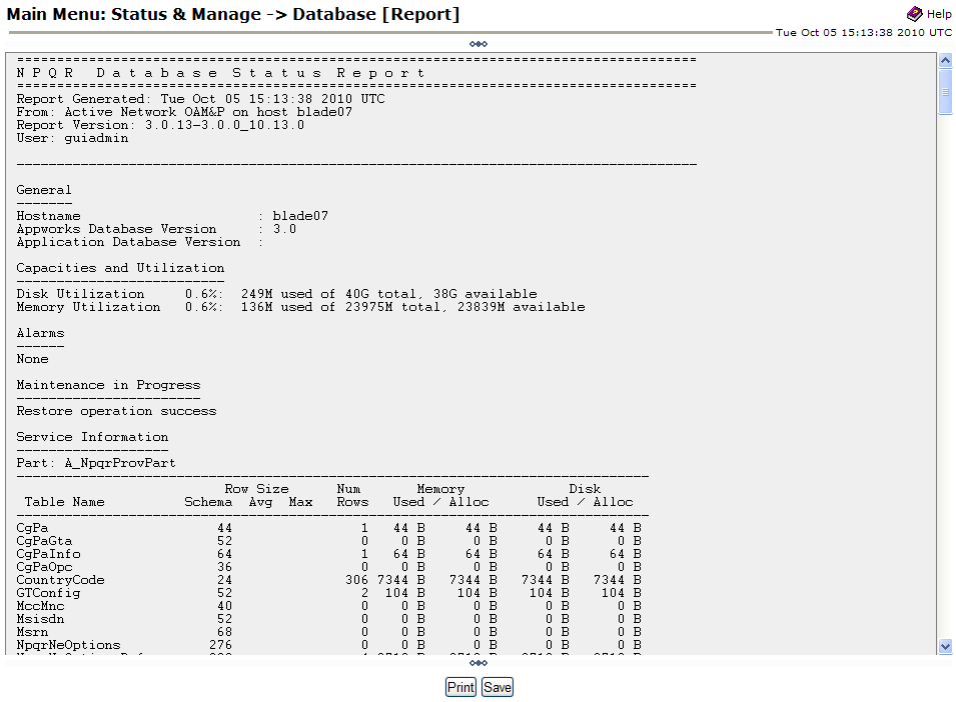
Procedure 1: Recovery Scenario 1

28 ☐	**NOAM VIP GUI:** Restart DSR application	Navigate to **Main Menu->Status & Manage->Server**,  Select the recovered server and click on **Restart**. 
29 ☐	**NOAM VIP GUI:** Recover the C-Level Server (DA-MP, SBRs, IPFE, SS7-MP)	Execute procedure *"Configure MP Servers"*, Steps 1, 5, 6, 7, 8, and 9 - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. **Note:** Also execute steps 9 and 10 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. **Note:** –**DSR 5.0/6.0/7.0 ONLY**: If this server is an IPFE server, ensure ipfeNetUpdate.sh from procedure *"IP Front End (IPFE) Configuration (Optional)"* from [5] has been executed. Repeat this step for any remaining failed MP servers.
30 ☐	**NOAM VIP GUI:** Restart DSR Application on recovered C-Level Servers.	Navigate to **Main Menu->Status & Manage->Server**  Select the recovered servers and click on **Restart**. 

Procedure 1: Recovery Scenario 1

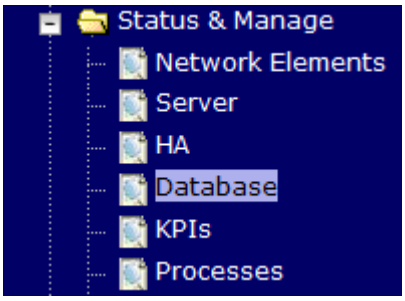
31 ☐	**NOAM VIP GUI:** Re-Sync NTP	Navigate to **Status & Manage -> Server**  Select each server that has been recovered and click **NTP Sync**. 
32 ☐	**NOAM VIP GUI:** Set HA on all C-Level Servers	Navigate to **Status & Manage -> HA**  Click on **Edit** at the bottom of the screen For each server whose Max Allowed HA Role is set to Standby, set it to **Active** Press **OK**
33 ☐	**ACTIVE NOAM:** Activate Optional Features	Establish an SSH session to the active NOAM, login as ***admusr.*** Refer to **Section 1.5** to activate any features that were previously activated. **Note:** While following the activation procedure, there may be application specific alarms present. Ignore these alarms and continue with the activation.

Procedure 1: Recovery Scenario 1

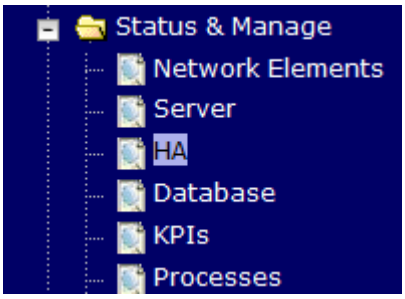
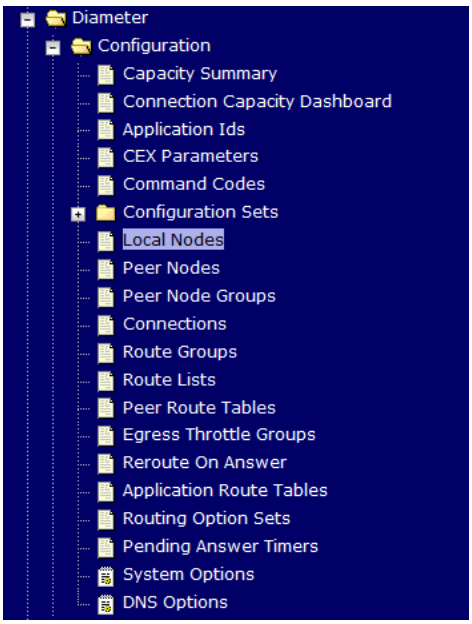
34 ☐	**NOAM VIP GUI:** Fetch and Store the database Report for the Newly Restored Data and Save it	Navigate to **Configuration-> Server**  Select the **active** NOAM server and click on the **Report** button at the bottom of the page. The following screen is displayed:  Click on **Save** and save the report to your local machine.

Procedure 1: Recovery Scenario 1

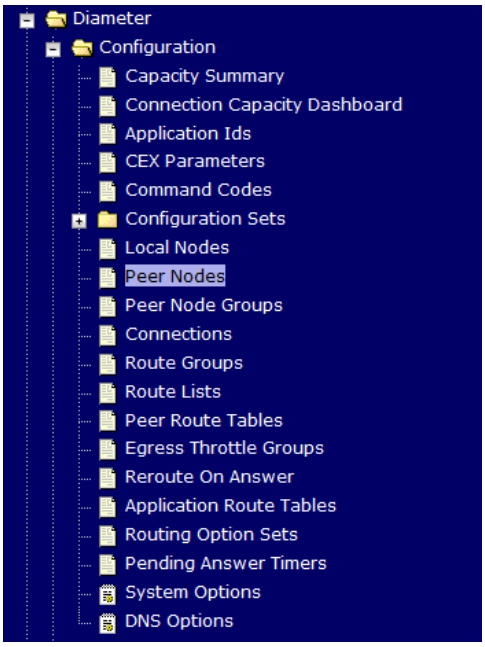
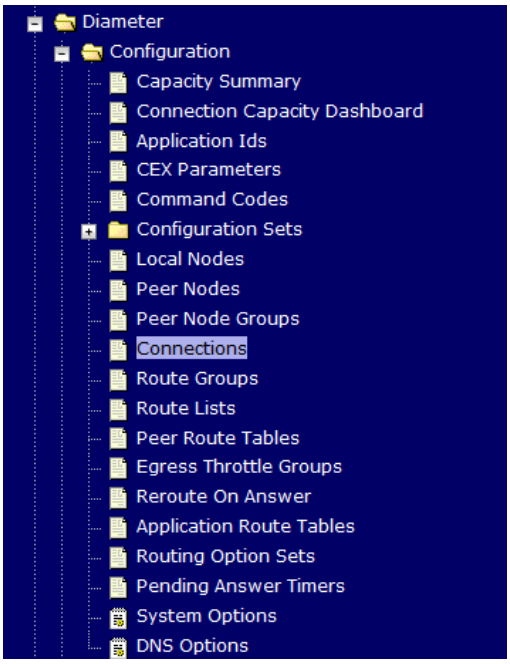
35 ☐	**ACTIVE NOAM:** Verify Replication Between Servers.	Login to the Active NOAM via SSH terminal as ***root(5.0) or admusr(6.0+)*** user.
		
		Execute the following command to verify replication is functioning as expected between the servers:
		
		$ sudo irepstat –m
		
		A similar output as the following shall be displayed:
		
		`-- Policy 0 ActStb [DbReplication] ----------`
		`RDU06-MP1 -- Stby`
		`  BC From RDU06-SO1 Active  0  0.50 ^0.17%cpu 42B/s  A=none`
		`  CC From RDU06-MP2 Active  0  0.10 ^0.17 0.88%cpu 32B/s  A=none`
		`RDU06-MP2 -- Active`
		`  BC From RDU06-SO1 Active  0  0.50 ^0.10%cpu 33B/s  A=none`
		`  CC To  RDU06-MP1 Active  0  0.10  0.08%cpu 20B/s  A=none`
		`RDU06-NO1 -- Active`
		`  AB To  RDU06-SO1 Active  0  0.50 1%R 0.03%cpu 21B/s`
		`RDU06-SO1 -- Active`
		`  AB From RDU06-NO1 Active  0  0.50 ^0.04%cpu 24B/s`
		`  BC To  RDU06-MP1 Active  0  0.50 1%R 0.04%cpu 21B/s`
		`  BC To  RDU06-MP2 Active  0  0.50 1%R 0.07%cpu 21B/s`

36 ☐	**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	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
---	---	---	---	---	---	---	---	---	---	---
NO_10303	NO2	Network OAM&P	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg
SO_10303	PSBR	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg
SO_10303	MP2	MP	Active	Active	Normal	0	Normal	Normal	Allowed	AutoInProg
SO_10303	SO1	System OAM	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg
NO_10303	NO1	Network OAM&P	Standby	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg
SO_10303	IPFE	MP	Active	OOS	Normal	0	Normal	Normal	Allowed	AutoInProg
SO_10303	SO2	System OAM	Active	OOS	Normal	0	Normal	NotApplicabl	Allowed	AutoInProg

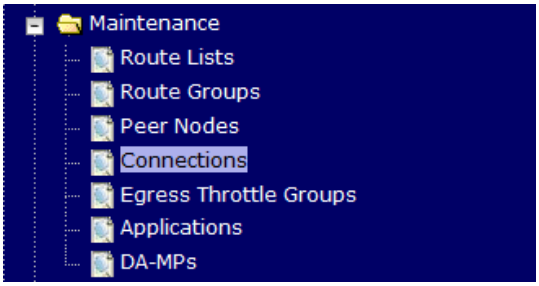
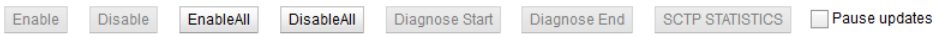
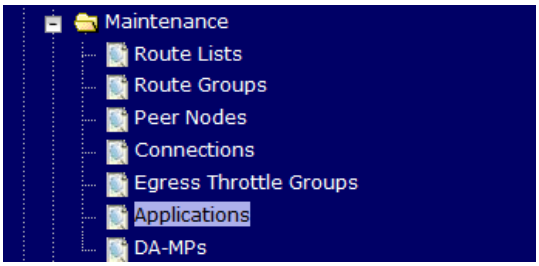
Procedure 1: Recovery Scenario 1

37 ☐	**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 Max HA Role** | **Application Max HA Role** | **Max Allowed HA Role** | **Mate Hostname List** | **Network Element** | **Server Role** | **Active VIPs** NO2 | Active | OOS | Active | NO1 | NO_10303 | Network OAM&P | 10.240.70.132 SO1 | Standby | OOS | Active | SO2 | SO_10303 | System OAM | SO2 | Active | OOS | Active | SO1 | SO_10303 | System OAM | 10.240.70.133 MP1 | Standby | Active | Active | MP2 | SO_10303 | MP | MP2 | Active | Active | Active | MP1 | SO_10303 | MP | IPFE | Active | OOS | Active | | SO_10303 | MP |
38 ☐	**SOAM VIP GUI:** Verify the Local Node Info	Navigate to **Main Menu->Diameter->Configuration->Local Node**  Verify that all the local nodes are shown.

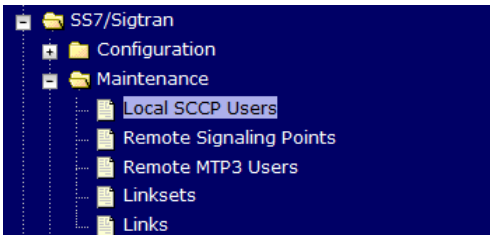
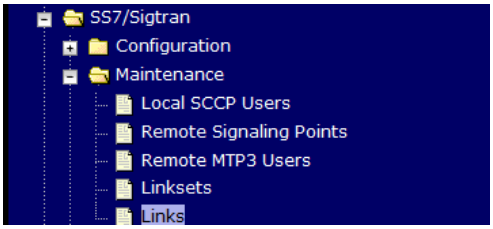
Procedure 1: Recovery Scenario 1

39 ☐	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.
40 ☐	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections**  Verify that all the connections are shown.

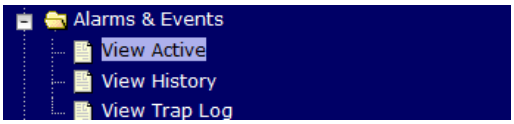
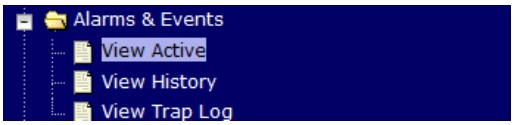
Procedure 1: Recovery Scenario 1

41 ☐	**MP Servers:** Disable SCTP Auth Flag- DSR 7.1 Only	For DSR 7.1 Only: For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix in [5]. Execute this procedure on all Failed MP Servers.
42 ☐	**SOAM VIP GUI:** Enable Connections if needed	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
43 ☐	**SOAM VIP GUI:** Enable Optional Features	Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**  Select the optional feature application configured in **step 37**. Click the **Enable** button. 

Procedure 1: Recovery Scenario 1

44 ☐	**SOAM VIP GUI:** Re-enable Transports if Needed (Applicable ONLY for DSR 6.0+)	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.
45 ☐	**SOAM VIP GUI:** Re-enable MAPIWF application if needed (Applicable ONLY for DSR 6.0+)	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.
46 ☐	**SOAM VIP GUI:** Re-enable links if needed (Applicable ONLY for DSR 6.0+)	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 1: Recovery Scenario 1

47 ☐	**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** H. My Oracle Support **(**MOS).
48 ☐	**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** H. My Oracle Support **(**MOS).
49 ☐	**Restore GUI Usernames and Passwords**	If applicable, Execute steps in **Section 6.0** to recover the user and group information restored.
50 ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**. DSR Database Backup to back up the Configuration databases:

5.1.2 Recovery Scenario 2 (Partial Outage with one Core RMS Server Intact)

For a partial outage with one core RMS server intact and available; the second RMS and expansion servers (if applicable) are recovered using recovery procedures of base hardware and software. All VMs are recovered using recovery procedures. Database replication 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 Base Hardware and Software for Failed RMS Server.

- Recover the base hardware
- Recover the Virtual Machines.
- Recover the software.

Recover PMAC if needed

Recover standby NOAM Guest

- Reconfigure the application

Recover standby SOAM and MP Guest

- Reconfigure the Application

Restart processes and re-enable provisioning and replication.

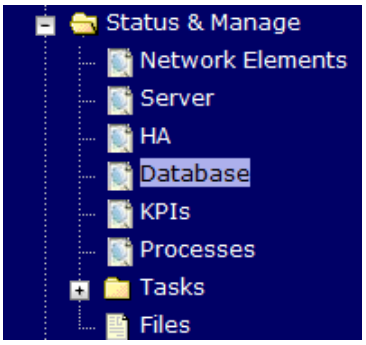
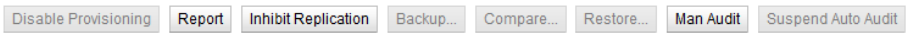
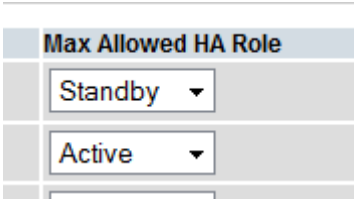
Procedure 2: Recovery Scenario 2

S T E P #	This procedure performs recovery if one core RMS server is intact. 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 H. 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 ☐	**Remove the Failed RMS Servers and Replace**	Remove the failed RMS Servers and Install replacement **Note:** If a partial failure occurred that impacts some of the VMs and not the entire server, execute the steps that relate to the failed VM.

Procedure 2: Recovery Scenario 2

4 ☐	**NOAM VIP GUI:** Login	Login to the NOAM GUI as the ***guiadmin*** user: 

Procedure 2: Recovery Scenario 2

5 ☐	**NOAM VIP GUI:** Disable Replication and set HA on Failed Servers	Navigate to **Main Menu -> Status & Manage -> Database**  Select the failed servers. Press the **Inhibit Replication** button  Navigate to **Main Menu -> Status & Manage -> HA** Select the **Edit** button  Select the failed Servers and set the *Max Allowed HA Role* to **Standby** 

Procedure 2: Recovery Scenario 2

6 ☐	**Recover RMS Server:** With PMAC	Execute this step if the failed RMS hosts the PMAC, otherwise skip to **step 7**: 1. Configure and verify the BIOS on the RMS. Execute procedure *"Configure the RMS Server BIOS Settings and Update Firmware"* – Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 2. Execute procedure *"Install TVOE on First RMS Server"* – Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. *3.* Execute procedure *"First RMS Configuration"* – Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 4. Recover the PMAC –Refer to **Table 5**: PMAC Disaster Recovery Reference Table for applicable PMAC Disaster Recovery Procedure. 5. Execute procedure *"Install TVOE on Additional Rack Mount Servers"* – Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. **Note:** This step can also be done for expansion servers (as mentioned in step 4) if needed, to reduce recovery time. *6.* **E**xecute procedure *"Configure TVOE on Additional Rack Mount Server"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 7. Execute procedure *"Load DSR and TPD ISO to the PMAC Server"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. *8.* Execute procedure *"Create NOAM Guest VMs"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. *9.* Execute procedure *"Create SOAM Guest VMs"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. *10.* Execute procedure *"Create MP Guest VMs"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 11. Execute procedure "Create IPFE Guest VMs" - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 12. IPM all the guests using procedure "Install the Software on Virtual Machines"- Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 13. If NetBackup was previously installed on the system, follow the Appendix *"Application NetBackup Client Installation Procedures"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure.

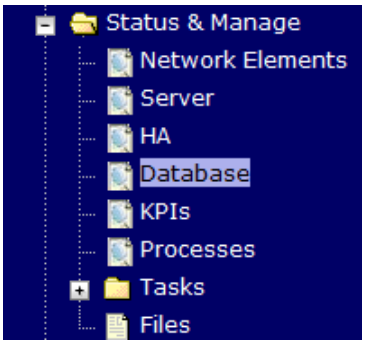
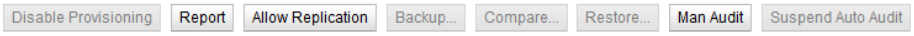
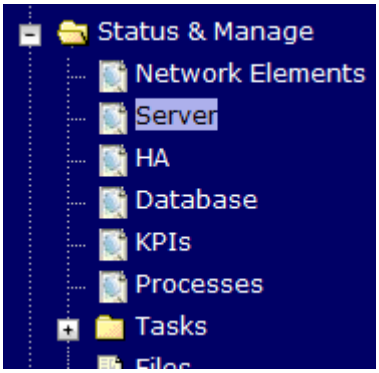
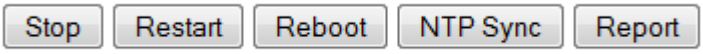
Procedure 2: Recovery Scenario 2

7 ☐	**Recover RMS Server:** Without PMAC	Execute this step if the failed RMS **DOES NOT** hosts the PMAC, otherwise skip this step. 1. Configure and verify the BIOS on the RMS. Execute procedure *"Configure the RMS Server BIOS Settings and Update Firmware"* – Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 2. Execute procedure *"Install TVOE on Additional Rack Mount Servers"* – Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. **Note:** This step can also be done for expansion servers (as mentioned in step 4) if needed, to reduce recovery time. *3.* **E**xecute procedure *"Configure TVOE on Additional Rack Mount Server"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 4. Execute procedure *"Load DSR and TPD ISO to the PMAC Server"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. *5.* Execute procedure *"Create NOAM Guest VMs"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. *6.* Execute procedure *"Create SOAM Guest VMs"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. *7.* Execute procedure *"Create MP Guest VMs"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 8. Execute procedure "Create IPFE Guest VMs" - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 9. IPM all the guests using procedure "Install the Software on Virtual Machines"- Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 10. If NetBackup was previously installed on the system, follow the Appendix *"Application NetBackup Client Installation Procedures"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure.

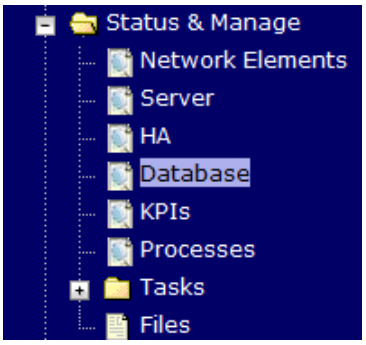
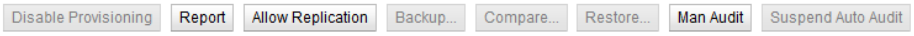
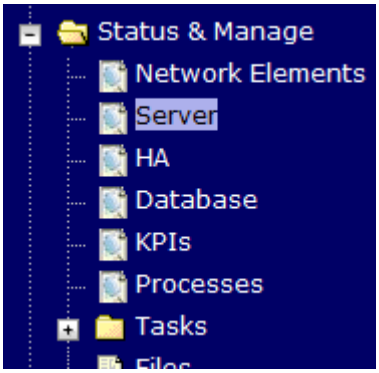
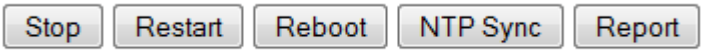
Procedure 2: Recovery Scenario 2

8 ☐	**Recover Expansion Servers**	Recover the expansion servers if needed (DSR 6.x and higher): 1. Configure and verify the BIOS on the RMS. Execute procedure *"Configure the RMS Server BIOS Settings and Update Firmware"* – Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 2. Execute procedure *"Install TVOE on Additional Rack Mount Servers"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 3. Execute procedure *"Configure TVOE on Additional Rack Mount Servers"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 4. Execute procedure *"Create MP Guest VMs"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 5. IPM all the guests created in this step using procedure *"Install the Software on Virtual Machines"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure.
9 ☐	**NOAM VIP GUI:** Recover NOAM	Recover the NOAM by executing the following steps: Configure the newly installed NOAM by executing procedure *"Configure the Second NOAM Server",* steps 1-2, 4-7 - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. **Note**: If installing NetBackup, execute step 12

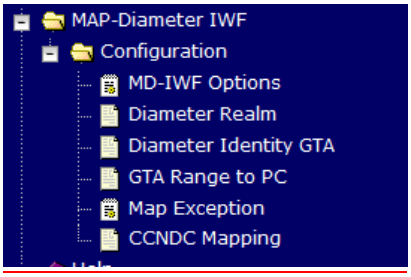
Procedure 2: Recovery Scenario 2

10 ☐	**NOAM VIP GUI:** Re-Enable Replication and Restart on the Failed NOAM	Navigate to **Main Menu -> Status & Manage -> Database**  Select the failed NOAM. Press the **Allow Replication** Button  Navigate to **Main Menu->Status & Manage->Server**  Select the recovered NOAM and click the **Restart** button 
11 ☐	**NOAM VIP GUI:** Recover SOAM	Recover the SOAM by executing the following steps: Configure the newly installed SOAM by executing procedure *"Configure the SOAM Servers"*, steps 1-3, 5-9 - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. **Note**: If installing NetBackup, execute step 11

Procedure 2: Recovery Scenario 2

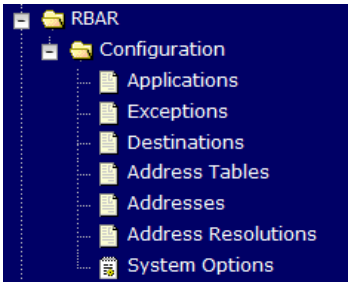
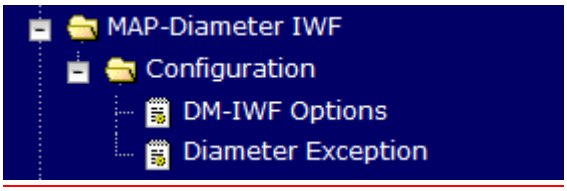
12 ☐	**NOAM VIP GUI:** Re-Enable Replication and Restart on the Failed SOAM	Navigate to **Main Menu -> Status & Manage -> Database**  Select the failed SOAM. Press the **Allow Replication** Button  Navigate to **Main Menu->Status & Manage->Server**  Select the recovered SOAM and click the **Restart** button 

Procedure 2: Recovery Scenario 2

13 ☐	**Recovered NOAM:** Verify Optional Feature Folder Exists (Map-Diameter IWF Only-DSR 6.0+) and activate	If Map-Diameter IWF was previously activated, Locate and verify the Map-Diameter IWF folder from Main Menu is visible and the configuration folder items are present:
		 
		For DSR 5.1, 6.0, and 7.0, you will have to run the following command to activate MAP-Diameter on the recovered NOAM:
		Note: For DSR 7.1, skip this step.
		`$ cd /usr/TKLC/dsr/prod/maint/loaders/activate`
		`$ ./load.mapinterworkingActivateAsourced`

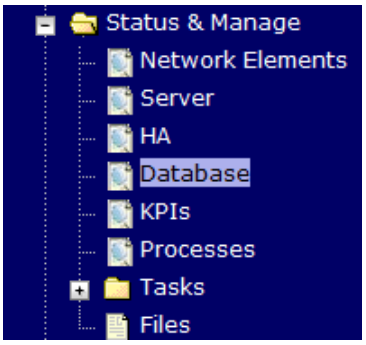
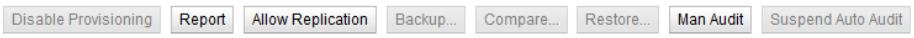
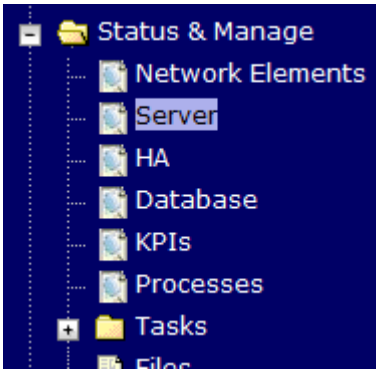
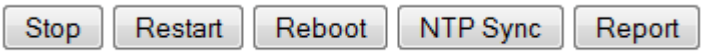
14 ☐	**Recovered SOAM GUI:** Login	Login to the Recovered SOAM GUI as the ***guiadmin*** user: 

Procedure 2: Recovery Scenario 2

15 ☐	**Recovered SOAM GUI:** Verify Optional Feature Folder Exists and activate	If optional features where previously activated (RBAR, Map-Diameter IWF), verify the folders are present under Main Menu of the recovered SOAM
		
		For RBAR:
		
		 
		
		For Map-Diameter Interworking:
		
		 
		
		For DSR 5.1, 6.0, and 7.0, you will have to run the following command to activate RBAR and/or MAP-Diameter on the recovered SOAM:
		
		Note: For DSR 7.1, skip this step.
		
		For RBAR:
		
		`$ cd /usr/TKLC/dsr/prod/maint/loaders/activate`
		`$ ./load.rbarActivateBsourced`
		
		For MAP-Diameter Interworking:
		
		`$ cd /usr/TKLC/dsr/prod/maint/loaders/activate`
		`$ ./load.mapinterworkingActivateBsourced`

16 ☐	**NOAM VIP GUI:** Recover MPs	Recover the failed DA-MP/IPFE/SS7-MP by executing the following steps: Configure the newly installed MP servers by executing procedure *"Configure MP Servers",* steps 1-2, 5-8 - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. For IPFE Servers, execute Procedure "*IP Front (IPFE) Configuration (Optional)"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. **Note:** For DSR 7.0+ skip steps 3-7 **Note:** Also execute step 9-10 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

17 ☐	**NOAM VIP GUI:** Re-Enable Replication and Restart on the Failed MP Servers	Navigate to **Main Menu -> Status & Manage -> Database**  Select the failed MP servers. Press the **Allow Replication** Button  Navigate to **Main Menu->Status & Manage->Server**  Select the recovered MP Servers and click the **Restart** button 

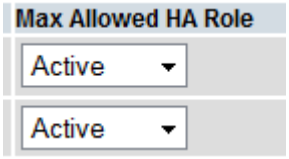
Procedure 2: Recovery Scenario 2

<table>
<tr>
<td>18
☐</td>
<td>NOAM VIP GUI:
Remove Forced Standby</td>
<td>Navigate to Main Menu -> Status & Manage -> HA

Select the Edit button

Select the failed Servers and set the Max Allowed HA Role to Active

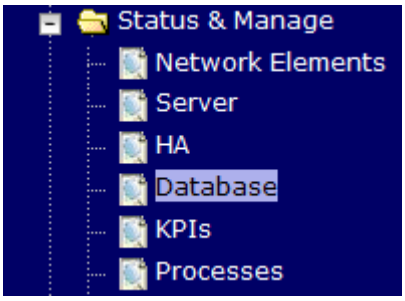
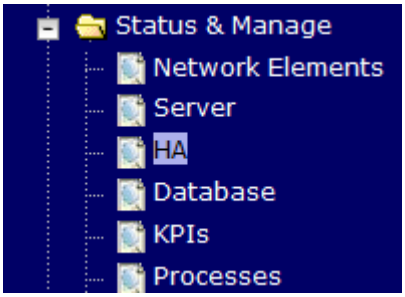
 
</td>
</tr>
<tr>
<td>19
☐</td>
<td>NOAM VIP GUI:
Verify Replication Between Servers</td>
<td>Execute the following command to verify replication is functioning as expected between the servers:

$ sudo irepstat –m

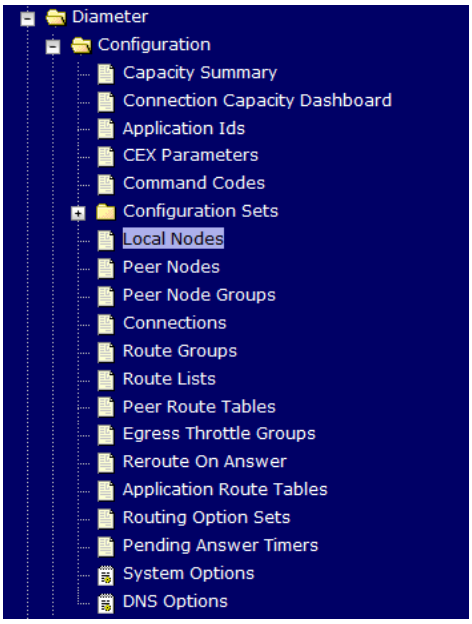
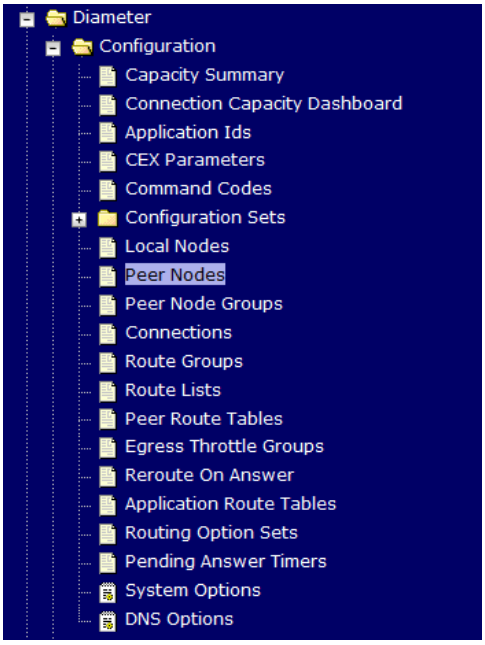
A similar output to below shall be generated:

-- Policy 0 ActStb [DbReplication] ----------
RDU06-MP1 -- Stby
BC From RDU06-SO1 Active 0 0.50 ^0.17%cpu 42B/s A=none
CC From RDU06-MP2 Active 0 0.10 ^0.17 0.88%cpu 32B/s A=none
RDU06-MP2 -- Active
BC From RDU06-SO1 Active 0 0.50 ^0.10%cpu 33B/s A=none
CC To RDU06-MP1 Active 0 0.10 0.08%cpu 20B/s A=none
RDU06-NO1 -- Active
AB To RDU06-SO1 Active 0 0.50 1%R 0.03%cpu 21B/s
RDU06-SO1 -- Active
AB From RDU06-NO1 Active 0 0.50 ^0.04%cpu 24B/s
BC To RDU06-MP1 Active 0 0.50 1%R 0.04%cpu 21B/s
BC To RDU06-MP2 Active 0 0.50 1%R 0.07%cpu 21B/s</td>
</tr>
</table>

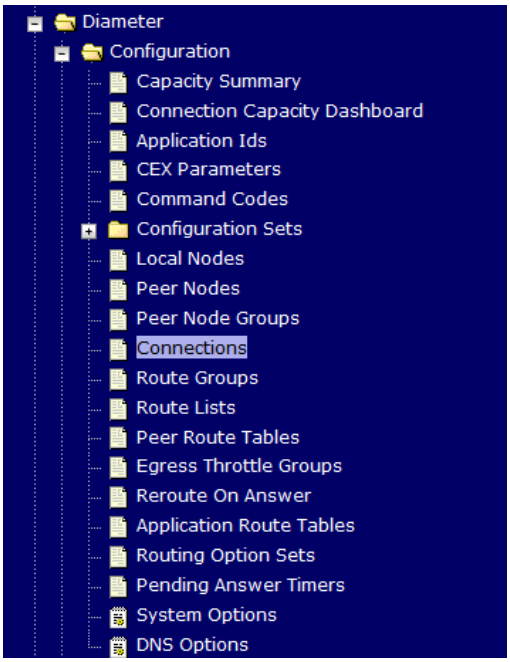
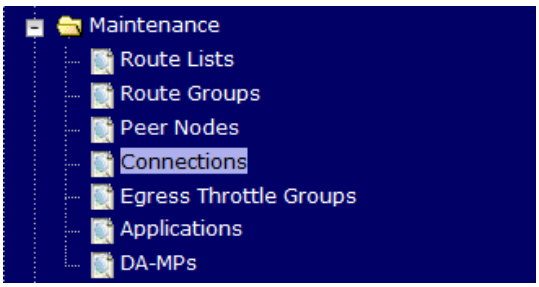
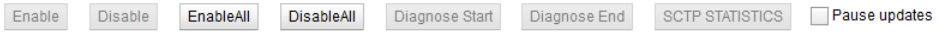
Procedure 2: Recovery Scenario 2

20 ☐	**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** / **Application Max HA Role** / **Status** / **DB Level** / **OAM Repl Status** / **SIG Repl Status** / **Repl Status** / **Repl Audit Status** NO_10303 / NO2 / Network OAM&P / Active / OOS / Normal / 0 / Normal / NotApplicabl / Allowed / AutoInProg SO_10303 / PSBR / MP / Active / Active / Normal / 0 / Normal / Normal / Allowed / AutoInProg SO_10303 / MP2 / MP / Active / Active / Normal / 0 / Normal / Normal / Allowed / AutoInProg SO_10303 / SO1 / System OAM / Standby / OOS / Normal / 0 / Normal / NotApplicabl / Allowed / AutoInProg NO_10303 / NO1 / Network OAM&P / Standby / OOS / Normal / 0 / Normal / NotApplicabl / Allowed / AutoInProg SO_10303 / IPFE / MP / Active / OOS / Normal / 0 / Normal / Normal / Allowed / AutoInProg SO_10303 / SO2 / System OAM / Active / OOS / Normal / 0 / Normal / NotApplicabl / Allowed / AutoInProg
21 ☐	**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 Max HA Role** / **Application Max HA Role** / **Max Allowed HA Role** / **Mate Hostname List** / **Network Element** / **Server Role** / **Active VIPs** NO2 / Active / OOS / Active / NO1 / NO_10303 / Network OAM&P / 10.240.70.132 SO1 / Standby / OOS / Active / SO2 / SO_10303 / System OAM / SO2 / Active / OOS / Active / SO1 / SO_10303 / System OAM / 10.240.70.133 MP1 / Standby / Active / Active / MP2 / SO_10303 / MP / MP2 / Active / Active / Active / MP1 / SO_10303 / MP / IPFE / Active / OOS / Active / / SO_10303 / MP /

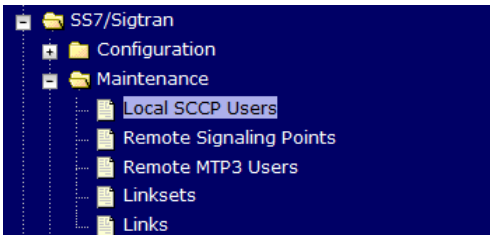
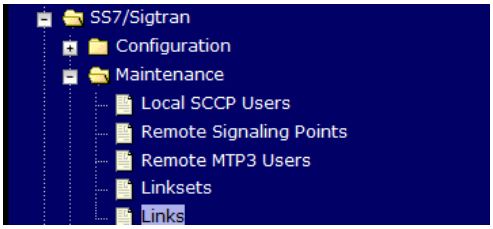
Procedure 2: Recovery Scenario 2

22 ☐	**SOAM VIP GUI:** Verify the Local Node Info	Navigate to **Main Menu->Diameter->Configuration->Local Node**  Verify that all the local nodes are shown.
23 ☐	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.

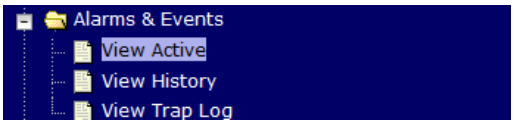
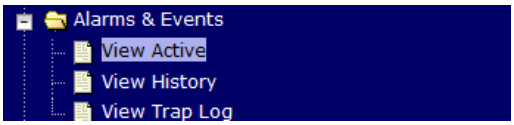
Procedure 2: Recovery Scenario 2

24 ☐	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections**  Verify that all the connections are shown.
25 ☐	**MP Servers:** Disable SCTP Auth Flag- DSR 7.1 Only	For DSR 7.1 Only: For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix in [5]. Execute this procedure on all Failed MP Servers.
26 ☐	**SOAM VIP GUI:** Enable Connections if needed	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 2: Recovery Scenario 2

27 ☐	**SOAM VIP GUI:** Re-enable Transports if Needed (Applicable ONLY for DSR 6.0+)	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.
28 ☐	**SOAM VIP GUI:** Re-enable MAPIWF application if needed (Applicable ONLY for DSR 6.0+)	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.
29 ☐	**SOAM VIP GUI:** Re-enable links if needed (Applicable ONLY for DSR 6.0+)	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 2: Recovery Scenario 2

30 ☐	**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** H. My Oracle Support **(**MOS).
31 ☐	**NOAM 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** H. My Oracle Support **(**MOS).
32 ☐	**Restore GUI Usernames and Passwords**	If applicable, Execute steps in **Section 6.0** to recover the user and group information restored.
33 ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**. DSR Database Backup to back up the Configuration databases:

5.1.3 Recovery Scenario 3 (Partial Outage with one or more Expansion Servers Failed)

For a partial outage with both core RMS servers intact and available; the Expansion RMS servesr are recovered using recovery procedures of base hardware and software. All VMs are recovered using recovery procedures. Database replication 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 Base Hardware and Software for Failed Expansion RMS Server.

- Recover the base hardware.
- Recover the Virtual Machines.
- Recover the software.

MP Guest

- Reconfigure the Application

Restart processes and re-enable provisioning and replication.

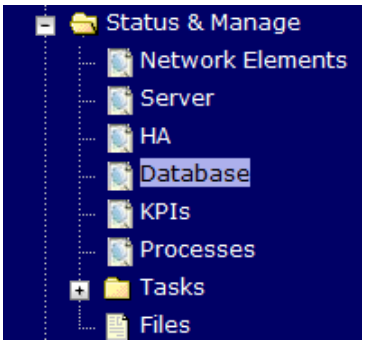
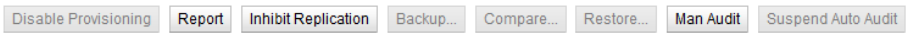
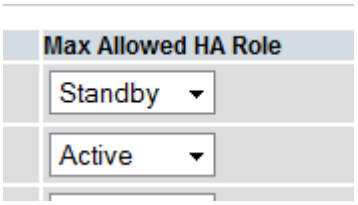
Procedure 3: Recovery Scenario 3

S T E P #	This procedure performs recovery if core RMS servers are intact. 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 H. 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 ☐	**Remove the Failed RMS Server and Replace**	Remove the failed RMS Server and Install replacement **Note:** If a partial failure occurred that impacts some of the VMs and not the entire server, execute the steps that relate to the failed VM.

Procedure 3: Recovery Scenario 3

4 ☐	**NOAM VIP GUI:** Login	Login to the NOAM GUI as the ***guiadmin*** user: 

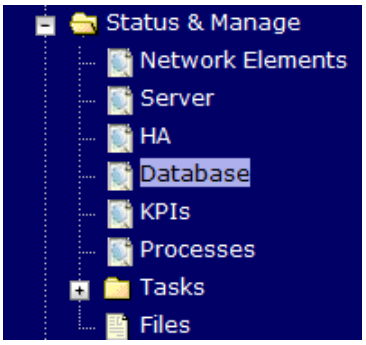
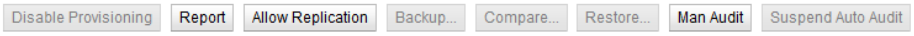
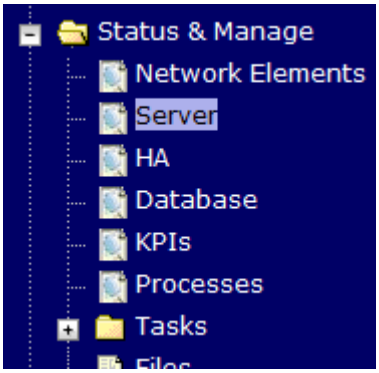
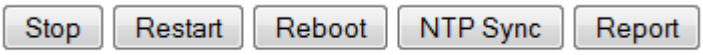
Procedure 3: Recovery Scenario 3

5 ☐	**NOAM VIP GUI:** Disable Replication and set HA on Failed Servers	Navigate to **Main Menu -> Status & Manage -> Database**  Select the failed servers. Press the **Inhibit Replication** button  Navigate to **Main Menu -> Status & Manage -> HA** Select the **Edit** button  Select the failed Servers and set the *Max Allowed HA Role* to **Standby** 

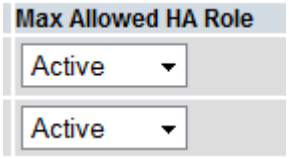
Procedure 3: Recovery Scenario 3

6 ☐	**Recover Expansion Servers**	Recover the expansion servers if needed (DSR 6.x and higher): 1. Configure and verify the BIOS on the RMS. Execute procedure *"Configure the RMS Server BIOS Settings and Update Firmware"* – Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 2. Execute procedure *"Install TVOE on Additional Rack Mount Servers"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 3. Execute procedure *"Configure TVOE on Additional Rack Mount Servers"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 4. Execute procedure *"Create MP Guest VMs"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. 5. IPM all the guests created in this step using procedure *"Install the Software on Virtual Machines"* - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure.
7 ☐	**NOAM VIP GUI:** Recover MPs	Recover the failed DA-MP/IPFE/SS7-MP by executing the following steps: Configure the newly installed MP servers by executing procedure *"Configure MP Servers",* steps 1-2, 5-8 - Refer to **Table 4**: DSR RMS Installation Reference Table for applicable DSR software RMS installation procedure. **Note:** Also execute step 9-10 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network

Procedure 3: Recovery Scenario 3

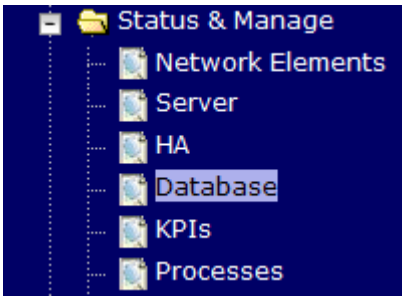
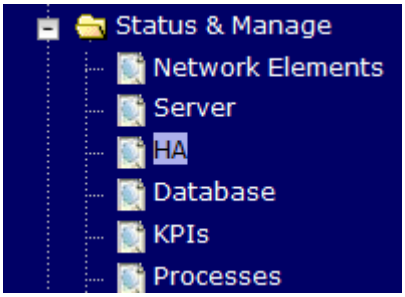
8 ☐	**NOAM VIP GUI:** Re-Enable Replication and Restart on the Failed MP Servers	Navigate to **Main Menu -> Status & Manage -> Database**  Select the failed MP servers. Press the **Allow Replication** Button  Navigate to **Main Menu->Status & Manage->Server**  Select the recovered MP Servers and click the **Restart** button 

Procedure 3: Recovery Scenario 3

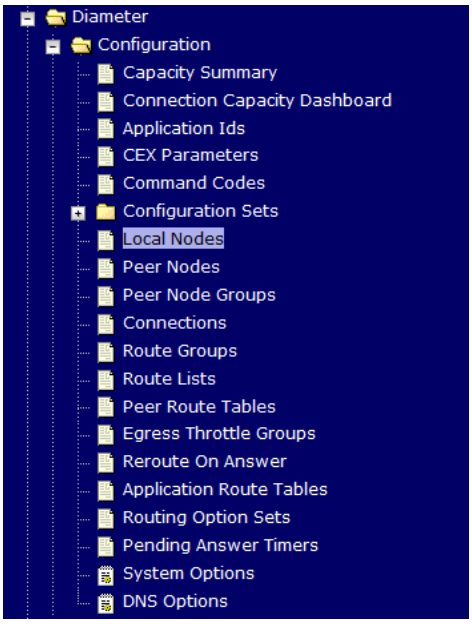
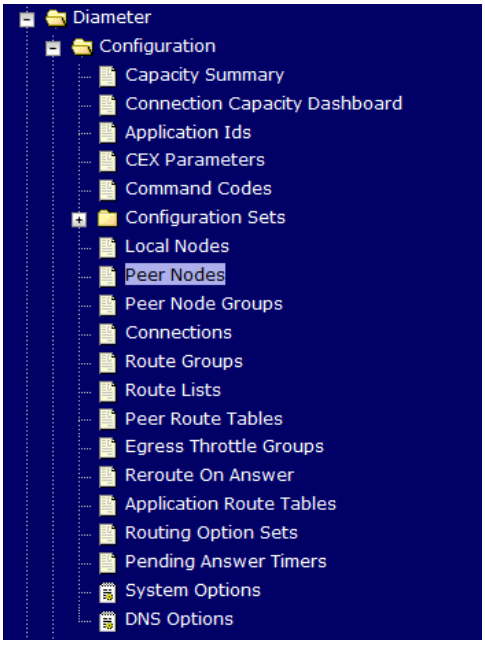
9 ☐	**NOAM VIP GUI:** Remove Forced Standby	Navigate to **Main Menu -> Status & Manage -> HA** Select the **Edit** button  Select the failed Servers and set the *Max Allowed HA Role* to **Active** 

10 ☐	**NOAM VIP GUI:** Verify Replication Between Servers	Execute the following command to verify replication is functioning as expected between the servers:
		
		$ sudo irepstat –m
		
		An output similar to below shall be generated:
		
		`-- Policy 0 ActStb [DbReplication] ----------`
		`RDU06-MP1 -- Stby`
		`  BC From RDU06-SO1 Active  0  0.50 ^0.17%cpu 42B/s  A=none`
		`  CC From RDU06-MP2 Active  0  0.10 ^0.17 0.88%cpu 32B/s  A=none`
		`RDU06-MP2 -- Active`
		`  BC From RDU06-SO1 Active  0  0.50 ^0.10%cpu 33B/s  A=none`
		`  CC To  RDU06-MP1 Active  0  0.10  0.08%cpu 20B/s  A=none`
		`RDU06-NO1 -- Active`
		`  AB To  RDU06-SO1 Active  0  0.50 1%R 0.03%cpu 21B/s`
		`RDU06-SO1 -- Active`
		`  AB From RDU06-NO1 Active  0  0.50 ^0.04%cpu 24B/s`
		`  BC To  RDU06-MP1 Active  0  0.50 1%R 0.04%cpu 21B/s`
		`  BC To  RDU06-MP2 Active  0  0.50 1%R 0.07%cpu 21B/s`

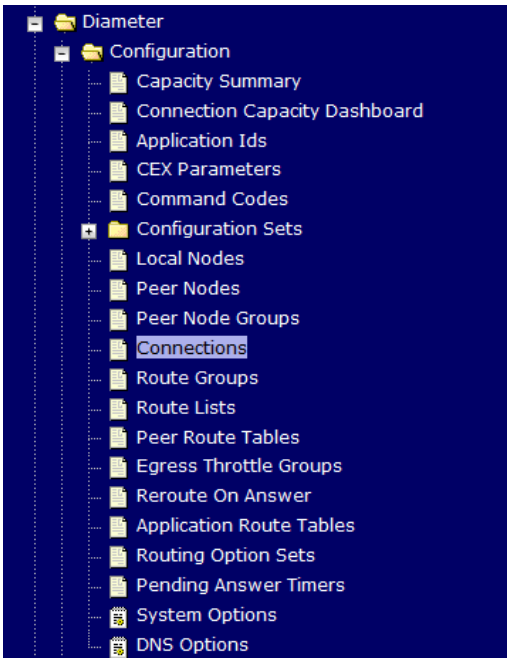
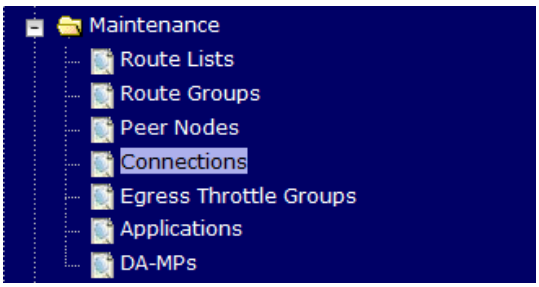
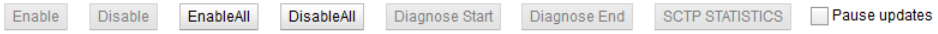
Procedure 3: Recovery Scenario 3

11 ☐	**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 | Application Max HA Role | Status | DB Level | OAM Repl Status | SIG Repl Status | Repl Status | Repl Audit Status NO_10303 | NO2 | Network OAM&P | Active | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg SO_10303 | PSBR | MP | Active | Active | Normal | 0 | Normal | Normal | Allowed | AutoInProg SO_10303 | MP2 | MP | Active | Active | Normal | 0 | Normal | Normal | Allowed | AutoInProg SO_10303 | SO1 | System OAM | Standby | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg NO_10303 | NO1 | Network OAM&P | Standby | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg SO_10303 | IPFE | MP | Active | OOS | Normal | 0 | Normal | Normal | Allowed | AutoInProg SO_10303 | SO2 | System OAM | Active | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg
12 ☐	**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 Max HA Role | Application Max HA Role | Max Allowed HA Role | Mate Hostname List | Network Element | Server Role | Active VIPs NO2 | Active | OOS | Active | NO1 | NO_10303 | Network OAM&P | 10.240.70.132 SO1 | Standby | OOS | Active | SO2 | SO_10303 | System OAM | SO2 | Active | OOS | Active | SO1 | SO_10303 | System OAM | 10.240.70.133 MP1 | Standby | Active | Active | MP2 | SO_10303 | MP | MP2 | Active | Active | Active | MP1 | SO_10303 | MP | IPFE | Active | OOS | Active | | SO_10303 | MP |

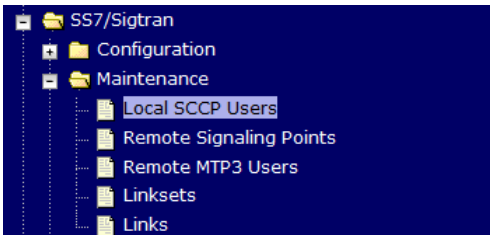
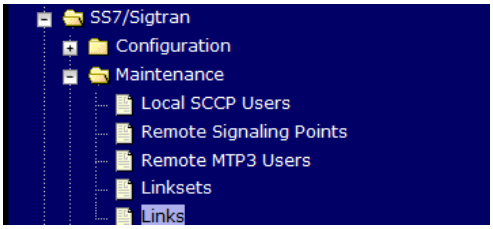
Procedure 3: Recovery Scenario 3

13 ☐	**SOAM VIP GUI:** Verify the Local Node Info	Navigate to **Main Menu->Diameter->Configuration->Local Node**  Verify that all the local nodes are shown.
14 ☐	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.

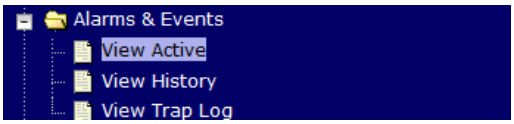
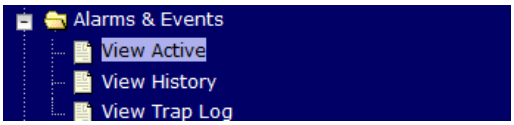
Procedure 3: Recovery Scenario 3

15 ☐	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections**  Verify that all the connections are shown.
16 ☐	**MP Servers:** Disable SCTP Auth Flag- DSR 7.1 Only	For DSR 7.1 Only: For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix in [5]. Execute this procedure on all Failed MP Servers.
17 ☐	**SOAM VIP GUI:** Enable Connections if needed	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

18 ☐	**SOAM VIP GUI:** Re-enable Transports if Needed (Applicable ONLY for DSR 6.0+)	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.
19 ☐	**SOAM VIP GUI:** Re-enable MAPIWF application if needed (Applicable ONLY for DSR 6.0+)	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.
20 ☐	**SOAM VIP GUI:** Re-enable links if needed (Applicable ONLY for DSR 6.0+)	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

21 ☐	**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** H. My Oracle Support **(**MOS).
22 ☐	**NOAM 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** H. My Oracle Support **(**MOS).
23 ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**. DSR Database Backup to back up the Configuration databases:

5.1.4 Recovery Scenario 4 (Both NOAM servers Failed with DR NOAM Available)

For a partial outage with both NOAM servers failed but a DR NO available, the DR NO 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 1. The major activities are summarized as follows:

Switch DR NOAM from secondary to primary

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

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

If applicable, recover any failed SOAM and MP servers by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.
- The database in intact at the active NOAM server and does not require restoration at the SOAM and MP servers.

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

Procedure 4: Recovery Scenario 4

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 H. 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 ☐	**Switch DR NOAM to Primary**	Execute **Appendix C**. Switching DR NOAM Site to Primary to have the DR NOAM become active.
4 ☐	**Recover System**	If **Both** SOAM servers have failed as well, execute **procedure 1** to recover the system.

Procedure 4: Recovery Scenario 4

5 ☐	**Recovered Active NOAM:** Login	Establish an SSH session to the recovered Active NOAM. Login as ***admusr***.
6 ☐	**Recovered Active NOAM:** Prepare recovered Active NOAM for optional feature activation (DSR 5.0/6.0/7.0)	**For DSR 5.0/6.0/7.0:** If DSR 7.1, skip this step Establish an SSH session to the Active SOAM, login as ***admusr.*** Execute the following command: `$ irem DsrApplication where "name in ('MD-IWF','DM-IWF')"`
7 ☐	**Recovered Active NOAM:** Verify Preparation (DSR 5.0/6.0/7.0)	**For DSR 5.0/6.0/7.0:** If DSR 7.1, skip this step Execute the following command to verify preparation of optional feature activation: `$ iqt -z -h -p -fname DsrApplication where "name in ('MD-IWF','DM-IWF')"` **Note:** There should be no output of this command, if there is, verify the correct entry of the command in **step 6**.

8 ☐	**Recovered Active NOAM:** Activate Optional Features	**For DSR 5.0/6.0/7.0:** If DSR 7.1, skip this step
		
		If MAP-Diameter IWF was previously activated, execute the following commands:
		
		`$ cd /usr/TKLC/dsr/prod/maint/loaders/activate`
		`$ ./load.mapinterworkingActivateAsourced`

9 ☐	**Recovered Standby NOAM:** Prepare and Activate Recovered Standby NOAM for Optional Feature Activation.	Repeat **Steps 5-8** for the preparing and activating previously activated features on the recovered Standby NOAM.
10 ☐	Switch DR NOAM Back to Secondary	Once the system have been recovered: Execute **Appendix D**. Returning a Recovered Site to Primary to have the recovered NOAM become primary again.

5.1.5 Recovery Scenario 5 (Database Recovery)

5.1.5.1 Recovery Scenario 5: Case 1

For a partial outage with

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

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

Procedure 5: Recovery Scenario 5 (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 H. 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 ☐	**Server in Question:** Login	Establish an SSH session to the server in question. Login as ***root(5.0)*** or ***admusr(6.0+)*** user.
3 ☐	**Server in Question:** Change runlevel to 3	Execute the following command to bring the system to runlevel 3. `$ sudo init 3`
4 ☐	**Server in Question:** Recover System	Execute the following command: `$ sudo /usr/TKLC/appworks/sbin/backout_restore` Follow the instructions that appear on the console prompt.
5 ☐	**Server in Question:** Change runlevel to 4	Execute the following command to bring the system back to runlevel 4. `$ sudo init 6`
6 ☐	**Server in Question:** Verify the server	Execute the following command to verify if the processes are up and running `$ sudo pm.getprocs`

Procedure 5: Recovery Scenario 5 (Case 1)

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

5.1.5.2 Recovery Scenario 5: Case 2

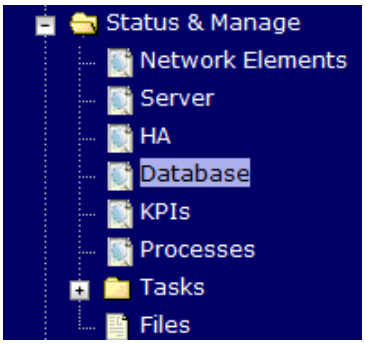
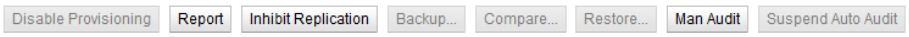
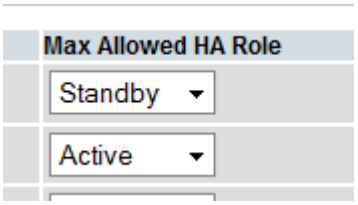
For a partial outage with

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

Procedure 5: Recovery Scenario 5 (Case 2)

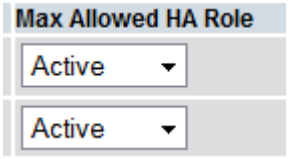
S T E P #	This procedure performs recovery if database got corrupted in the system and system is in the state to get replicated Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix H. My Oracle Support (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 ☐	**NOAM VIP GUI:** Login	Login to the NOAM GUI as the ***guiadmin*** user: 

Procedure 5: Recovery Scenario 5 (Case 2)

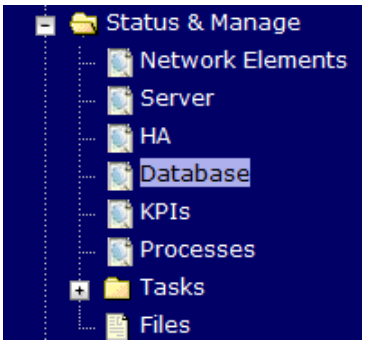
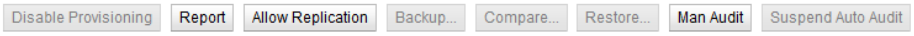
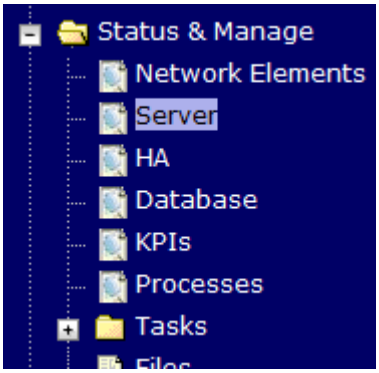
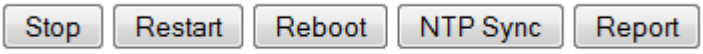
3 ☐	**NOAM VIP GUI:** Disable Replication and set HA on Failed Servers	Navigate to **Main Menu -> Status & Manage -> Database**  Select the failed servers. Press the **Inhibit Replication** button  Navigate to **Main Menu -> Status & Manage -> HA** Select the **Edit** button  Select the failed Servers and set the *Max Allowed HA Role* to **Standby** 
4 ☐	**Server in Question:** Login	Establish an SSH session to the server in question. Login as ***root(5.0)*** or ***admusr(6.0+)*** user.

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`

Procedure 5: Recovery Scenario 5 (Case 2)

6 ☐	**NOAM VIP GUI:** Remove Forced Standby	Navigate to **Main Menu -> Status & Manage -> HA** Select the **Edit** button  Select the failed Servers and set the *Max Allowed HA Role* to **Active** 
7 ☐	**Server in Question:** Restart	Execute the following commands to take the server to Dbup and start the DSR application: `$ sudo init 6`

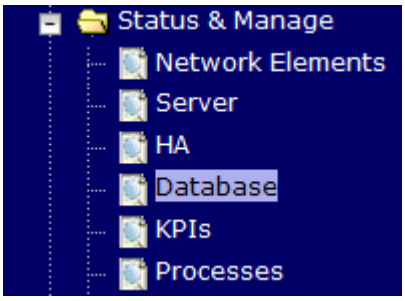
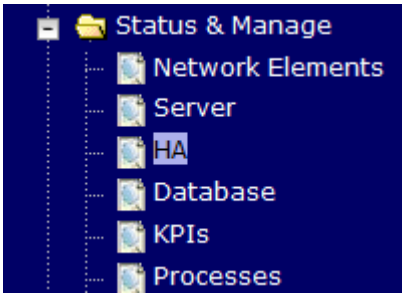
Procedure 5: Recovery Scenario 5 (Case 2)

8 ☐	**NOAM VIP GUI:** Re-Enable Replication and Restart on the Failed MP Servers	Navigate to **Main Menu -> Status & Manage -> Database**  Select the failed MP servers. Press the **Allow Replication** Button  Navigate to **Main Menu->Status & Manage->Server**  Select the recovered MP Servers and click the **Restart** button 

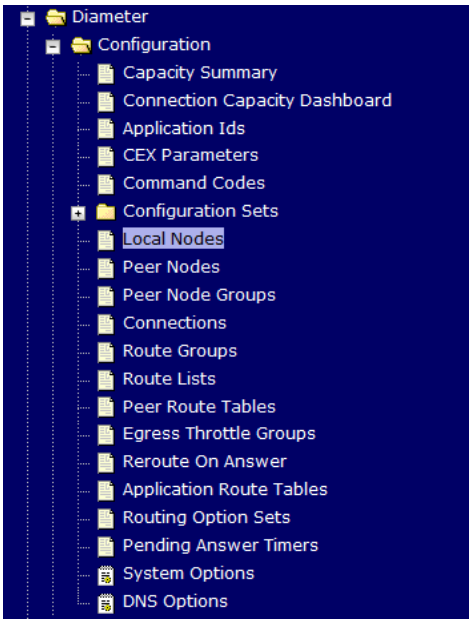
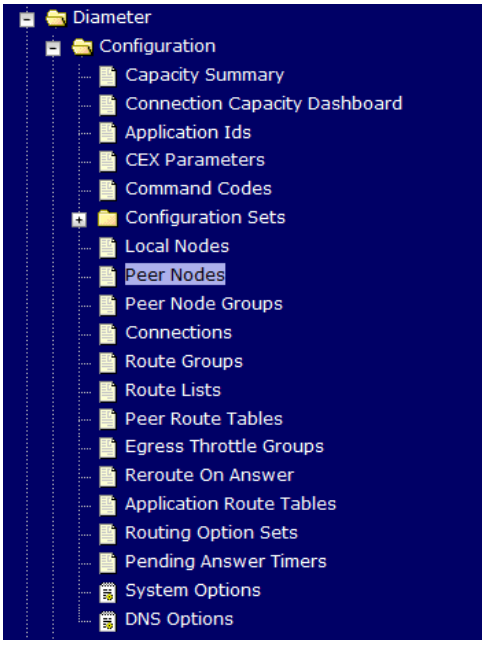
Procedure 5: Recovery Scenario 5 (Case 2)

9 ☐	**NOAM VIP GUI:** Verify Replication Between Servers	Execute the following command to verify processes, replication, and merging are functioning as expected between the servers: **$ sudo irepstat –m** An output similar to below shall be generated: -- Policy 0 ActStb [DbReplication] ---------- RDU06-MP1 -- Stby BC From RDU06-SO1 Active 0 0.50 ^0.17%cpu 42B/s A=none CC From RDU06-MP2 Active 0 0.10 ^0.17 0.88%cpu 32B/s A=none RDU06-MP2 -- Active BC From RDU06-SO1 Active 0 0.50 ^0.10%cpu 33B/s A=none CC To RDU06-MP1 Active 0 0.10 0.08%cpu 20B/s A=none RDU06-NO1 -- Active AB To RDU06-SO1 Active 0 0.50 1%R 0.03%cpu 21B/s RDU06-SO1 -- Active AB From RDU06-NO1 Active 0 0.50 ^0.04%cpu 24B/s BC To RDU06-MP1 Active 0 0.50 1%R 0.04%cpu 21B/s BC To RDU06-MP2 Active 0 0.50 1%R 0.07%cpu 21B/s **$ sudo pm.getprocs** An output similar to below shall be generated: **S pid procTag $1 stat spawnTime N cmd** **A 9597 CacdProcessRes 0 Up 06/01 10:13:30 1 cacd -v** **A 9598 DSROAM_Proc 0 Up 06/01 10:13:30 1 dsroam** **A 10202 Imysqld Up 06/01 10:04:20 1 Imysqld.start -force** **A 10203 ProcWatch Up 06/01 10:04:20 1 ProcWatch -L -w2097152** **A 10205 apwSoapServer Up 06/01 10:04:20 1 !CMNOSIGCHK=1 apwSoapServ er** **A 13480 cacd Up 06/01 10:04:52 1 ha.proc -s Active CacdPro cessRes** **A 10208 cmha Up 06/01 10:04:20 1 cmha** **A 10210 cmplatalarm Up 06/01 10:04:20 1 cmplatalarm** **A 10211 cmsnmpsa Up 06/01 10:04:20 1 cmsnmpsa -R 1.3.6.1.4.1.3 23.5.3.28.1** **A 10215 cmsoapa Up 06/01 10:04:20 1 cmsoapa** **A 8217 dsroam Up 06/01 10:08:10 1 ha.proc -s Active DSROAM_ Proc** **A 10240 eclipseHelp Up 06/01 10:04:20 1 eclipseHelp** **A 10218 idbsvc Up 06/01 10:04:20 1 idbsvc -M10 -ME204 -D40 - DE820 -W1 -S2** **A 13477 idbunlock Up 06/01 10:04:52 1 idbunlock -f** **A 10219 inetmerge Up 06/01 10:04:20 1 inetmerge** **A 10222 inetrep Up 06/01 10:04:20 1 inetrep** **A 10228 oampAgent Up 06/01 10:04:20 1 oampAgent** **A 10230 pm.watchdog Up 06/01 10:04:20 1 pm.watchdog** **A 10233 raclerk Up 06/01 10:04:20 1 raclerk -r 6000** **A 10234 re.portmap Up 06/01 10:04:20 1 re.portmap -c100** **A 10236 statclerk Up 06/01 10:04:20 1 statclerk -s -0** **A 10238 vipmgr Up 06/01 10:04:20 1 vipmgr** **A -1 AstateInit Done 06/01 10:04:52 1 AstateInit** **A -1 auditPTask Done 06/01 10:04:52 1 auditPeriodicTask** **A -1 auditTasks Done 06/01 10:04:52 1 auditDefunctTasks** **A -1 guiReqMapLoad Done 06/01 10:04:20 1 guiReqMapLoad** **A -1 mkdbhooks Done 06/01 10:04:20 1 mkdbhooks** **$ sudo inetmstat** An output similar to below shall be generated: nodeId InetMerge State dir dSeq dTime updTime info NO-1 Standby To 0 0.00 10:59:49 NO-1 Active From 0 0.00 10:59:49 SO-2 Active From 0 0.00 10:59:49 SO-1 Standby From 0 0.00 10:59:49

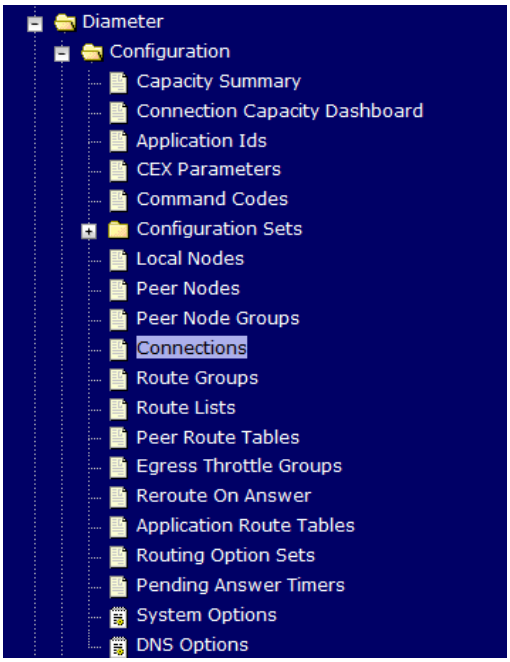
Procedure 5: Recovery Scenario 5 (Case 2)

10 ☐	**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 | Application Max HA Role | Status | DB Level | OAM Repl Status | SIG Repl Status | Repl Status | Repl Audit Status NO_10303 | NO2 | Network OAM&P | Active | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg SO_10303 | PSBR | MP | Active | Active | Normal | 0 | Normal | Normal | Allowed | AutoInProg SO_10303 | MP2 | MP | Active | Active | Normal | 0 | Normal | Normal | Allowed | AutoInProg SO_10303 | SO1 | System OAM | Standby | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg NO_10303 | NO1 | Network OAM&P | Standby | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg SO_10303 | IPFE | MP | Active | OOS | Normal | 0 | Normal | Normal | Allowed | AutoInProg SO_10303 | SO2 | System OAM | Active | OOS | Normal | 0 | Normal | NotApplicabl | Allowed | AutoInProg
11 ☐	**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 Max HA Role | Application Max HA Role | Max Allowed HA Role | Mate Hostname List | Network Element | Server Role | Active VIPs NO2 | Active | OOS | Active | NO1 | NO_10303 | Network OAM&P | 10.240.70.132 SO1 | Standby | OOS | Active | SO2 | SO_10303 | System OAM | SO2 | Active | OOS | Active | SO1 | SO_10303 | System OAM | 10.240.70.133 MP1 | Standby | Active | Active | MP2 | SO_10303 | MP | MP2 | Active | Active | Active | MP1 | SO_10303 | MP | IPFE | Active | OOS | Active | | SO_10303 | MP |

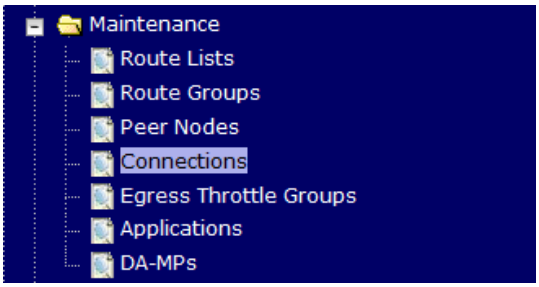
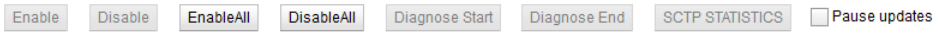
Procedure 5: Recovery Scenario 5 (Case 2)

12 ☐	**SOAM VIP GUI:** Verify the Local Node Info	Navigate to **Main Menu->Diameter->Configuration->Local Node**  Verify that all the local nodes are shown.
13 ☐	**SOAM VIP GUI:** Verify the Peer Node Info	Navigate to **Main Menu->Diameter->Configuration->Peer Node**  Verify that all the peer nodes are shown.

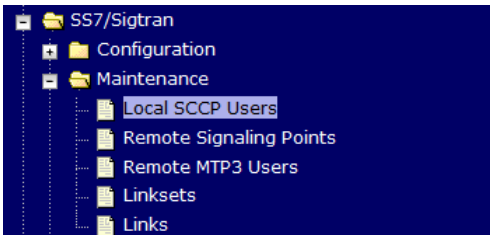
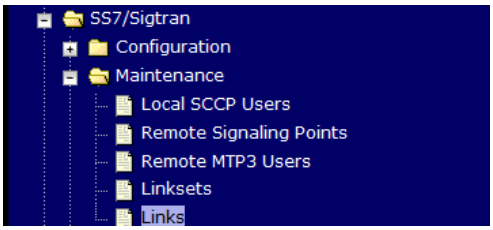
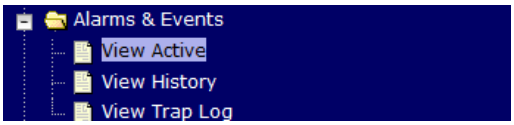
Procedure 5: Recovery Scenario 5 (Case 2)

14 ☐	**SOAM VIP GUI:** Verify the Connections Info	Navigate to **Main Menu->Diameter->Configuration->Connections**  Verify that all the connections are shown.
15 ☐	**MP Servers:** Disable SCTP Auth Flag- DSR 7.1 Only	For DSR 7.1 Only: For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix in [5]. Execute this procedure on all Failed MP Servers.

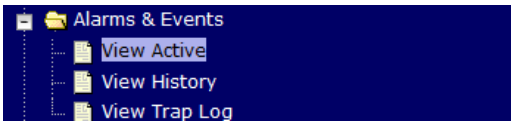
Procedure 5: Recovery Scenario 5 (Case 2)

16 ☐	**SOAM VIP GUI:** Enable Connections if needed	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
17 ☐	**SOAM VIP GUI:** Re-enable Transports if Needed (Applicable ONLY for DSR 6.0+)	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 5: Recovery Scenario 5 (Case 2)

18 ☐	**SOAM VIP GUI:** Re-enable MAPIWF application if needed (Applicable ONLY for DSR 6.0+)	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.
19 ☐	**SOAM VIP GUI:** Re-enable links if needed (Applicable ONLY for DSR 6.0+)	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.
20 ☐	**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** H. My Oracle Support **(**MOS).

Procedure 5: Recovery Scenario 5 (Case 2)

21 ☐	**NOAM 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** H. My Oracle Support **(**MOS).
22 ☐	**Backup and Archive All the Databases from the Recovered System**	Execute **Appendix A**. DSR 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.
```

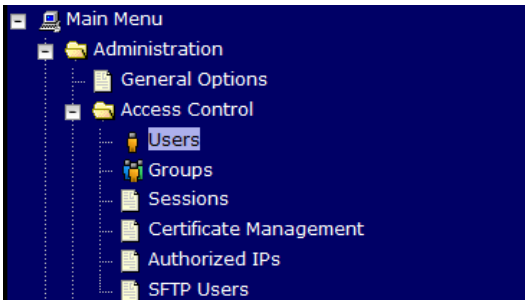
These users were removed prior to creation of the backup and archive file. They will be reintroduced by system restoration of that file.

6.2 Keeping a Restored user

Procedure 6: 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 H. 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 6: Keep Restored User

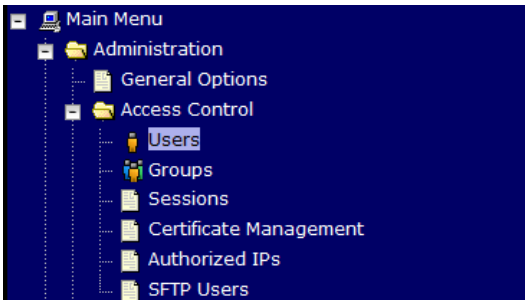
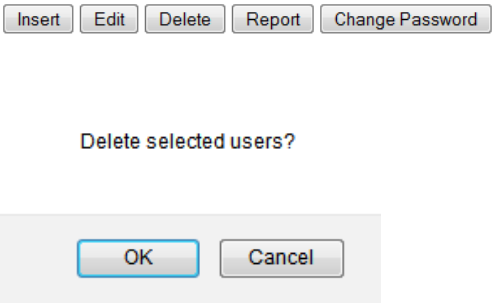
3 ☐	**After Restoration:** Reset User Passwords	Navigate to **Administration -> Access Control -> Users**  Select the user Click the **Change Password** button  Enter a new password  Click the **Continue** button

6.3 Removing a Restored User

Procedure 7: 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 H. 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 7: Remove the Restored User

2 ☐	**After Restoration:** Remove 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.

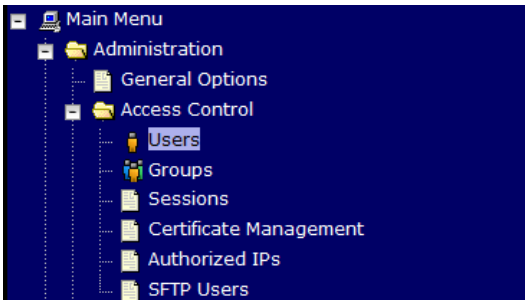
```
- User 'testuser' exists in current database but not in the selected backup
file.
```

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

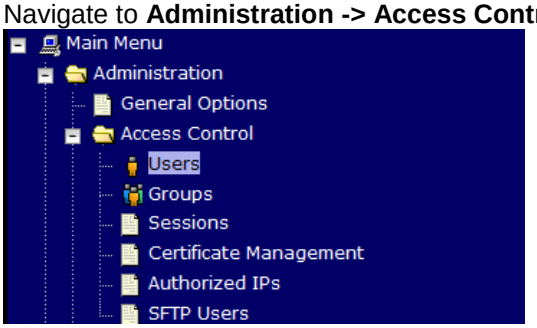
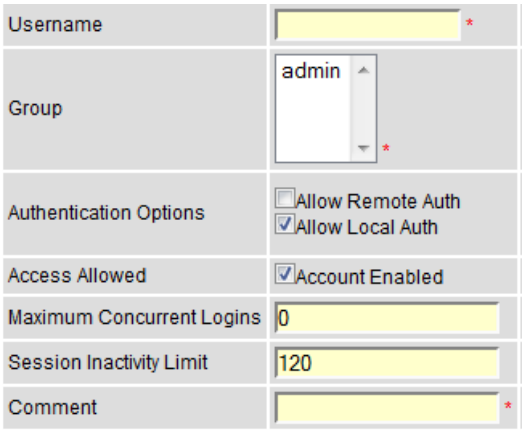
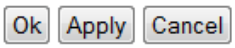
Procedure 8: Restoring an Archive that does not Contain a Current User

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 H. My Oracle Support (MOS), and ask for assistance.	
1 ☐	**Before Restoration:** Notify Affected Users Before Restoration	Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.
2 ☐	**Before Restoration:** 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: 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
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 8: Restoring an Archive that does not Contain a Current User

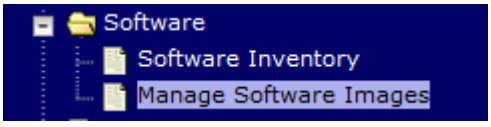
5 ☐	**After Restoration:** Recreate affected user	Navigate to **Administration -> Access Control -> Users**  Click **Insert**  Recreate the user using the data collected in **Step 3.**  Click **Ok** 
6 ☐	**After Restoration:** Repeat for Additional Users	Repeat **Step 5** to recreate additional users.
7 ☐	**After Restoration:** Reset the Passwords	See **Procedure 6** for resetting passwords for a user.

7.0 IDIH Disaster Recovery

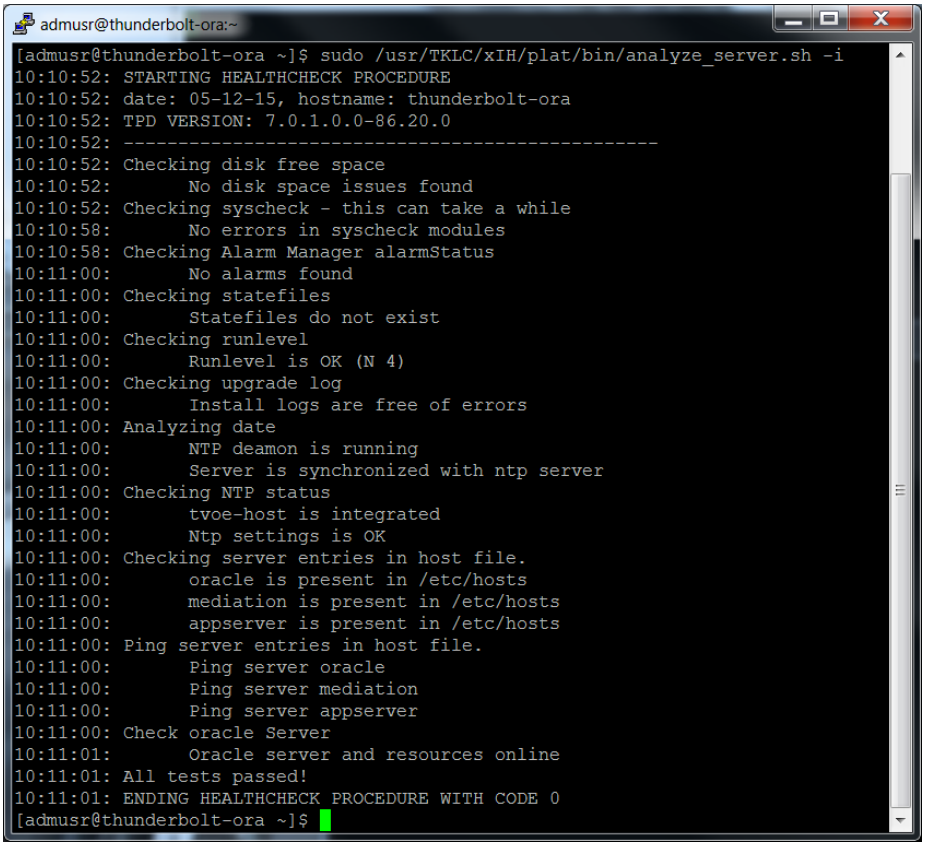
The fdconfig xml file you use for disaster recovery is different from the one used for fresh installation. The one for disaster recovery has hostname-**upgrade**_xx-xx-xx.xml file format. It took out the oracle server installation part since for disaster recovery it is not needed.

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

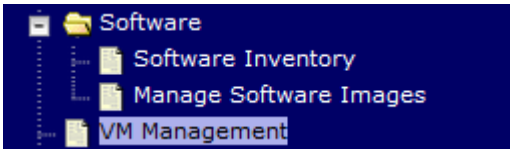
Procedure 9: IDIH Disaster Recovery Preparation

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 H. 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: 
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. **Note:** If the necessary software images are not available please follow the instructions from the applicable IDIH release installation and configuration guides – Referenced in **Table 7**: IDIH Installation Reference Table

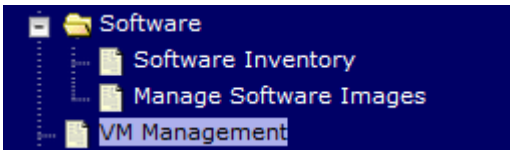
Procedure 9: IDIH Disaster Recovery Preparation

3 ☐	**Oracle Guest:** Login	Establish an SSH session to the Oracle guest, login as ***admusr***.
4 ☐	**Oracle Guest:** Perform Database Health check	Execute the following command to perform a database health check: `$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i` Output: 

Procedure 10: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

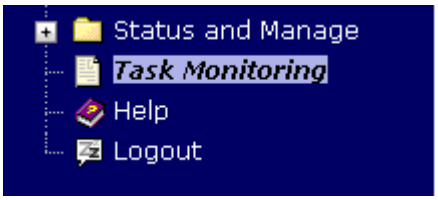
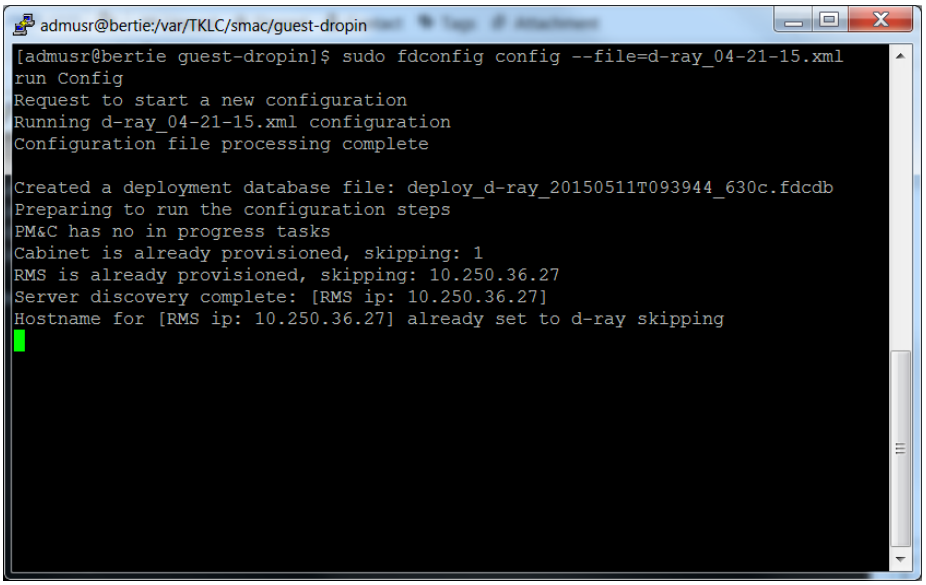
S T E P #	This procedure performs disaster recovery for the IDIH by re-installing the mediation and application servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix H. My Oracle Support (MOS),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

Procedure 10: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

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***.

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.

Procedure 10: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

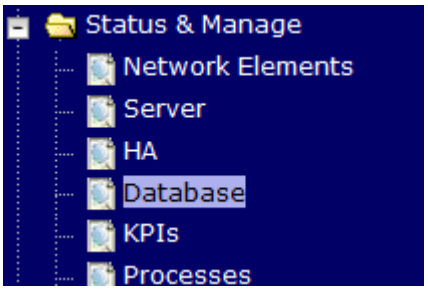
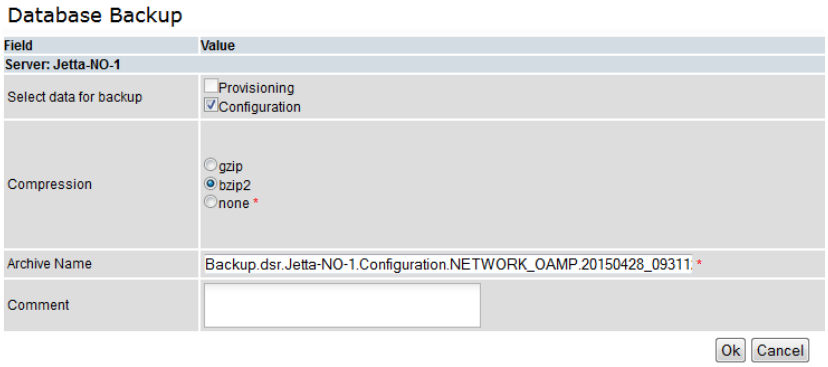
6 ☐	**PMAC GUI:** Monitor the Configuration	If not already done so, establish a GUI session on the PMAC server. Navigate to **Main Menu -> Task Monitoring**  Monitor the IDIH configuration to completion. Alternatively, you can monitor the fdconfig status through the command line after executing the fdconfig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

Appendix A. DSR Database Backup

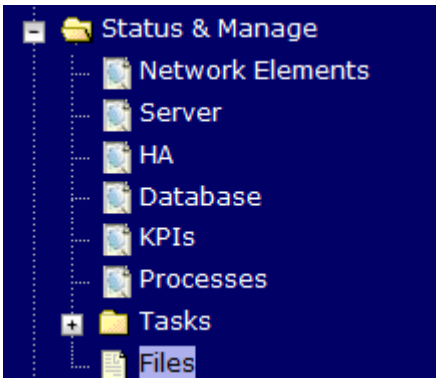
Procedure 11: Restoring an Archive that does not Contain a Current User

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 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 H. 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: 

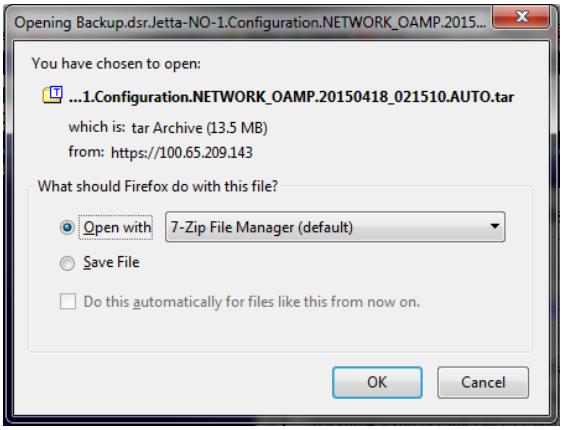
Procedure 11: Restoring an Archive that does not Contain a Current User

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 11: Restoring an Archive that does not Contain a Current User

3 ☐	**NOAM/SOAM VIP:** Verify the backup file existence.	Navigate to **Main Menu -> Status & Manage -> Files**  **Main Menu: Status & Manage -> Files** Filter Tasks Jetta-NO-1 | Jetta-NO-2 | Jetta-SO-1 | Jetta-SO-2 | Jetta-DAMP-1 | Jetta-DAMP-2 **File Name** Backup.DSR.Jetta-NO-1.FullDBParts.NETWORK_OAMP.20150421_143846.UPG.tar.bz2 Backup.DSR.Jetta-NO-1.FullRunEnv.NETWORK_OAMP.20150421_143846.UPG.tar.bz2 backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150414_021511.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150415_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150416_021511.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150417_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150418_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150419_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150420_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150421_021511.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150422_021511.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150423_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150424_021511.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150425_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150426_021510.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150427_021511.AUTO.tar backup/Backup.dsr.Jetta-NO-1.Configuration.NETWORK_OAMP.20150428_021511.AUTO.tar Select the Active NOAM or SOAM tab. The files on this server will be displayed. Verify the existence of the backup file.

Procedure 11: Restoring an Archive that does not Contain a Current User

4 ☐	**NOAM/SOAM VIP:** Download the file to a local machine.	From the previous step, choose the backup file. Select the **Download** button  1.1 GB used (5.93%) of 18.4 GB available | System utilization: 1.1 GB (5.99%) of 18.4 GB available. Select **OK** to confirm the download. 
5 ☐	**Upload the Image to Secure Location**	Transfer the backed up image saved in the previous step to a secure location where the Server Backup files are fetched in case of system disaster recovery.
6 ☐	**Backup Active SOAM**	Repeat **Steps 2 through 5** to back up the Active SOAM

Appendix B. Recovering/Replacing Failed Cisco 4948 Aggregation Switches

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

Procedure 12: Recovering a Failed Aggregation Switch (Cisco 4948E/4948E-F)

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 H. My Oracle Support (MOS), and ask for assistance.	
1 ☐	**Recover failed Aggregation Switches:** Cisco 4948E/4948E-F	Login to the PMAC via SSH as ***root(5.0)*** or ***admusr(6.0+)*** 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>` Refer to procedure *"Replace a failed 4948/4948E/4948E-F switch (c-Class system) (netConfig)"* to replace a failed Aggregation switch. - Refer to [13] for the applicable platform configuration reference. **Note:** You will need a copy of the HP Misc Firmware DVD or ISO *(or firmware file obtained from the appropriate hardware vendor),* the original networking xml files custom for this installation, and the switch backup files. These will either be stored on the PMAC in a designation location, or can be obtained from the NAPD.

Appendix C. Switching DR NOAM Site to Primary

Upon the loss of a Primary DSR NOAM Site, the DR NOAM Site should become primary. The following steps are used to enable such switchover.

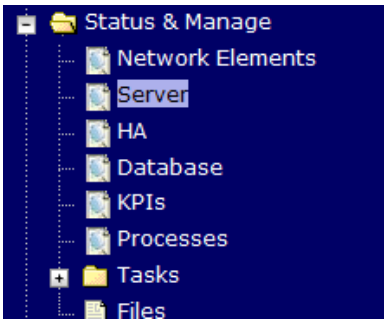
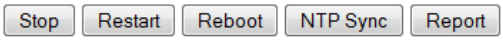
Preconditions:

- User cannot access the primary DSR
- User still can access the DR DSR
- Provisioning has stopped

Procedure 13: Switching a DR NOAM Site to Primary

S T E P #		
	The intent of this procedure is to switch a DR site to Primary. 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 H. My Oracle Support (MOS), and ask for assistance.	
1 ☐	**DR-NOAM VIP:** Login	Establish a GUI session on the DR-NOAM server by using the VIP IP address of the DR-NOAM. Open the web browser and enter a URL of: `http://<Primary_DR_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

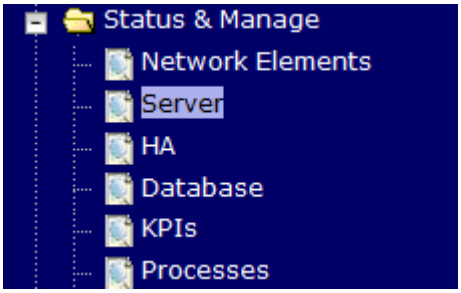
Procedure 13: Switching a DR NOAM Site to Primary

2 ☐	**DR-NOAM VIP:** Disable DSR Application on DR-NOAM Servers	Navigate to **Main Menu -> Status & Manage -> Server**  Select the row that has the Active DR-NOAM server. Select the **Stop** button.  **Note:** At this time, HA switch over causes an automatic logout.
3 ☐	**DR-NOAM VIP:** Login	Establish a GUI session on the DR-NOAM server by using the VIP IP address of the DR-NOAM. Open the web browser and enter a URL of: `http://<Primary_DR_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

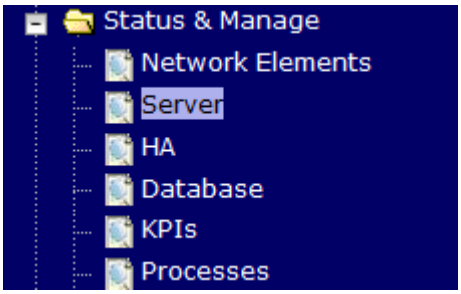
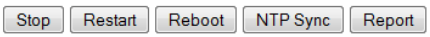
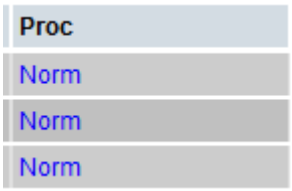
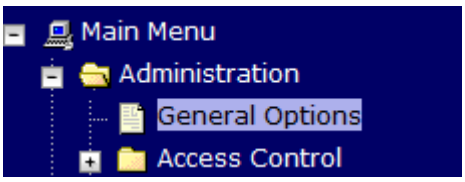
Procedure 13: Switching a DR NOAM Site to Primary

4 ☐	**DR-NOAM VIP:** Repeat	Repeat **step 2** to disable the DSR application on the now active DR NOAM. Note: The DSR application should now be stopped on all DR-NOAMs.
5 ☐	**DR-NOAM VIP:** Verify DSR application is stopped.	Verify that **"PROC"** column on both DR DSR servers show **"Man"** indicating that application is manually stopped
6 ☐	**Primary DR-NOAM:** Establish an SSH session	Login via SSH to the physical IP of the chosen primary DR-NOAM server as ***root(5.0)*** or ***admusr(6.0+)*** user.

7 ☐	**Primary DR-NOAM:** Change Role to Primary	Execute the command
		
		`$ sudo top.setPrimary`
		
		Note: This step makes the DR DSR take over as the Primary.
		
		Execute the following command to verify the role was changed to primary:
		
		`$ sudo top.myrole`
		
		System generates several replication and collection alarms as replication/collection links to/from former Primary NOAM servers becomes inactive.

8 ☐	**Primary DR-NOAM:** Verify Replication	Navigate to **Main Menu -> Status & Manage -> Server**  It may take several minutes for replication; afterward the **"DB"** and **"Reporting Status"** columns should show **"Normal"**. DB / Reporting Status Norm / Norm Norm / Norm Norm / Norm

Procedure 13: Switching a DR NOAM Site to Primary

9 ☐	**New Primary NOAM:** Re-enable the application.	Navigate to **Main Menu -> Status & Manage -> Server**  Select the row that has the active New-Primary NOAM server. Click the **Restart** button and then click the OK button.  Verify that **"PROC"** column now shows "Norm".  General operations can now resume to the VIP of the new-Primary DSR.
10 ☐	**New Primary NOAM:** Decrease the Durability Admin status	Lower the durability admin status to (NOAM pair) to exclude former-Primary NOAM servers from the provisioning database durability. A value greater than 2 must be adjusted downward. Navigate to **Main Menu -> Administration -> General Options**  Set "cm.idb.durableAdminState" to 2 (NOAM pair)  Click the **OK** button

Procedure 13: Switching a DR NOAM Site to Primary

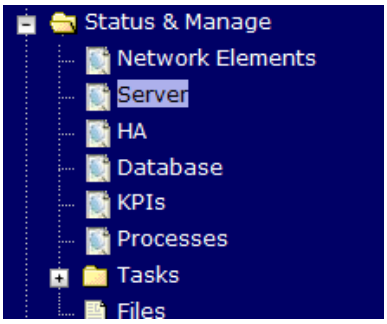
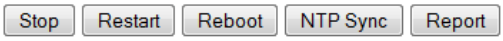
11 ☐	**New Primary NOAM:** Repeat for standby of new-primary NOAM Server	Repeat **steps 8-10** for standby of the new-Primary NOAM server.

Appendix D. Returning a Recovered Site to Primary

Procedure 14: Returning a Recovered Site to Primary

S T E P #		
	The intent of this procedure is to return a recovered site to primary. 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 H. My Oracle Support (MOS), and ask for assistance.	
1 ☐	**Primary NOAM VIP:** Login	Establish a GUI session on the primary NOAM server by using the VIP IP address of the primary NOAM. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

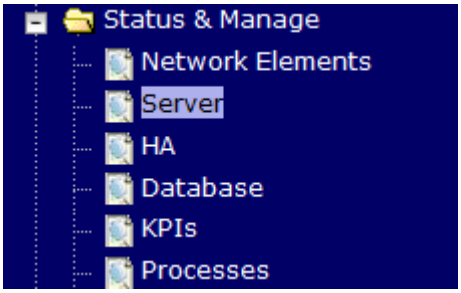
Procedure 14: Returning a Recovered Site to Primary

2 ☐	**Primary NOAM VIP:** Disable DSR Application on DR-NOAM Servers	Navigate to **Main Menu -> Status & Manage -> Server**  Select the row that has the Active DR-NOAM server. Select the **Stop** button.  **Note:** At this time, HA switch over causes an automatic logout.
3 ☐	**Primary NOAM VIP:** Login	Establish a GUI session on the primary NOAM server by using the VIP IP address of the NOAM. Open the web browser and enter a URL of: `http://<Primary_NOAM_VIP_IP_Address>` Login as the ***guiadmin*** user: 

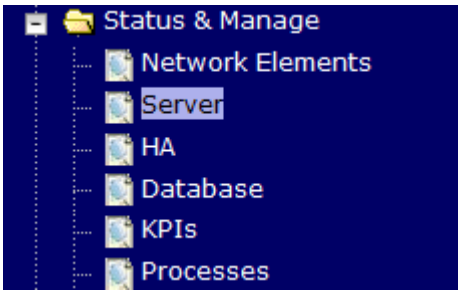
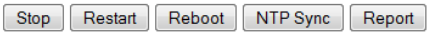
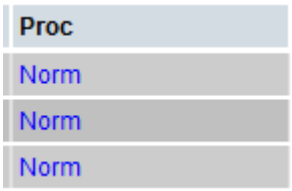
Procedure 14: Returning a Recovered Site to Primary

4 ☐	**Primary NOAM VIP:** Repeat	Repeat **step 2** to disable the DSR application on the now active DR NOAM. Note: The DSR application should now be stopped on all DR-NOAMs.
5 ☐	**Primary NOAM VIP:** Verify DSR application is stopped.	Verify that **"PROC"** column on both DR DSR servers show **"Man"** indicating that application is manually stopped
6 ☐	**Primary NOAM:** Establish an SSH session	Login via SSH to the physical IP of the chosen primary DR-NOAM server as ***root(5.0)*** or ***admusr(6.0+)*** user.

7 ☐	**Primary NOAM:** Change Role to Secondary	Execute the command
		
		`$ sudo top.setSecondary`
		
		Note: This step makes the primary NOAM to revert to DR-NOAM
		
		Execute the following command to verify the role was changed to secondary:
		
		`$ sudo top.myrole`

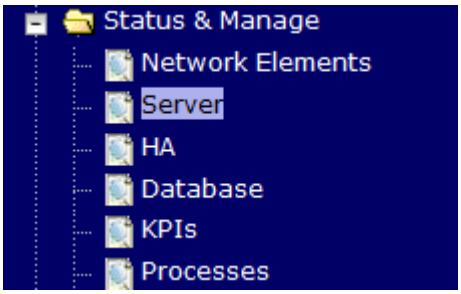
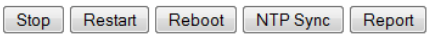
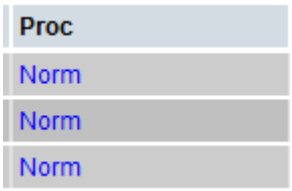
8 ☐	**New DR-NOAM VIP:** Verify Replication	Navigate to **Main Menu -> Status & Manage -> Server**  It may take several minutes for replication; afterward the **"DB"** and **"Reporting Status"** columns should show **"Norm"**. DB / Reporting Status Norm / Norm Norm / Norm Norm / Norm

Procedure 14: Returning a Recovered Site to Primary

9 ☐	**New DR-NOAM VIP:** Re-enable the application.	Navigate to **Main Menu -> Status & Manage -> Server**  Select the row that has the formerly Primary NOAM server. Click the **Restart** button and then click the OK button.  Verify that **"PROC"** column now shows "Norm". 
10 ☐	**To-Be-Primary NOAM:** Establish an SSH session	Login via SSH to the physical IP of the chosen primary DR-NOAM server as ***root(5.0)*** or ***admusr(6.0+)*** user.

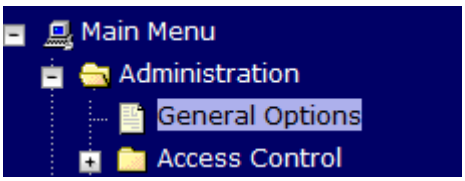
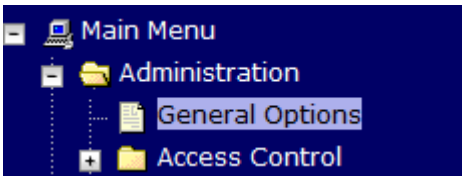
11 ☐	**To-Be-Primary DSR NOAM**: Set To-be-Primary DSR NOAM to Primary	Execute the following command:
		`$ sudo top.setPrimary`
		Note: This step makes the DSR take over as the Primary.
		Execute the command to verify the server role was changed to Primary:
		`$ sudo top.myrole`
		System generates several replication and collection alarms as replication/collection links to/from former Primary NOAM servers becomes inactive.

Procedure 14: Returning a Recovered Site to Primary

12 ☐	**New Primary NOAM:** Re-enable the application.	Navigate to **Main Menu -> Status & Manage -> Server**  Select the row that has the active New-Primary NOAM server. Click the **Restart** button and then click the OK button.  Verify that **"PROC"** column now shows "Norm".  Provisioning can now resume to the VIP of the new-Primary DSR.

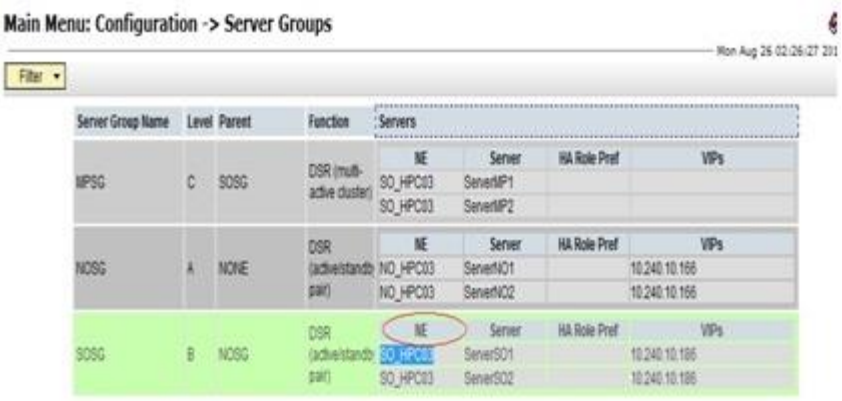
13 ☐	**New Primary DSR NOAM:** Verify Replication	Monitor **Main Menu -> Status & Manage -> Server** screen at new-Primary DSR.
		It may take several minutes for replication; afterward the "DB" and "Reporting Status" columns should show "Normal"
		Note: the inetmerge process might have to be restarted if replication is taking excessive time. To restart it, ssh to the active site NOAM and run the following command to restart the replication process:
		For DSR 5.0:
		`$ pm.kill inetmerge`
		For DSR 6.0+:
		`$ sudo pm.kill inetmerge`

Procedure 14: Returning a Recovered Site to Primary

14 ☐	**New Primary NOAM:** Decrease the Durability Admin status	Lower the durability admin status to (NOAM pair) to exclude former-Primary NOAM servers from the provisioning database durability. A value greater than 2 must be adjusted downward. Navigate to **Main Menu -> Administration -> General Options**  Set “cm.idb.durableAdminState” to 2 (NOAM pair)  Click the **OK** button
15 ☐	**New Primary NOAM:** Set Durability admin status to include DR-NOAM (Optional)	If you reduced the durability status in **Procedure 13**, raise durability admin status to its former value (NOAM + DRNOAM) Navigate to **Main Menu -> Administration -> General Options**  Set “durableAdminState” to 3(NO DRNOAM)  Click the **OK** button Now new DRNOAM DSR servers are part of provisioning database durability.

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

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

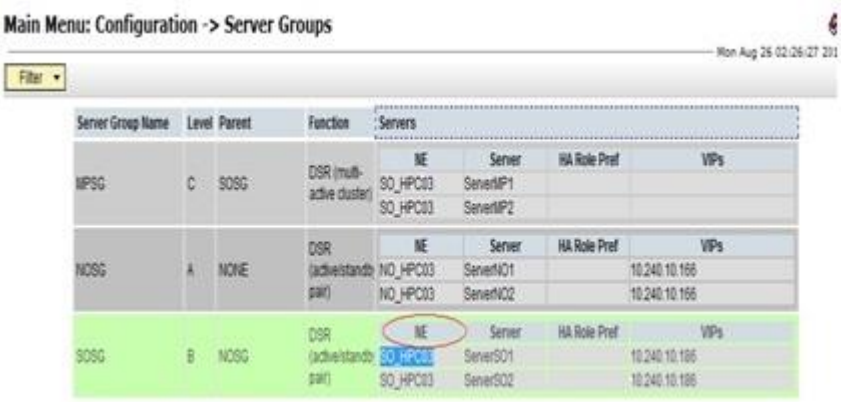
S T E P #		
	The intent of this procedure is to inhibit A and B level replication on all C Level servers of this site Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix H. My Oracle Support (MOS), and ask for assistance.	
1 ☐	**Active NOAM:** Login	Login to the Active NOAM server via SSH as ***root(5.0) or admusr(6.0+)*** user.
2 ☐	**Active NOAM:** Inhibit replication on all C level Servers	Execute the following command: `$ for i in $(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<NE name of the site>'"); do iset -finhibitRepPlans='A B' NodeInfo where "nodeName='$i'"; done` **Note:** NE name of the site can be found out by logging into the Active NOAM GUI and going to **Configuration->Server Groups** screen. Please see the snapshot below for more details. E.g. if ServerSO1 belong 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 is disabled. Verification of replication inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site 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 A B SO_HPC03 C2254.233 MP1 MP1 Active A B SO_HPC03

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

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 H. My Oracle Support (MOS), and ask for assistance.	
1 ☐	**Active NOAM:** Login	Login to the Active NOAM server via SSH as ***root(5.0) or admusr(6.0+)*** user.
2 ☐	**Active NOAM:** Un-Inhibit replication on all C level Servers	Execute the following command: `$ for i in $(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<NE name of the site>'"); do iset -finhibitRepPlans='' NodeInfo where "nodeName='$i'"; done` **Note:** NE name of the site can be found out by logging into the Active NOAM GUI and going to **Configuration->Server Groups** screen. Please see the snapshot below for more details. E.g. if ServerSO1 belong 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 Inhibited.	After executing above steps to un-inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled. Verification of replication un-inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP 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 G. Workarounds for Issues not fixed in this Release

<table>
<tr><th>Issue</th><th>Associated PR</th><th>Workaround</th></tr>
<tr><td>Inetmerge alarm after force restore</td><td rowspan="2">222826</td><td rowspan="2">Get the clusterID of the NO using the following command:

$ top.myrole
myNodeId=A3603.215
myMasterCapable=true

Then update the clusterId field in RecognizedAuthority table to have the same clusterid:

$ ivi RecognizedAuthority
e.g.
iload -ha -xU -frecNum -fclusterId -ftimestamp RecognizedAuthority \
<<'!!!!'
0|A1878|1436913769646
!!!!</td></tr>
<tr><td>Incorrect NodeID</td></tr>
<tr><td>Inetsync alarms after performing disaster recovery</td><td>222828</td><td>Restart the Inetsync service on all affected servers using the following commands:

$ pm.set off inetsync
$ pm.set on inetsync</td></tr>
<tr><td>Active NO /etc/hosts file does not contain server aliases after force restore done.
Note: This is no longer needed in DSR 7.1</td><td rowspan="2">222829,234357</td><td rowspan="2">Release 5.0:

From the recovered NOAM server command line, execute:

$ AppWorks AppWorks_AppWorks updateServerAliases <NO Host Name></td></tr>
<tr><td>Active NO cannot communicate with other Servers</td></tr>
</table>

SOAM VIP reports no servers at the Status & Manage Server screen.	Bug 20045979	Perform the following command to see the 'db' directory permission: **$ ls –ltr** drwx---523 root root 20480 Nov 11 22:44 db **<-- Not Correct** Perform the following command to change the directory permissions: **$ sudo chmod 777 db** Verify the directory permissions are correct: **$ ls –ltr** drwxrwxrwx **523 root root 20480 Nov 11 22:44 db** **<-- Correct**

Appendix H. 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.