Oracle® Communications
Diameter Signaling Router
Rack Mount Server Disaster Recovery Guide
Release 8.0/8.1
E76187-03

July 2017
# Table of Contents

Table of Contents........................................................................................................3
List of Procedures ...........................................................................................................5
List of Tables ..................................................................................................................5
List of Figures ..................................................................................................................5

1.0 Introduction................................................................................................................6
  1.1 Purpose and Scope ......................................................................................................6
  1.2 References ................................................................................................................6
  1.3 Acronyms ...................................................................................................................7
  1.4 Terminology ..............................................................................................................8
  1.5 Optional Features .....................................................................................................9
  1.6 Revision History ......................................................................................................9

2.0 General Description .................................................................................................10
  2.1 Complete Server Outage (All Servers) ..................................................................11
  2.2 Partial server outage with one NOAM server intact and all SOAMs failed ..........11
  2.3 Partial server outage with both NOAM servers failed and one SOAM server intact ..........................................................................................................................11
  2.4 Partial server outage with NOAM and one SOAM server intact ..........................11
  2.5 Partial server outage with Both NOAMs failed and DR-NOAM available ..........11
  2.6 Partial Service outage with corrupt database .........................................................11

3.0 Procedure Overview ...............................................................................................12
  3.1 Required Materials .................................................................................................12
  3.2 Disaster Recovery Strategy ......................................................................................13

4.0 Procedure Preparation ............................................................................................15

5.0 Disaster Recovery Procedure ..................................................................................16
  5.1 Recovering and Restoring System Configuration ................................................17
    5.1.1 Recovery Scenario 1 (Complete Server Outage) ..............................................17
    5.1.2 Recovery Scenario 2 (Partial Server Outage with at least one NOAM server intact and all SOAMs failed) ..........................................................62
    5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact) ..........................................................96
    5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact) ...............................................................138
    5.1.5 Recovery Scenario 5 (Both NOAM servers failed with DR-NOAM available) ..............................................................................................................164
    5.1.6 Recovery Scenario 6 (Database Recovery) .......................................................170

6.0 Resolving User Credential Issues after Database Restore .......................................185
  6.1 Restoring a Deleted User .......................................................................................185
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2 Keeping a Restored user</td>
<td>186</td>
</tr>
<tr>
<td>6.3 Removing a Restored User</td>
<td>188</td>
</tr>
<tr>
<td>6.4 Restoring a Modified User</td>
<td>190</td>
</tr>
<tr>
<td>6.5 Restoring an Archive that does not contain a Current User</td>
<td>191</td>
</tr>
<tr>
<td>7.0 IDIH Disaster Recovery</td>
<td>197</td>
</tr>
<tr>
<td>Appendix A. Database Backup</td>
<td>205</td>
</tr>
<tr>
<td>Appendix B. Recovering/Replacing Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 8 Only)</td>
<td>209</td>
</tr>
<tr>
<td>Appendix C. Inhibit A and B Level Replication on C-Level Servers</td>
<td>214</td>
</tr>
<tr>
<td>Appendix D. Un-Inhibit A and B Level Replication on C-Level Servers</td>
<td>216</td>
</tr>
<tr>
<td>Appendix E. Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)</td>
<td>217</td>
</tr>
<tr>
<td>Appendix F. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)</td>
<td>219</td>
</tr>
<tr>
<td>Appendix G. Restore TVOE Configuration from Backup Media</td>
<td>222</td>
</tr>
<tr>
<td>Appendix H. Restore PMAC from Backup</td>
<td>232</td>
</tr>
<tr>
<td>Appendix I. Workarounds for Issues not fixed in this Release</td>
<td>242</td>
</tr>
<tr>
<td>Appendix J. SNMP Configuration</td>
<td>242</td>
</tr>
<tr>
<td>Appendix K. Restore Provisioning Database</td>
<td>245</td>
</tr>
<tr>
<td>Appendix L. Recover PDB Relay</td>
<td>249</td>
</tr>
<tr>
<td>Appendix M. My Oracle Support (MOS)</td>
<td>250</td>
</tr>
</tbody>
</table>
List of Procedures

Procedure 1: Recovery Scenario 1 ................................................................. 18
Procedure 3: Recovery Scenario 3 ................................................................. 97
Procedure 4: Recovery Scenario 4 ............................................................... 139
Procedure 5: Recovery Scenario 5 ............................................................... 165
Procedure 6: Recovery Scenario 6 (Case 1) ................................................ 170
Procedure 7: Recovery Scenario 6 (Case 2) ................................................ 178
Procedure 8: Keep Restored User ............................................................... 186
Procedure 9: Remove the Restored User ..................................................... 188
Procedure 10: Restoring an Archive that does not Contain a Current User ....... 191
Procedure 11: IDIH Disaster Recovery Preparation ...................................... 198
Procedure 12: IDIH Disaster Recovery (Re-Install Mediation and Application Servers) .......................................................... 201
Procedure 13: Database Backup ................................................................. 205
Procedure 14: Recovering a Failed Aggregation Switch (Cisco 4948E/4948E-F) HP DL380 Only .......................................................... 209
Procedure 15: Inhibit A and B Level Replication on C-Level Servers .............. 214
Procedure 16: Un-Inhibit A and B Level Replication on C-Level Servers .......... 216
Procedure 15: Inhibit A and B Level Replication on C-Level Servers .............. 217
Procedure 16: Un-Inhibit A and B Level Replication on C-Level Servers .......... 219
Procedure 17: Restore TVOE Configuration from Backup Media .................. 222
Procedure 18: Restore PMAC from Backup Media ...................................... 232
Procedure 19: Restore PMAC from Backup Server ...................................... 236
Procedure 20: SNMP Configuration ......................................................... 242

List of Tables

Table 1 Acronyms ......................................................................................... 7
Table 2 Terminology .................................................................................... 8
Table 3 Optional Features .......................................................................... 9
Table 4. Recovery Scenarios ....................................................................... 15

List of Figures

Figure 1. Determining Recovery Scenario ................................................ 14
1.0 Introduction

1.1 Purpose and Scope

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

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

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

1.2 References

[1] TPD Initial Product Manufacture
[2] Platform 7.2 Configuration Procedure Reference
[9] DSR Hardware and Software Installation Procedure 1/2
[12] DSR DTLS Feature Activation Procedure
### 1.3 Acronyms

#### Table 1 Acronyms

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

#### Table 2 Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base hardware</td>
<td>Base hardware includes all hardware components (bare metal) and electrical wiring to allow a server to power on.</td>
</tr>
<tr>
<td>Base software</td>
<td>Base software includes installing the server’s operating system: Oracle Platform Distribution (TPD).</td>
</tr>
<tr>
<td>Failed server</td>
<td>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.</td>
</tr>
<tr>
<td>Software Centric</td>
<td>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.</td>
</tr>
<tr>
<td>Enablement</td>
<td>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.</td>
</tr>
</tbody>
</table>
1.5 Optional Features

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

Table 3 Optional Features

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

1.6 Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2016</td>
<td>Initial Release</td>
</tr>
</tbody>
</table>
2.0 General Description

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Conditions</th>
</tr>
</thead>
</table>
| Recovery of the entire network from a total outage | - All NOAM servers failed  
- All SOAM servers failed |
| Recovery of one or more servers with at least one NOAM server intact | - 1 or more NOAM servers intact  
- 1 or more SOAM or MP servers failed |
| Recovery of the NOAM pair with one or more SOAM servers intact | - All NOAM servers failed  
- 1 or more SOAM servers intact |
| Recovery of one or more server with at least one NOAM and one SOAM server intact | - 1 or more NOAM servers intact  
- 1 or more SOAM servers intact  
- 1 SOAM or 1 or more MP servers failed |

Recovery of one or more server with corrupt databases that cannot be restored via replication from the active parent node.

Note: For Failed Aggregation switches (HP DL380 Gen 8 Only) refer to Appendix B. Recovering/Replacing Failed Cisco 4948 Aggregation Switches.
2.1 Complete Server Outage (All Servers)

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

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

2.2 Partial server outage with one NOAM server intact and all SOAMs failed

This case assumes that at least one NOAM servers intact. All SOAM servers have failed (including SOAM spares-If equipped) and are recovered using base recovery of hardware and software. Database is restored on the SOAM server and replication will recover the database of the remaining servers.

2.3 Partial server outage with both NOAM servers failed and one SOAM server intact

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

2.4 Partial server outage with NOAM and one SOAM server intact

The simplest case of disaster recovery is with at least one NOAM and at least one SOAM servers intact. All servers are recovered using base recovery of hardware and software. Database replication from the active NOAM and SOAM servers will recover the database to all servers. (Note: this includes failures of any disaster recovery NOAM servers)

2.5 Partial server outage with Both NOAMs failed and DR-NOAM available

For a partial outage with both NOAM servers failed but a DR NOAM available, the DR NOAM is switched from secondary to primary then recovers the failed NOAM servers.

2.6 Partial Service outage with corrupt database

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

Case 2: Database is corrupted but replication channel is active
3.0 Procedure Overview

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

3.1 Required Materials

The following items are needed for disaster recovery:

1. A hardcopy of this document (E76187) and hardcopies of all documents in the reference list
2. Hardcopy of all NAPD performed at the initial installation and network configuration of this customer's site. If the NAPD cannot be found, escalate this issue within My Oracle Support (MOS) until the NAPD documents can be located.
3. DSR recent backup files: Electronic backup file (preferred) or hardcopy of all DSR configuration and provisioning data.
5. The xml configuration files used to configure the Cisco 4948 aggregation switches, available on the PMAC Server (or PMAC backup)
6. The switch backup files taken after the switch is configured, available on the PMAC Server (or PMAC backup)
7. The network element XML file used for the initial configuration.
8. Firmware files as provide by hardware vendor
9. NetBackup Files if they exist. This may require the assistance of the customer’s NetBackup administrator.
10. PMAC and TVOE backups (If available)
11. One (1) target release DSR Media, or a target-release ISO
12. One (1) target release SDS Media, or a target-release ISO (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen9 Only)
13. Three (3) target release iDIH Media, or target-release ISOs
14. Site specific VM Placement and Socket Pinning workbook used during deployment(Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen9 Only)
15. Latest RADIUS shared secret encryption key file backup (DpiKf.bin.enchr)
16. List of activated and enabled features

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

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

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

1. Identify all failed servers
2. Is database Corrupted?
   - Yes
   - No
3. Are both NOAM Servers Failed?
   - Yes
   - No
4. DR NOAM Installed?
   - Yes
   - No
5. Are all SOAM Servers failed?
   - Yes
   - No
6. Is the recent database backup available that can be restored?
   - Yes
   - No
7. Follow Recovery Scenario 6 (Case 2)
8. Follow Recovery Scenario 6 (Case 1)
9. Contact MOS
10. Follow Recovery Scenario 5
11. Follow Recovery Scenario 2
12. Follow Recovery Scenario 3
13. Follow Recovery Scenario 1
# 4.0 Procedure Preparation

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

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

## Table 4. Recovery Scenarios

<table>
<thead>
<tr>
<th>Recovery Scenario</th>
<th>Failure Condition</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>• All NOAM servers failed.</td>
<td>Section 5.1.1 Recovery Scenario 1 (Complete Server Outage)</td>
</tr>
<tr>
<td></td>
<td>• All SOAM servers failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MP servers may or may not be failed.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>• At least 1 NOAM server is intact and available.</td>
<td>Section 5.1.2 Recovery Scenario 2 (Partial Server Outage with at least one NOAM server intact and all SOAMs failed)</td>
</tr>
<tr>
<td></td>
<td>• All SOAM servers failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MP servers may or may not be failed.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>• All NOAM servers failed.</td>
<td>Section 5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact)</td>
</tr>
<tr>
<td></td>
<td>• At least 1 SOAM server out of Active, StandBy, Spare is intact and available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MP servers may or may not be failed.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>• At least 1 NOAM server is intact and available.</td>
<td>Section 5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)</td>
</tr>
<tr>
<td></td>
<td>• At least 1 SOAM server out of Active, StandBy, Spare is intact and available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 or more MP servers have failed.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>• Both NOAM servers failed.</td>
<td>Section 5.1.5 Recovery Scenario 5 (Both NOAM servers Available)</td>
</tr>
<tr>
<td></td>
<td>• DR NOAM is Available</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SOAM servers may or may not be failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MP servers may or may not be failed.</td>
<td></td>
</tr>
</tbody>
</table>
6: Case 1
- Server is intact
- Database gets corrupted on the server
- Replication channel from parent is inhibited because of upgrade activity

6: Case 2
- Server is intact
- Database gets corrupted on the server
- Latest Database backup of the corrupt server is NOT present
- Server having a corrupted database
- Replication channel is not inhibited
- Server has the same release as that of its Active parent

5.0 Disaster Recovery Procedure

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

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

**** WARNING *****

**** WARNING *****

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

Recovering Base Hardware:
1. Hardware Recovery will be executed by the appropriate HW vendor.
2. Base Hardware Replacement must be controlled by engineer familiar with DSR Application
5.1 Recovering and Restoring System Configuration

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

5.1.1 Recovery Scenario 1 (Complete Server Outage)

For a complete server outage, TVOE is recovered on all RMS Servers. The VMs are re-created and configured. The database restored on one of the NOAM and SOAM servers. Database replication from the active NOAM server will recover the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures’ detailed steps are in Procedure 1. The major activities are summarized as follows:

Recover Base Hardware and Software for all RMSs:

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

Recover PMAC

Recover Active NOAM Guest.

- Recover the NOAM database.
- Reconfigure the application

Recover Standby NOAM Guest.

- Reconfigure the Application

Recover Query Server (SDS Only) Guest

- Reconfigure the Application

Recover all SOAM and MP/DP Guest.

- Recover the SOAM database.
- Reconfigure the Application

Recover IDIH if necessary

Restart processes and re-enable provisioning and replication.
Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Workarounds</td>
<td>Refer to Appendix I. Workarounds for issues not fixed in this release to understand any workarounds required during this procedure.</td>
</tr>
<tr>
<td>2.</td>
<td>Gather Required Materials</td>
<td>Gather the documents and required materials listed in Section 3.1 Required Materials</td>
</tr>
<tr>
<td>3.</td>
<td>Replace Failed Equipment</td>
<td>HW vendor to replace the failed equipment</td>
</tr>
</tbody>
</table>
| 4.     | Recover PMAC TVOE Host (If Required): Configure BIOS Settings and Update Firmware | 1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:
   - **HP DL380 Gen8:** “Configure HP Gen 8 Server BIOS Settings”
   - **Oracle X5-2/Netra X5-2/X6-2:** “Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings”
   - **HP DL380 Gen9:** “Configure HP Gen9 Server BIOS Settings”
   2. Verify and/or upgrade server firmware by executing procedure “Upgrade Rack Mount Server Firmware” from reference [8] Note: To determine the VM placement, refer 12 for workbook reference. Also refer Appendix S: VM placement in HP DL380 Gen8/Gen9 (Onboard 1Gbps NICs) and CPU Pinning in HP DL380 Gen9 (Onboard 1Gbps NICs) from [8] for pinning information on HP DL380 Gen 9. |
| 5.     | Recover PMAC and PMAC TVOE Host: Backup Available | This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step.  
   1. Restore the TVOE backup by executing Appendix G. Restore TVOE Configuration from Backup Media on ALL failed rack mount servers
   2. Restore the PMAC backup by executing Appendix H. Restore PMAC from Backup
   Proceed to Step 7 |
| 6.     | Recover PMAC and PMAC TVOE Host: Backup Not Available | This step assumes that TVOE and PMAC backups are NOT available, if the TVOE and PMAC have already been restored, skip this step  
   1. Execute procedure “Install and Configure TVOE on First RMS (PMAC Host)” from reference [8]  
   2. Execute section “Install PMAC” from reference [8] |
## Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Execute section “Initialize the PMAC Application” from reference [8] &lt;br&gt;Proceed to Next Step</td>
</tr>
<tr>
<td>7.</td>
<td><strong>Recovery Failed Cisco 4948 Aggregation Switches</strong> (HP DL380 Only) &lt;br&gt;Oracle X5-2/Netra X5-2/X6-2/HP DL380 GEN 9 SKIP THIS STEP &lt;br&gt;Recover failed Cisco 4948 aggregation switches, if needed: &lt;br&gt;Backup configuration files available: Refer to Appendix B. &lt;br&gt;Recovering/Replacing Failed Cisco 4948 Aggregation Switches to recover failed Cisco 4948 aggregation switches &lt;br&gt;Backup configuration files NOT available: Execute section “Configure Cisco 4948E-F Aggregation Switches (HP DL 380 Gen 8 Only)” from reference [8]</td>
</tr>
<tr>
<td>8.</td>
<td><strong>Configure PMAC (No Backup)</strong> &lt;br&gt;If PMAC backup was NOT restored in step 5, execute this step. Otherwise <strong>Skip this Step.</strong> &lt;br&gt;Execute sections “Configure PMAC Server (NetBackup Only)” and “Add RMS to the PMAC Inventory” from reference [8]</td>
</tr>
<tr>
<td>9.</td>
<td><strong>Install/Configure Additional Rack Mount Servers</strong> (Backups available) &lt;br&gt;This step assumes that TVOE backups are available, if backups are NOT available, skip this step. &lt;br&gt;1. Execute procedure “Install TVOE on Additional Rack Mount Servers” from reference [8] &lt;br&gt;2. Restore the TVOE backup by executing Appendix E. Restore TVOE Configuration from Backup Media on ALL failed rack mount servers</td>
</tr>
<tr>
<td>10.</td>
<td><strong>Install/Configure Additional Rack Mount Servers</strong> (Backups NOT available) &lt;br&gt;This step assumes that TVOE backups are NOT available, if backups are available, execute the previous step. &lt;br&gt;1. Execute procedure “Install TVOE on Additional Rack Mount Servers” from reference [8] &lt;br&gt;2. Execute “Configure TVOE on Additional Rack Mount Servers” from reference [8]</td>
</tr>
<tr>
<td>11.</td>
<td><strong>Configure BIOS Settings and Update Firmware on Additional Rack Mount Servers</strong> &lt;br&gt;1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]: &lt;br&gt;   - <strong>HP DL380 Gen8:</strong> “Configure HP Gen 8 Server BIOS Settings” &lt;br&gt;   - <strong>Oracle X5-2/Netra X5-2/X6-2:</strong> “Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings” &lt;br&gt;   - <strong>HP DL380 Gen9:</strong> “Configure HP Gen9 Server BIOS Settings” &lt;br&gt;2. Verify and/or upgrade server firmware by executing procedure</td>
</tr>
</tbody>
</table>
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.</td>
<td>Deploy Redundant PMAC (if required)</td>
<td>Refer to procedure “Deploy Redundant PMAC (Optional)” to re-deploy and configure any redundant PMACs previously configured.</td>
</tr>
<tr>
<td>14.</td>
<td>PMAC: Determine if a fdconfig file exists from the initial deployment.</td>
<td>Determine whether the fdconfig backup file exists: <code>[admusr@melbourne-pmac-1 ~]$ ll /usr/TKLC/smac/etc/fdc/</code> Examine the results and verify whether the rms config file <code>&lt;hostname&gt;.cfg</code> exists. Note: There may be multiple fdconfig backup files here with respect to each RMS. Select the respective one according to the RMS.</td>
</tr>
<tr>
<td>15.</td>
<td>If fdconfig backup file does NOT exist:</td>
<td>Execute this step ONLY If the fdconfig backup file does NOT exist: If the fdconfig file does NOT exist: Create the needed file(s) by executing section “Virtual Machine/Network Fast Deployment” from reference [8] <strong>WARNING:</strong> It is very important to ensure the file(s) created only affect the TVOE server(s) and its Guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service. Skip to step 24 if this step was executed</td>
</tr>
<tr>
<td>16.</td>
<td>PMAC: Load ISOs into PMAC if not done already</td>
<td>Execute this step ONLY If the fdconfig backup file exists and located at step 14: If the DSR, SDS, and TPD ISOs are NOT loaded in to the PMAC: Execute procedures 14 of section “Virtual Machine/Network Fast Deployment” from reference [8]</td>
</tr>
</tbody>
</table>
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td>PMAC [If fdc backup file exists]: Edit/Update Configuration File</td>
</tr>
</tbody>
</table>

If already loaded into PMAC, skip this step.

**Execute this step ONLY if the fdconfig backup file exists and located at step 14:**

**Edit the fdconfig file to include only the required/failed servers.**

**Note:** Comment out configuration items that are not needed.

**Note:** It is recommended that a separate configuration file be created for EACH rack mount server being deployed.

**Note:** Cabinet ID in the config file needs to match the cabinet already defined in PM&C.

The following items are mandatory:

- `siteName`
- `tpdIsso`
- `dsrIsso` (if DSR VMs are being configured)
- `sdsIsso` (if SDS VMs are being configured)
- `NETWORK_xmi` (if DSR/SDS NOAM/DRNOAMs are being configured)
- `XMIGATEWAY` (if DSR/SDS NOAM/DRNOAMs are being configured)
- `XMISUBNETMASK` (if DSR/SDS NOAM/DRNOAMs are being configured)
- `DSRNOAM1XMIIIPADDRESS` (if DSRNOAM1 is being configured)
- `DSRNOAM2XMIIIPADDRESS` (if DSRNOAM2 is being configured)
- `DSRDRNOAM1XMIIIPADDRESS` (if DSRDRNOAM1 is being configured)
- `DSRDRNOAM2XMIIIPADDRESS` (if DSRDRNOAM2 is being configured)
- `SDSNOAM1XMIIIPADDRESS` (if SDSNOAM1 is being configured)
- `SDSNOAM2XMIIIPADDRESS` (if SDSNOAM2 is being configured)
- `SDSDRNOAM1XMIIIPADDRESS` (if SDSDRNOAM1 is being configured)
- `SDSDRNOAM2XMIIIPADDRESS` (if SDSDRNOAM2 is being configured)

**Note:** Refer to Appendix R: VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8]

**Note:** Comment out SDS and DSR profile items if corresponding products are not used.

**Note:** [Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9]: Refer to Appendix Q.3: Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8]

**Note:** The VM names should not be modified in the .cfg file. The names are fixed and will be prefixed in the siteName.

**Note:** The VM locations should not be changed from their ‘RMSx’ format. Each RMS should correspond with a separate Rack Mount Server.

**WARNING:**

It is very important to ensure the file(s) created only affect the TVOE server(s) and its Guests being recovered. Failure to ensure working servers are not included in the file
### Procedure 1: Recovery Scenario 1

- **Could result in those servers/guests being taken out of service.**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.</td>
<td><strong>PMAC</strong>&lt;br&gt; [If fdconfig backup file exists]: Copy the located backed up fdconfig file to the RMS directory &lt;br&gt; <strong>Execute this step ONLY if the fdconfig backup file exists and located at step 14:</strong>&lt;br&gt; $ cp /usr/TKL/smac/etc/fdc/&lt;backup_fdc_file&gt; /usr/TKL/smac/etc/RMS/</td>
</tr>
</tbody>
</table>
| 19. | **PMAC**<br> [If fdconfig backup file exists]: Execute the config.sh script<br> **Execute this step ONLY if the fdconfig backup file exists and located at step 14:**<br> Execute config.sh against the modified back up config file defined above.<br> **Note:** If the below command is executed on multiple cfg files, it will overwrite the existing xml file. It is recommended to rename the xml file before running the below command again.<br> $ sudo ./config.sh <config file><br> Sample Output:
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 20.  | **PMAC**  
|       | *If fdc backup file exists*:  
|       | Execute Fast Deployment |

**Execute this step ONLY If the fdconfig backup file exists and located at step 14:**

With the file generated from the config.sh script, execute the following command to start fast deployment:

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

**Note:** This is a long duration command. If the screen command was run prior
Procedure 1: Recovery Scenario 1

21. PMAC GUI
   [If fdc backup file exists ]:
   Monitor the Configuration

   Execute this step ONLY If the fdconfig backup file exists and located at step 14:

   If not already done so, establish a GUI session on the PMAC server.

   Navigate to Main Menu -> Task Monitoring

   Monitor the configuration to completion:

   ![PMAC GUI](image)

   Note: Should a failure occur with fdconfig, logs can be accessed in /var/TKLC/log/fdconfig/fdconfig.log

   [admusr@melbourne-pmac-1 fdconfig]$ sudo fdconfig dumpsteps --file=deploy_melbourne_20170329T202458_701b.fdcdb

   Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb"

   Here are the steps that were generated

   -------------- begin ---------------

   Dump of DB steps:
   NUM PHS DLY INFRA ID SVRTYPE CMD ELEMENT PRE STATE TO BGTS
   COMMAND TEXT

   ----------------------------
   1 1 0 pmac Fast_Deployment 0 21 0 Complete 300 0 Check PM&C is available
   2 1 0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet
   3 1 0 pmac Fast_Deployment 0 3 melbourne_RMS3 1 Skipped 900 0 Add Rms
   4 2 0 pmac Fast_Deployment 1
### Procedure 1: Recovery Scenario 1

1. Run below command to restart the fdconfig after a failure has occurred and has been resolved:

   ```
   $ sudo fdconfig restart --
   file=deploy_melbourne_20170329T202458_701b.fdcdb
   ```

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td>PMAC [If fdc backup file exists]: Repeat for each Rack mount server configuration file</td>
</tr>
<tr>
<td></td>
<td>Execute this step ONLY If the fdconfig backup file exists and located at step 14: Repeat steps 14-21 for each rack mount server/configuration file located at step 14, if required.</td>
</tr>
<tr>
<td>23.</td>
<td>PMAC [If fdc backup file exists]: Backup FDC file</td>
</tr>
<tr>
<td></td>
<td>Execute this step ONLY If the fdconfig backup file exists and located at step 14: Copy the updated fdc file to the fdc backup directory:</td>
</tr>
<tr>
<td></td>
<td>$ sudo cp /usr/TKLC/smac/etc/RMS/&lt;fdc_file&gt; /usr/TKLC/smac/etc/fdc/</td>
</tr>
<tr>
<td></td>
<td>Change permissions:</td>
</tr>
<tr>
<td></td>
<td>$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/&lt;fdc_file&gt;</td>
</tr>
<tr>
<td>24.</td>
<td>Perform CPU Pinning</td>
</tr>
<tr>
<td></td>
<td>Configure VM CPU socket pinning on each TVOE host to optimize performance by executing procedure “CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen9 Only)” from reference [8]</td>
</tr>
<tr>
<td></td>
<td>1. Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources.</td>
</tr>
<tr>
<td></td>
<td>2. Obtain most recent “RADIUS shared secret encryption key” file DpiKf.bin.enctr from external backup sources (Only when the RADIUS Key Revocation MOP has been executed on the system)</td>
</tr>
<tr>
<td></td>
<td>From required materials list in Section 3.1 Required Materials; use site survey documents and Network Element report (if available), to determine network configuration data.</td>
</tr>
<tr>
<td>26.</td>
<td>Execute DSR Installation Procedure for the First NOAM</td>
</tr>
<tr>
<td></td>
<td>Verify the networking data for Network Elements</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Use the backup copy of network configuration data and site surveys (Step 2)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> SDS disaster recovery actions can and should be worked simultaneously, doing so would allow faster recovery of the complete solution</td>
</tr>
</tbody>
</table>
Procedure 1: Recovery Scenario 1

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
|   | (i.e. stale DB on DP servers will not receive updates until SDS-SOAM servers are recovered. The following steps will be written to accommodate both DSR and SDS disaster recovery steps.  
  **IMPORTANT:** While creating the first NOAMs in this step, it is important that the server hostname is the same as one of the NOAM hostnames used prior to the disaster.  
  **DSR:**  
  1. Configure the first NOAM server by executing procedure “Configure First NOAM NE and Server” from reference [8]  
  2. Configure the NOAM server group by executing procedure “Configure the NOAM Server Group” from reference [8]  
  **SDS:**  
  1. Configure the first SDS NOAM server by executing procedure “Configure First SDS NOAM NE and Server” from reference [8]  
  2. Configure the SDS NOAM server group by executing procedure “Configure the SDS NOAM Server Group” from reference [8]  
  27. **NOAM GUI:** Login  
   - DSR Only, if SDS, Skip to Step 32  
   - Login to the NOAM GUI as the **guiadmin** user: |
Procedure 1: Recovery Scenario 1

28. NOAM GUI:
Upload the Backed up Database File

DSR Only, if SDS, Skip to Step 32

Browse to Main Menu->Status & Manage->Files

Select the Active NOAM server. The following screen will appear:
Procedure 1: Recovery Scenario 1

Click on **Upload** as shown below and select the file “**NO Provisioning and Configuration:**” file backed up after initial installation and provisioning.

1. Click on **Browse** and locate the backup file
2. Check **This is a backup file** box
3. Click on **Open** as shown below.

Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.

29. **NOAM GUI:** Disable Provisioning

   **DSR Only, if SDS, Skip to Step 32**

   Click on **Main Menu->Status & Manage->Database**
**Procedure 1: Recovery Scenario 1**

<table>
<thead>
<tr>
<th><strong>30.</strong></th>
<th><strong>NOAM GUI:</strong> Verify the Archive Contents and Database Compatibility</th>
<th><strong>DSR Only, If SDS, Skip to Step 32</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disable Provisioning</strong> by clicking on <strong>Disable Provisioning</strong> button at the bottom of the screen as shown below.</td>
<td><strong>Select the Active NOAM server and click on the Compare.</strong></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Disable Provisioning button" /></td>
<td><img src="image" alt="Compare button" /></td>
<td></td>
</tr>
<tr>
<td>A confirmation window will appear, press <strong>OK</strong> to disable Provisioning.</td>
<td>The following screen is displayed; click the button for the restored database file that was uploaded as a part of <strong>Step 28</strong> of this procedure.</td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Confirmation window" /></td>
<td><img src="image" alt="Database Compare screen" /></td>
<td></td>
</tr>
<tr>
<td><strong>Verify</strong> that the output window matches the screen below.</td>
<td><strong>Note:</strong> You will get a database mismatch regarding the Topology Compatibility and possibly User compatibility (due to authentication) These warnings are expected. If these are the only mismatches, proceed, otherwise stop and contact Appendix M. My Oracle Support (MOS) and ask for assistance.</td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Note: Archive Contents and Database Compatibilities must be the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Archive Contents:</strong> Configuration data</td>
</tr>
<tr>
<td><strong>Database Compatibility:</strong> The databases are compatible.</td>
</tr>
</tbody>
</table>

#### Note: The following is expected Output for Topology Compatibility Check since we are restoring from existing backed up database 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.

<table>
<thead>
<tr>
<th>31.</th>
<th><strong>ACTIVE NOAM:</strong> Restore the Database</th>
<th><strong>DSR Only,</strong> if SDS, Skip to Step 32</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>From <strong>Main Menu-&gt;Status &amp; Manage-&gt;Database</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select the <strong>Active NOAM</strong> server, and click on <strong>Restore</strong> as shown below.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Image of the interface showing the restore process" /></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The following screen will be displayed. Select the proper backup provisioning and configuration file.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Image of the interface showing backup selection" /></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Click <strong>OK</strong> Button. The following confirmation screen will be displayed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Image of the confirmation screen" /></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you get errors related to the warnings highlighted in the previous step, that is expected. If no other errors are displayed, select the <strong>Force</strong> checkbox as shown above and Click <strong>OK</strong> to proceed with the DB restore.</td>
<td></td>
</tr>
</tbody>
</table>
Procedure 1: Recovery Scenario 1

Database Restore Confirm

Incompatible archive selected

The selected database came from ZombieNOAM

Archive Contents
Configuration data

Database Compatibility
The databases are compatible.

Confirm archive "backup/Backup.dsr.ZombieNOAM1.Configuration"

Force Restore? [ ] Force

Ok   Cancel

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

32. SDS NOAM:
Transfer SDS Configuration and Provisioning backup Database Files

SDS Only, if DSR, Skip this step

Using the IP of the recovered SDS NOAM, transfer the uncompressed backup database files to the /var/TKLC/db/filemgmt directory

**Linux:**

1. From the command line of a Linux machine use the following command to copy the configuration backup file to the SDS NOAM guest:

   ```
   # scp <path_to_configuration_db_file> admusr@<SDS_NOAM_IP>:/var/TKLC/db/filemgmt
   ```

2. From the command line of a Linux machine use the following command to copy the provisioning backup file to the SDS NOAM guest:

   ```
   # scp <path_to_provisioning_db_file> admusr@<SDS_NOAM_IP>:/var/TKLC/db/filemgmt
   ```

**Note:** where `<path_to_db_file>` is the path to the backup database file on the local system and `<SDS_NOAM_IP>` is the recovered SDS NOAM IP address.
## Procedure 1: Recovery Scenario 1

### Windows:
Use WinSCP to copy the backup database files into the `/var/TKLC/db/filemgmt` directory. Please refer to [9] procedure *Using WinSCP to copy the backup image to the customer system*.

<table>
<thead>
<tr>
<th>33.</th>
<th><strong>SDS NOAM:</strong> Login</th>
<th>SDS Only, if DSR, Skip this step</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Establish an SSH session to the SDS active NOAM XMI IP address, login as <code>admusr</code>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>34.</th>
<th><strong>SDS NOAM:</strong> Stop running applications</th>
<th>SDS Only, if DSR, Skip this step</th>
</tr>
</thead>
</table>
|     | Issue the following command to stop running applications. Leave database running:
|     | `$ sudo prod.stop --ignore-cap` |

**Note:** This step may take several minutes to complete.

<table>
<thead>
<tr>
<th>35.</th>
<th><strong>SDS NOAM:</strong> Restore configuration Database</th>
<th>SDS Only, if DSR, Skip this step</th>
</tr>
</thead>
</table>
|     | Restore the configuration DB by executing the following command:
|     | `$ sudo idb.restore -n -t /var/TKLC/db/filemgmt -v
<full path to configuration archive file name>` |

<table>
<thead>
<tr>
<th>36.</th>
<th><strong>SDS NOAM:</strong> Restore provisioning Database</th>
<th>SDS Only, if DSR, Skip this step</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Refer Appendix K. Restore Provisioning Database to restore the provisioning DB.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>37.</th>
<th><strong>SDS NOAM:</strong> Start running applications</th>
<th>SDS Only, if DSR, Skip this step</th>
</tr>
</thead>
</table>
|     | Start the SDS application by executing the following command:
|     | `$ sudo prod.start` |

<table>
<thead>
<tr>
<th>38.</th>
<th><strong>NOAM VIP GUI:</strong> Login</th>
<th>SDS Only, if DSR, Skip this step</th>
</tr>
</thead>
</table>
|     | Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:
|     | `http://<Primary_NOAM_VIP_IP_Address>` |

Login as the *guiadmin* user:
## Procedure 1: Recovery Scenario 1

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 39. | **NOAM VIP GUI:** Monitor and Confirm database restoral | Wait for **5-10 minutes** for the System to stabilize with the new topology:  
Monitor the Info tab for **“Success”**. This will indicate that the restore is complete and the system is stabilized.  
The following alarms **must** be ignored for NOAM and MP Servers until all the Servers are configured:  
Alarms with Type Column as **“REPL” , “COLL” , “HA”** (with mate NOAM), **“DB”** (about Provisioning Manually Disabled)  
**Note:** Do not pay attention to these alarms until all the servers in the system are completely restored.  
**Note:** The Configuration and Maintenance information will be in the same state it was backed up during initial backup. |
| 40. | **Active NOAM:** Set Failed Servers to OOS | Navigate to **Main Menu -> Status & Manage -> HA** |
Procedure 1: Recovery Scenario 1

Select **Edit**

**Modifying HA attributes**

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Max Allowed HA Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieNOAM1</td>
<td>Active</td>
<td>The maximum des</td>
</tr>
<tr>
<td>ZombieNOAM2</td>
<td>OOS</td>
<td>The maximum des</td>
</tr>
<tr>
<td>ZombieRNOAM1</td>
<td>OOS</td>
<td>The maximum des</td>
</tr>
</tbody>
</table>

Set the Max Allowed HA Role drop down box to **OOS** for the failed servers.

Select **Ok**

41. **NOAM VIP GUI:**
   - **Recover Standby NOAM**
   - Install the second NOAM server:
     - **DSR:**
       - Execute procedure “Configure the Second NOAM Server”, steps 1, 3-6 from reference [8]
     - **SDS:**
       - Execute procedure “Configure the Second SDS NOAM Server”, steps 1, 3-6 from reference [8]

42. **Install NetBackup Client (Optional)**
   - If NetBackup is used execute procedure “Install NetBackup Client (Optional)” from reference [8]

43. **NOAM VIP GUI:**
   - **Set HA on Standby NOAM**
   - Navigate to **Status & Manage -> HA**
Procedure 1: Recovery Scenario 1

Click on Edit at the bottom of the screen

Select the standby NOAM server, set it to Active

![Modifying HA attributes](image)

Press OK

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

45. **Active NOAM:**
   - Correct the RecognizedAuthority table
   - Establish an SSH session to the active NOAM, login as admusr.
   - Execute the following command:
Procure 1: Recovery Scenario 1

$ sudo top.setPrimary
- Using my cluster: A1789
- Updating A1789.022: <DSR_NOAM_B_hostname>
- Updating A1789.144: <DSR_NOAM_A_hostname>

46. NOAM VIP GUI: Perform Keyexchange with Remote Import Server

  SDS Only, DSR Skip This Step

  1) Navigate to Main Menu -> SDS -> Configuration -> Options

  2) Uncheck the Remote Import Enabled Box:

  3) Click Apply

  Note: Re-navigate to Main Menu -> SDS -> Configuration -> Options to clear Success banner.

  4) Re-Enter the Remote Import Password:

  5) Click Apply

  Note: Re-navigate to Main Menu -> SDS -> Configuration -> Options to clear Success banner.

  6) Check the Remote Import Enabled Box:
## Procedure 1: Recovery Scenario 1

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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>51. SDS NOAM VIP GUI:</strong> Restart SDS application</td>
<td><strong>SDS Only, DSR Skip This Step</strong></td>
</tr>
<tr>
<td>Navigate to Main Menu-&gt;Status &amp; Manage-&gt;Server</td>
<td></td>
</tr>
<tr>
<td>Select the recovered Query server and click on Restart.</td>
<td></td>
</tr>
</tbody>
</table>

**52. NOAM VIP GUI:** Stop Replication to the C-Level Servers of this Site. (DSR Only) | **DSR Only, if SDS, Skip This Step** |
|   |   |
|   |   |

Click on **Edit** at the bottom of the screen

Select the Query server, set it to **Observer**

Press **OK**
<table>
<thead>
<tr>
<th>Procedure 1: Recovery Scenario 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Warning</strong></td>
<td>Prior to continuing this procedure, replication to C Level servers at the SOAM site being recovered <strong>MUST</strong> be inhibited.</td>
</tr>
<tr>
<td>Failure to inhibit replication to the working c-level servers will result in their database being destroyed!</td>
<td></td>
</tr>
<tr>
<td>If the spare SOAM is also present in the site and lost: Execute Appendix E. Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)</td>
<td></td>
</tr>
<tr>
<td>If the spare SOAM is NOT deployed in the site: Execute Appendix C. Inhibit A and B Level Replication on C-Level Servers to inhibit replication to working C Level servers before continuing.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>53. NOAM VIP GUI: Recover Active SOAM Server</th>
<th>Install the SOAM servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSR: Execute procedure “Configure the SOAM Servers”, steps 1-3, and 5-9 from reference [8]</td>
<td></td>
</tr>
<tr>
<td>Note: If you are using NetBackup, also execute step 12 of procedure “Configure the SOAM Servers” from reference [8]</td>
<td></td>
</tr>
<tr>
<td>SDS: Execute procedure “Configure the SDS DP SOAM Servers”, steps 1-3, and 5-8 from reference [8]</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>54. NOAM VIP GUI: Set HA on SOAM Server</th>
<th>Navigate to Status &amp; Manage -&gt; HA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click on <strong>Edit</strong> at the bottom of the screen</td>
<td>Select the SOAM server, set it to <strong>Active</strong></td>
</tr>
</tbody>
</table>
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>55.</td>
<td><strong>NOAM VIP GUI:</strong> Restart DSR application</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;Status &amp; Manage-&gt;Server.</strong></td>
</tr>
<tr>
<td></td>
<td>Select the recovered SOAM server and click on <strong>Restart.</strong></td>
</tr>
<tr>
<td>56.</td>
<td><strong>NOAM VIP GUI:</strong> Upload the backed up SOAM Database file (DSR Only)</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;Status &amp; Manage-&gt;Files</strong></td>
</tr>
<tr>
<td></td>
<td>Select the Active SOAM server tab. The following screen will appear. Click on <strong>Upload as shown below</strong> and select the file “<strong>SO Provisioning and Configuration:</strong>” file backed up after initial installation and provisioning.</td>
</tr>
<tr>
<td></td>
<td>1. Click on <strong>Browse</strong> and locate the backup file</td>
</tr>
</tbody>
</table>
Procedure 1: Recovery Scenario 1

2. Check **This is a backup file** Box
3. Click on Open as shown below.

Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.

57. **Recovered SOAM GUI:** Login (DSR Only)

**DSR Only, if SDS, Skip This Step**

Establish a GUI session on the recovered SOAM server.
Open the web browser and enter a URL of:

```
http://<Recovered_SOAM_IP_Address>
```

Login as the **guiadmin** user:
### Procedure 1: Recovery Scenario 1

#### 58. Recovered SOAM GUI:
- Verify the Archive Contents and Database Compatibility (DSR Only)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>DSR Only, if SDS, Skip This Step</strong></td>
</tr>
<tr>
<td></td>
<td>Click on <strong>Main Menu-&gt;Status &amp; Manage-&gt;Database</strong></td>
</tr>
<tr>
<td></td>
<td>Select the <strong>Active SOAM</strong> server and click on the <strong>Compare</strong>.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Database Compare" /></td>
</tr>
<tr>
<td></td>
<td>The following screen is displayed; click the button for the restored database file that was uploaded as a part of <strong>Step 56</strong> of this procedure.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Database Compare" /></td>
</tr>
<tr>
<td></td>
<td><strong>Verify</strong> that the output window matches the screen below.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Database Archive Compare" /></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Archive Contents and Database Compatibilities must be the following:</td>
</tr>
<tr>
<td></td>
<td><strong>Archive Contents:</strong> Configuration data</td>
</tr>
<tr>
<td></td>
<td><strong>Database Compatibility:</strong> The databases are compatible.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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:</td>
</tr>
<tr>
<td></td>
<td><strong>Topology Compatibility</strong></td>
</tr>
<tr>
<td></td>
<td><strong>THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility.</td>
</tr>
<tr>
<td></td>
<td>If the verification is successful, Click <strong>BACK</strong> button and continue to <strong>next step</strong> in this procedure.</td>
</tr>
</tbody>
</table>
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>59.</td>
<td><strong>Recovered SOAM GUI:</strong> Restore the Database (DSR Only)</td>
</tr>
<tr>
<td></td>
<td>DSR Only, if SDS, Skip This Step</td>
</tr>
<tr>
<td></td>
<td>Select the <em>Active SOAM</em> server, and click on <strong>Restore</strong> as shown below.</td>
</tr>
<tr>
<td></td>
<td>The following screen will be displayed. Select the proper back up provisioning and configuration file.</td>
</tr>
<tr>
<td></td>
<td><img src="database_compare.png" alt="" /></td>
</tr>
<tr>
<td></td>
<td>Click <strong>OK</strong> Button. The following confirmation screen will be displayed.</td>
</tr>
<tr>
<td></td>
<td>If you get an error for Node Type Compatibility, that is expected. If no other errors are displayed, select the <strong>Force</strong> checkbox as shown above and Click <strong>OK</strong> to proceed with the DB restore.</td>
</tr>
<tr>
<td></td>
<td><img src="database_restore_confirm.png" alt="" /></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> After the restore has started, the user will be logged out of XMI SOAM GUI since the restored Topology is old data.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the spare SOAM is in another network and is unreachable, the database restore cannot be done.</td>
</tr>
<tr>
<td></td>
<td><strong>Workaround</strong> - If the spare SOAM is unreachable and ping (from recovered SOAM server to spare SOAM server) hangs (as evidenced by &quot;ps -ef</td>
</tr>
<tr>
<td>60.</td>
<td><strong>Recovered SOAM GUI:</strong> Monitor and Confirm database</td>
</tr>
<tr>
<td></td>
<td>DSR Only, if SDS, Skip This Step</td>
</tr>
<tr>
<td></td>
<td>Wait for <strong>5-10 minutes</strong> for the System to stabilze with the new topology:</td>
</tr>
</tbody>
</table>
**Procedure 1: Recovery Scenario 1**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
</table>
| 61.  | **NOAM VIP GUI: Login** Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  
    | [http://<Primary_NOAM_VIP_IP_Address>](http://<Primary_NOAM_VIP_IP_Address>) Login as the *guiadmin* user: |
|      | ![Oracle System Login](image)                                        |
|      | Note: If you are using NetBackup, also execute step 12 of procedure  
    | "Configure the SOAM Servers" from reference [8]                      |

**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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
</table>
| 62.  | **NOAM VIP GUI: Recover the Remaining SOAM Servers** Recover the **remaining** SOAM servers (**Standby, Spare**):  
    | **DSR:** Execute procedure "Configure the SOAM Servers", steps 1-3, and 5-9, from reference [8]  
    | **Note:** If you are using NetBackup, also execute step 12 of procedure  
    | "Configure the SOAM Servers" from reference [8] |
## Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>SDS:</th>
<th>Execute procedure “Configure the SDS DP SOAM Servers”, steps 1-3, and 5-8 from reference [8]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>63. NOAM VIP GUI:</strong> Set HA on Remaining SOAMs</td>
<td>Navigate to <strong>Status &amp; Manage -&gt; HA</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Status &amp; Manage hierarchy" /></td>
</tr>
<tr>
<td></td>
<td>Click on <strong>Edit</strong> at the bottom of the screen</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Edit button" /></td>
</tr>
<tr>
<td></td>
<td>Select the recovered SOAM server, set it to <strong>Active</strong></td>
</tr>
<tr>
<td></td>
<td>Press <strong>OK</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>64. NOAM VIP GUI:</strong> Restart DSR application</th>
<th>Navigate to <strong>Main Menu -&gt; Status &amp; Manage -&gt; Server,</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="Status &amp; Manage hierarchy" /></td>
</tr>
<tr>
<td></td>
<td>Select the recovered standby SOAM server and click on <strong>Restart.</strong></td>
</tr>
</tbody>
</table>
Procedure 1: Recovery Scenario 1

65. NOAM VIP GUI: Start Replication on Working C-Level Servers (DSR Only)

DSR Only, if SDS, Skip This Step

Un-Inhibit (Start) Replication to the working C-Level Servers which belongs to the same site as of the failed SOAM servers.

If the spare SOAM is also present in the site and lost: Execute Appendix F. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)

If the spare SOAM is NOT deployed in the site: Execute Appendix D. Un-Inhibit A and B Level Replication on C-Level Servers

Navigate to Status & Manage -> Database

If the "Repl Status" is set to "Inhibited", click on the Allow Replication button as shown below using the following order, otherwise if none of the servers are inhibited, skip this step and continue with the next step:

- Active NOAM Server
- Standby NOAM Server
- Active SOAM Server
- Standby SOAM Server
- Spare SOAM Server (if applicable) – Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only
- Active DR NOAM Server
- Standby DR NOAM Server
- MP/IPFE Servers
- SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare) – Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only

Verify that the replication on all the working servers is allowed. This can be done by examining the Repl Status table as seen below:
Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>OAM Repl Status</th>
<th>SIG Repl Status</th>
<th>Repl Status</th>
<th>Repl Audit Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NotApplicable</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
<tr>
<td>Normal</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
<tr>
<td>Normal</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
<tr>
<td>Normal</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
</tbody>
</table>

66. **SOAM VIP GUI:** Perform Keyexchage with Export Server

Navigate to Main Menu -> Administration -> Remote Servers -> Data Export

- Remote Servers
  - LDAP Authentication
  - SNMP Trapping
  - Data Export
  - DNS Configuration

Click on **SSH Key Exchange** at the bottom of the screen

Enter the Password and press **OK**

67. **(DSR Only) Activate PCA Feature**

If you have PCA installed in the system being recovered, execute the procedure “PCA Activation on entire network” on recovered NOAM Server from [7] to re-activate PCA.

**Note:** If not all SOAM sites are recovered at this point, then you should repeat activation for each “new” SOAM site that comes online.

68. **NOAM VIP GUI:** Recover the C-Level Server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs)

**DSR:**

Execute procedure “Configure the MP Servers”, Steps 1, 9-13 from reference [8]

**Note:** Execute steps 14-16 of procedure “Configure the MP Servers”, from reference [8] if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.

**SDS (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only):**

Execute procedure “Configure the SDS DP Servers”, Steps 1, 5-8 from
Procedure 1: Recovery Scenario 1

**69.** NOAM VIP GUI: Set HA on all C-Level Servers

Navigate to **Status & Manage -> HA**

Click on **Edit** at the bottom of the screen

For each recovered C-Level whose Max Allowed HA Role is set to OOS, set it to **Active**

Press **OK**

**70.** NOAM VIP GUI: Restart DSR Application on recovered C-Level Servers.

Navigate to **Main Menu->Status & Manage->Server**

Select the recovered C-Level servers and click on **Restart**.

**71.** NOAM VIP GUI: DSR Only, SDS Skip This Step

reference [8]

Repeat this step for any remaining failed MP servers.
**Procedure 1: Recovery Scenario 1**

[ ] Start replication on all C-Level Servers (DSR Only)

Un-Inhibit *(Start)* Replication to the **ALL** C-Level Servers

Navigate to **Status & Manage -> Database**

![Status & Manage](image)

If the “Repl Status” is set to “Inhibited”, click on the Allow Replication button as shown below using the following order:

- Active NOAM Server
- Standby NOAM Server
- Active SOAM Server
- Standby SOAM Server
- Spare SOAM Server *(if applicable)-Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only)*
- Active DR NOAM Server
- Standby DR NOAM Server
- MP/IPFE Servers
- SBRS *(if SBR servers are configured, start with the active SBR, then standby, then spare) –Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only*

Verify that the replication on all the working servers is allowed. This can be done by examining the Repl Status table as seen below:

<table>
<thead>
<tr>
<th>OAM Repl Status</th>
<th>SIG Repl Status</th>
<th>Repl Status</th>
<th>Repl Audit Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NotApplicable</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
<tr>
<td>Normal</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
<tr>
<td>Normal</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
</tbody>
</table>

72. [ ] **ACTIVE NOAM:** Perform key exchange between the active-NOAM and recovered servers.

Establish an SSH session to the Active NOAM, login as `admusr`.

Execute the following command to perform a key exchange from the active NOAM to each recovered server:

```
$ keyexchange admusr@<Recovered Server Hostname>
```
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 73.  | **ACTIVE NOAM:** Activate Optional Features  
DSR Only, if SDS, Skip This Step  
Establish an SSH session to the active NOAM, login as *admusr*.  
**Note For PCA Activation:**  
If you have PCA installed in the system being recovered, execute the procedure “*PCA Activation on entire server*” on recovered NOAM Server from [6] to re-activate PCA.  
**Note:** If not all SOAM sites are recovered at this point, then you should repeat activation for each "new" SOAM site that comes online.  
**Note:** If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.  
Refer to **Section 1.5 Optional Features** to activate any features that were previously activated. |
| 74.  | **NOAM VIP GUI:** Fetch and Store the database Report for the Newly Restored Data and Save it  
Navigate to **Main Menu -> Status & Manage -> Database**  
![Diagram](image.png)  
Select the *active* NOAM server and click on the **Report** button at the bottom of the page.  
The following screen is displayed: |
Procedure 1: Recovery Scenario 1

Click on Save and save the report to your local machine.

| 75. | ACTIVE NOAM: Verify Replication Between Servers. |

Login to the Active NOAM via SSH terminal as admusr.

Execute the following command:

```
$ sudo irepstat -m
```

Output like below shall be generated:

```
-- Policy 0 ActStb [DbReplication] -----------------------------
-----------
Oahu-DAMP-1 -- Active
    BC From Oahu-SOAM-2 Active 0 0.50 ^0.15%cpu 25B/s A-me
    CC To  Oahu-DAMP-2 Active 0 0.10 0.14%cpu 25B/s A-me
Oahu-DAMP-2 -- Stby
    BC From Oahu-SOAM-2 Active 0 0.50 ^0.11%cpu 31B/s
    CC From Oahu-DAMP-1 Active 0 0.10 ^0.14 1.16%cpu 31B/s
Oahu-IPFE-1 -- Active
    BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 24B/s
    A=C3642.212
Oahu-IPFE-2 -- Active
    BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 28B/s
    A=C3642.212
Oahu-NOAM-1 -- Stby
    AA From Oahu-NOAM-2 Active 0 0.25 ^0.03%cpu 23B/s
Oahu-NOAM-2 -- Active
    AA To  Oahu-NOAM-1 Active 0 0.25 1% 0.04%cpu 61B/s
    AB To  Oahu-SOAM-2 Active 0 0.50 1% 0.05%cpu 75B/s
Oahu-SOAM-1 -- Stby
    BB From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 27B/s
```
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Oahu-NOAM-2 -- Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>AB From Oahu-NOAM-2 Active 0 0.50 ^0.03%cpu 24B/s</td>
</tr>
<tr>
<td>BB To Oahu-NOAM-1 Active 0 0.50 1%R 0.04%cpu 32B/s</td>
</tr>
<tr>
<td>BC To Oahu-IPFE-1 Active 0 0.50 1%R 0.04%cpu 21B/s</td>
</tr>
<tr>
<td>BC To Oahu-SS7MP-2 Active 0 0.50 1%R 0.04%cpu 21B/s</td>
</tr>
</tbody>
</table>

*irepstat ( 40 lines) (h)elp (m)erged*

#### 76. NOAM VIP GUI: Verify the Database states

Click on **Main Menu->Status and Manager->Database**

Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below:

<table>
<thead>
<tr>
<th>Network Element</th>
<th>Server</th>
<th>Role</th>
<th>OAM Max HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieDRNOAM</td>
<td>ZombieDRNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM2</td>
<td>Network OAM&amp;P</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM2</td>
<td>System OAM</td>
<td>N/A</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM1</td>
<td>System OAM</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM</td>
<td>ZombieDRNOAM2</td>
<td>Network OAM&amp;P</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSS7MP2</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSS7MP1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieFTE1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieFTE2</td>
<td>MP</td>
<td>Active</td>
</tr>
</tbody>
</table>

#### 77. NOAM VIP GUI: Upload the backed up RADIUS Key file (RADIUS Only)

**DSR Only, if SDS, Skip This Step**

If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)

Navigate to **Main Menu->Status & Manage->Files**
Procedure 1: Recovery Scenario 1

Select the Active NOAM server tab. The following screen will appear. Click on Upload as shown below and select the file "RADIUS shared secret encryption key:" file backed up after initial installation and provisioning or after key revocation execution.

Click on Browse and Locate the DpiKf.bin.encr file and click on Open as shown below.

Click on the Upload button. The file will take a few seconds to upload depending on the size of the file. The file will be visible on the list of entries after the upload is complete.

Note: This file should be deleted from the operator's local servers as soon as key file is uploaded to Active NOAM server.

78. NOAM VIP:
Copy and distribute RADIUS Key file on Active NOAM (RADIUS Only)-Part 1

If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)

Login to the Active NOAM VIP via SSH terminal as admusr user.

Execute the following commands to copy the key file:
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Command 1</th>
<th>Command 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>$ cd /usr/TKLC/dpi/bin</code></td>
<td><code>$ ./sharedKrevo -decr</code></td>
</tr>
<tr>
<td><code>$ sudo rm /var/TKLC/db/filemgmt/&lt;backed up key file name&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>

Execute following command to check if all the servers in topology are accessible:

```
$ ./sharedKrevo -checkAccess
```

#### Example output:

```
[admusr@NOAM-2 bin]$ ./sharedKrevo -checkAccess
FIPS integrity verification test failed. 1450723084: [INFO] 'NOAM-1' is accessible.
FIPS integrity verification test failed. 1450723084: [INFO] 'SOAM-1' is accessible.
FIPS integrity verification test failed. 1450723085: [INFO] 'SOAM-2' is accessible.
FIPS integrity verification test failed. 1450723085: [INFO] 'IPFE' is accessible.
FIPS integrity verification test failed. 1450723085: [INFO] 'MP-2' is accessible.
```

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

<table>
<thead>
<tr>
<th>No.</th>
<th>NOAM VIP:</th>
</tr>
</thead>
<tbody>
<tr>
<td>79.</td>
<td>Copy and distribute RADIUS Key file on Active NOAM (RADIUS Only)-Part 2</td>
</tr>
</tbody>
</table>

If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)

Execute following command to distribute key file to all the servers in the topology :

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

Example output:
Procedure 1: Recovery Scenario 1

Note: For any errors contact Appendix M. My Oracle Support (MOS)

80. 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”.

<table>
<thead>
<tr>
<th>Hostname</th>
<th>OAM HA Role</th>
<th>Application HA Role</th>
<th>Max Allowed HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Standby</td>
</tr>
</tbody>
</table>

81. NOAM GUI: Enable Provisioning

Click on Main Menu->Status & Manage->Database
**Procedure 1: Recovery Scenario 1**

<table>
<thead>
<tr>
<th></th>
<th>Status &amp; Manage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Network Elements</td>
</tr>
<tr>
<td></td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td>HA</td>
</tr>
<tr>
<td></td>
<td>Database</td>
</tr>
<tr>
<td></td>
<td>KPIs</td>
</tr>
<tr>
<td></td>
<td>Processes</td>
</tr>
<tr>
<td>+</td>
<td>Tasks</td>
</tr>
<tr>
<td></td>
<td>Files</td>
</tr>
</tbody>
</table>

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

![Enable Provisioning Button](image)

A confirmation window will appear, press **OK** to enable Provisioning.

<table>
<thead>
<tr>
<th></th>
<th><strong>SOAM GUI:</strong> Enable Provisioning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>DSR Only, if SDS, Skip This Step</strong></td>
</tr>
<tr>
<td></td>
<td>Click on <strong>Main Menu-&gt;Status &amp; Manage-&gt;Database</strong></td>
</tr>
</tbody>
</table>

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

![Enable Site Provisioning Button](image)

A confirmation window will appear, press **OK** to enable Provisioning.

<table>
<thead>
<tr>
<th></th>
<th><strong>SOAM VIP GUI:</strong> Verify the Local Node Info (DSR Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>DSR Only, SDS Skip This Step</strong></td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;Diameter-&gt;Configuration-&gt;Local Node</strong></td>
</tr>
</tbody>
</table>
## Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 84. | **SOAM VIP GUI:** Verify the Peer Node Info (DSR Only) | **DSR Only, SDS Skip This Step**
|     | Navigate to Main Menu->Diameter->Configuration->Peer Node |
|     | Verify that all the peer nodes are shown. |

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 85. | **SOAM VIP GUI:** Verify the Connections Info (DSR Only) | **DSR Only, SDS Skip This Step**
|     | Navigate to Main Menu->Diameter->Configuration->Connections |
|     | Verify that all the connections are shown. |

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 86. | **MP Servers:** | **DSR Only, SDS Skip This Step**
|     | |
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable SCTP Auth Flag (DSR Only)</td>
<td>For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [12]. Execute this procedure on all Failed MP Servers.</td>
</tr>
</tbody>
</table>
| 87. | SOAM VIP GUI: Enable Connections if needed (DSR Only) | DSR Only, SDS Skip This Step

**Navigate to** Main Menu - Diameter - Maintenance - Connections

- Select each connection and click on the Enable button. Alternatively you can enable all the connections by selecting the EnableAll button.

Verify that the Operational State is Available.

**Note:** If a Disaster Recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution.

| 88. | SOAM VIP GUI: Enable Optional Features (DSR Only) | DSR Only, SDS Skip This Step

**Navigate to** Main Menu -> Diameter -> Maintenance -> Applications

- Select the optional feature application configured in step 73.

Click the Enable button.

| 89. | SOAM VIP GUI: Re-enable Transports if needed (DSR Only) | DSR Only, SDS Skip This Step

**Navigate to** Main Menu -> Transport Manager -> Maintenance -> Transport
Procedure 1: Recovery Scenario 1

90. Needed (DSR Only)

Select each transport and click on the Enable button

Verify that the Operational Status for each transport is Up.

91. DSR Only, SDS Skip This Step

SOAM VIP GUI:
Re-enable MAPIWF application if needed (DSR Only)

Navigate to Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users

Click on Enable button corresponding to MAPIWF Application Name.

Verify that the SSN Status is Enabled.

SOAM VIP GUI:
Re-enable links if needed (DSR Only)

Navigate to Main Menu->SS7/Sigtran->Maintenance->Links

Click on Enable button for each link.
## Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th></th>
<th>Verify that the Operational Status for each link is Up.</th>
</tr>
</thead>
</table>
| 92. | **SOAM VIP GUI: Examine All Alarms**  
     Navigate to **Main Menu->Alarms & Events->View Active**  
     Examine all active alarms and refer to the on-line help on how to address them.  
     If needed contact **Appendix M. My Oracle Support (MOS)**. |
| 93. | **NOAM VIP GUI: Examine All Alarms**  
     Login to the NOAM VIP if not already logged in.  
     Navigate to **Main Menu->Alarms & Events->View Active**  
     Examine all active alarms and refer to the on-line help on how to address them.  
     If needed contact **Appendix M. My Oracle Support (MOS)**. |
| 94. | **Restore GUI Usernames and Passwords**  
     If applicable, Execute steps in **Section 6.0** to recover the user and group information restored. |
| 95. | **Backup and Archive All the Databases from the Recovered System**  
     Execute **Appendix A. Database Backup** to back up the Configuration databases: |
| 96. | **Recover IDIH (If Configured)**  
     If any components of IDIH were affected, refer to **Section 7.0** to perform the disaster recovery on IDIH. |
| 97. | **SNMP Workaround**  
     Refer to **Appendix J. SNMP Configuration** to configure SNMP as a workaround in the following cases:  
     1) If SNMP is not configured in DSR/SDS  
     2) If SNMP is already configured and **SNMPv3** is selected as enabled |
**Procedure 1: Recovery Scenario 1**

<table>
<thead>
<tr>
<th>version</th>
<th></th>
</tr>
</thead>
</table>
5.1.2 Recovery Scenario 2 (Partial Server Outage with at least one NOAM server intact and all SOAMs failed)

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

Recover **Standby NOAM** server *(if needed)* by recovering base hardware and software.
- Recover the base hardware.
- Recover the software.

Recover **Query Server** *(if needed)* by recovering base hardware and software.
- Recover the base hardware.
- Recover the software.

Recover **Active SOAM** server by recovering base hardware, software and database.
- Recover the base hardware.
- Recover the software.
- Recover the Database.

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

Recover IDIH if necessary
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Workarounds</th>
<th>Collect Required Materials</th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
</table>
| 1.     | This procedure performs recovery if at least 1 NOAM server is available but all SOAM servers in a site have failed. This includes any SOAM server that is in another location.  
Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.  
If this procedure fails, contact Appendix M. My Oracle Support (MOS) and ask for assistance. | Refer to Appendix I. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.  
Refer to Appendix J. SNMP Configuration to configure SNMP as a workaround in the following cases:  
1) If SNMP is not configured in DSR/SDS  
2) If SNMP is already configured and SNMPv3 is selected as enabled version | Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  
http://<Primary_NOAM_VIP_IP_Address>  
Login as the guiadmin user: |
## Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Active NOAM: Set Failed Servers to OOS</td>
</tr>
</tbody>
</table>

Navigate to **Main Menu -> Status & Manage -> HA**

Select **Edit**
Procedure 2: Recovery Scenario 2

Set the Max Allowed HA Role drop down box to OOS for the failed servers.

Select Ok

5. Replace Failed Equipment

HW vendor to replace the failed equipment

6. Recover PMAC TVOE Host (If Required): Configure BIOS Settings and Update Firmware

1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:
   - HP DL380 Gen8: “Configure HP Gen 8 Server BIOS Settings”

2. Verify and/or upgrade server firmware by executing procedure “Upgrade Rack Mount Server Firmware” from reference [8]

7. Recover PMAC and PMAC TVOE Host: Backup Available

If the PMAC is located on the failed rack mount server(s), execute this step. Otherwise skip to step 10.

This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step.

1. Restore the TVOE backup by executing Appendix G. Restore TVOE Configuration from Backup Media on ALL failed rack mount servers

2. Restore the PMAC backup by executing Appendix H. Restore PMAC from Backup

Proceed to Step 10
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>Recover PMAC and PMAC TVOE Host: Backup Not Available</td>
</tr>
<tr>
<td></td>
<td><strong>If the PMAC is located on the failed rack mount server(s), execute this step. Otherwise skip to step 10.</strong></td>
</tr>
<tr>
<td></td>
<td>This step assumes that TVOE and PMAC backups are NOT available, if the TVOE and PMAC have already been restored, <strong>skip this step</strong></td>
</tr>
<tr>
<td></td>
<td>1. Execute procedure “Install and Configure TVOE on First RMS (PMAC Host)” from reference [8]</td>
</tr>
<tr>
<td></td>
<td>2. Execute section “Install PMAC” from reference [8]</td>
</tr>
<tr>
<td></td>
<td>3. Execute section “Initialize the PMAC Application” from reference [8]</td>
</tr>
<tr>
<td></td>
<td><strong>Proceed to Next Step</strong></td>
</tr>
<tr>
<td>9.</td>
<td>Configure PMAC (No Backup)</td>
</tr>
<tr>
<td></td>
<td><strong>If PMAC backup was NOT restored in step 7, execute this step. Otherwise Skip this Step.</strong></td>
</tr>
<tr>
<td></td>
<td>Execute sections “Configure PMAC Server (NetBackup Only)” and “Add RMS to the PMAC Inventory” from reference [8]</td>
</tr>
<tr>
<td>10.</td>
<td>Install/Configure Additional Rack Mount Servers</td>
</tr>
<tr>
<td></td>
<td><strong>If TVOE backups were NOT performed on any additional rack mount servers or are not available, execute this step. Otherwise Skip this Step</strong></td>
</tr>
<tr>
<td></td>
<td>1. Execute procedure “Install TVOE on Additional Rack Mount Servers” from reference [8]</td>
</tr>
<tr>
<td></td>
<td>2. Execute “Configure TVOE on Additional Rack Mount Servers” from reference [8]</td>
</tr>
<tr>
<td></td>
<td>3. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:</td>
</tr>
<tr>
<td></td>
<td>- HP DL380 Gen8: “Configure HP Gen 8 Server BIOS Settings”</td>
</tr>
<tr>
<td></td>
<td><strong>HP DL380 GEN 8 SKIP THIS STEP</strong></td>
</tr>
<tr>
<td></td>
<td>Refer to the DSR VM placement and Pinning workbook to determine proper VM placement and pinning.</td>
</tr>
<tr>
<td>12.</td>
<td>Deploy Redundant PMAC</td>
</tr>
<tr>
<td></td>
<td><strong>If the redundant PMAC is located on the failed rack mount server(s), execute this step. Otherwise skip to next step.</strong></td>
</tr>
<tr>
<td></td>
<td>Refer to procedure “Deploy Redundant PMAC (Optional)” to re-deploy and configure any redundant PMACs previously configured.</td>
</tr>
<tr>
<td>13.</td>
<td>PMAC: Determine if an fdconfig file exists from the</td>
</tr>
</tbody>
</table>
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>No.</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
</table>
| 14. | **If FDCONFIG backup file does NOT exist:** | **Execute this step ONLY If the fdconfig backup file does **NOT** exist:**  
Examine the results and verify whether the rms config file <hostname>.cfg exists.  
**Note:** There may be multiple fdconfig backup files here with respect to each RMS. Select the respective one according to the RMS.  
If the fdconfig file does NOT exist: Create the needed file(s) by executing section “Virtual Machine/Network Fast Deployment” from reference [8]  
**WARNING:** It is very important to ensure the file(s) created only affect the TVOE server(s) and its Guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service. |
| 15. | **PMAC [If fdc backup file exists ]:**  
Load ISOs into PMAC if not done already | **Execute this step ONLY If the fdconfig backup file exists and located at step 13:**  
Examine the results and verify whether the rms config file <hostname>.cfg exists.  
If the DSR, SDS, and TPD ISOs are NOT loaded in to the PMAC: Execute procedures 14 of section “Virtual Machine/Network Fast Deployment” from reference [8]  
If already loaded into PMAC, skip this step. |
| 16. | **PMAC [If fdc backup file exists ]:**  
Edit/Update Configuration File | **Execute this step ONLY If the fdconfig backup file exists and located at step 13:**  
Examine the results and verify whether the rms config file <hostname>.cfg exists.  
**Edit the fdconfig file to include only the required/failed servers.**  
**Note:** Comment out configuration items that are not needed.  
**Note:** It is recommended that a separate configuration file be created for EACH rack mount server being deployed.  
Note:Cabinet ID in the config file needs to match the cabinet already defined in PM&C”  
The following items are mandatory:  
- siteName  
- tpdIso  
- dsrIso (if DSR VMs are being configured)  
- sdsIso (if SDS VMs are being configured)  
- NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured)  
- XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured)  
- XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured)  
- DSRNOAM1XMIIADDRESS (if DSRNOAM1 is being configured)  
- DSRNOAM2XMIIADDRESS (if DSRNOAM2 is being configured)  
- DSRDRNOAM1XMIIADDRESS (if DSRDRNOAM1 is being configured) |
## Procedure 2: Recovery Scenario 2

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
|   | - DSRDROAM2XMIPvADDRESS (if DSRDROAM2 is being configured)  
|   | - SDSNOAM1XMIPvADDRESS (if SDSNOAM1 is being configured)  
|   | - SDSNOAM2XMIPvADDRESS (if SDSNOAM2 is being configured)  
|   | - SDSDRNOAM1XMIPvADDRESS (if SDSDRNOAM1 is being configured)  
|   | - SDSDRNOAM2XMIPvADDRESS (if SDSDRNOAM2 is being configured)  

**Note:** Refer to Appendix R: VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8]

Note: Comment out SDS and DSR profile items if corresponding products are not used.

**Note:** [Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9]: Refer to Appendix Q.3: Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8]

**Note:** The VM names should not be modified in the .cfg file. The names are fixed and will be prefixed in the siteName.

**Note:** The VM locations should not be changed from their 'RMSx' format. Each RMS should correspond with a separate Rack Mount Server.

### WARNING:

It is very important to ensure the file(s) created only affect the TVOE server(s) and its Guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 17. PMAC [If fdc backup file exists]: | Copy the located backedup fdc file to the RMS directory  
| Execute this step ONLY If the fdconfig backup file exists and located at step 13: | $ cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file> /usr/TKLC/smac/etc/RMS/  
|   |   |
| 18. PMAC [If fdc backup file exists]: | Execute the config.sh script  
| Execute this step ONLY If the fdconfig backup file exists and located at step 13: |   |
## Procedure 2: Recovery Scenario 2

Execute config.sh against the modified backup config file defined above:

**Note:** If the below command is executed on multiple cfg files, it will overwrite the existing xml file. It is recommended to rename the xml file before running the below command again.

```bash
$ sudo ./config.sh <config file>
```

Sample Output:

```
[admusr@5010441PMAC RMS]$ sudo ./config.sh rms.cfg
Validating cfg file...
Successful validation of cfg file.
Added Cabinet 101 to Fast Deployment File.
Added Zombie_TPOE1 to Fast Deployment File.
Added Zombie_TPOE2 to Fast Deployment File.
Added xmi(bond0.4) to Fast Deployment File.
Added im1(bond0.3) to Fast Deployment File.
Added rep(bond1.10) to Fast Deployment File.
Added xal(bond1.6) to Fast Deployment File.
Added xal2(bond1.7) to Fast Deployment File.
Added xal3(bond1.8) to Fast Deployment File.
Added xal4(bond1.9) to Fast Deployment File.
Added xal5(bond1.11) to Fast Deployment File.
Added xal6(bond1.12) to Fast Deployment File.
Added xal7(bond1.13) to Fast Deployment File.
Added xal8(bond1.14) to Fast Deployment File.
Added xal9(bond1.15) to Fast Deployment File.
Added xal10(bond1.16) to Fast Deployment File.
Added xal11(bond1.17) to Fast Deployment File.
Added xal12(bond1.18) to Fast Deployment File.
Added xal13(bond1.19) to Fast Deployment File.
Added xal14(bond1.20) to Fast Deployment File.
Added xal15(bond1.21) to Fast Deployment File.
Added xal16(bond1.22) to Fast Deployment File.
Added Zombie_DSHERNTO2 to Fast Deployment File.
Added Zombie_DSHERNTO1 to Fast Deployment File.
Added Zombie_DSHERNTO2 to Fast Deployment File.
Added Zombie_DSHERNTO1 to Fast Deployment File.
Added Zombie_DSHERNTO2 to Fast Deployment File.
Added Zombie_DSHERNTO1 to Fast Deployment File.
Added Zombie_DSHERNTO2 to Fast Deployment File.
Added Zombie_DSHERNTO1 to Fast Deployment File.
Validating Fast Deployment File.......
Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml"
Configuration file validation successful.
Validation complete.
Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml
SUCCESS: OPERATION SUCCESS!!
```

| 19. PMAC [If fdconfig backup file exists]: | Execute this step ONLY if the fdconfig backup file exists and located at step 13: |
### Procedure 2: Recovery Scenario 2

**Execute Fast Deployment**

With the file generated from the config.sh script, execute the following command to start fast deployment:

```bash
$ screen
$ sudo fdconfig config --
file=<fd_config.xml>
```

**Note:** This is a long duration command. If the screen command was run prior to executing the fdconfig, perform a “screen -dr” to resume the screen session in the event of a terminal timeout etc.

**PMAC GUI [If fdc backup file exists]:**

Monitor the Configuration

**Execute this step ONLY if the fdconfig backup file exists and located at step 13:**

- If not already done so, establish a GUI session on the PMAC server.
- Navigate to **Main Menu -> Task Monitoring**

Monitor the configuration to completion:

```
[admusr@melbourne-pmac-1 fdconfig]$ sudo fdconfi
g dumpsteps --
file=deploy_melbourne_20170329T202458_701b.fdcdb
```

Here are the steps that were generated

```
---------- begin ----------
```
## Procedure 2: Recovery Scenario 2

### Dump of DB steps:

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>TEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUM</td>
<td>PHS</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1 0</td>
<td>pmac</td>
</tr>
<tr>
<td>2 1 0</td>
<td>pmac</td>
</tr>
<tr>
<td>3 1 0</td>
<td>pmac</td>
</tr>
<tr>
<td>4 2 0</td>
<td>pmac</td>
</tr>
</tbody>
</table>

Run Below command to restart the fdconfig after a failure has occurred and has been resolved:

```bash
$sudo fdconfig restart --
file=deploy_melbourne_20170329T202458_701b.fdcd
```

| PMAC | [If fdc backup file exists ]:
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>21.</td>
<td>Repeat for each Rack mount server configuration file</td>
</tr>
<tr>
<td></td>
<td>Repeat steps 13-20 for each rack mount server/configuration file located at step 13, if required.</td>
</tr>
</tbody>
</table>

| PMAC | [If fdc backup file exists ]:
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td>Backup FDC file</td>
</tr>
<tr>
<td></td>
<td>Execute this step only If the fdconfig backup file exists and located at step 13:</td>
</tr>
<tr>
<td></td>
<td>Issue the following commands:</td>
</tr>
<tr>
<td></td>
<td>Copy the updated fdc file to the fdc backup directory:</td>
</tr>
</tbody>
</table>

```bash
$sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file>/usr/TKLC/smac/etc/fdc/
```

<table>
<thead>
<tr>
<th>Change permissions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/&lt;fdc_file&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Perform CPU Pinning</th>
<th>Configure VM CPU socket pinning on each TVOE host to optimize performance by executing procedure “CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only)” from reference [8]</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>NOAM VIP GUI: Login</th>
<th>If the failed server(s) are NOT OAM type, skip to step 47</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>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:</td>
</tr>
</tbody>
</table>
## Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 25. | **NOAM VIP GUI:** Recover Standby NOAM (if needed)  
DSR:  
Execute procedure “Configure the Second NOAM Server”, steps 1, 3-6 from reference [8]  
SDS:  
Execute procedure “Configure the Second SDS NOAM Server”, steps 1, 3-6 from reference [8] |
| 26. | **Install NetBackup Client (Optional)**  
If NetBackup is used execute procedure “Install NetBackup Client (Optional)” from reference [8] |
| 27. | **NOAM VIP GUI:**  
Set HA on Standby NOAM  
Navigate to Status & Manage -> HA |
Procedure 2: Recovery Scenario 2

28. **NOAM VIP GUI:** Restart DSR application

Navigate to **Main Menu->Status & Manage->Server,**

Select the recovered standby NOAM server and click on **Restart.**

29. **NOAM VIP GUI:** Recover Query Servers

**SDS Only, DSR Skip This Step**

Execute procedure “Configuring SDS Query Servers”, steps 1, 4-7 from reference [8] if recovering query servers.
## Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>SDS NOAM VIP GUI:</th>
<th>SDS only, DSR Skip This Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.</td>
<td>Set HA on Query Server</td>
<td>Navigate to <strong>Status &amp; Manage -&gt; HA</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Status &amp; Manage</strong></td>
<td><strong>Network Elements</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Server</strong></td>
<td><strong>HA</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Database</strong></td>
<td><strong>KPIs</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Processes</strong></td>
<td><strong>Tasks</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Files</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Edit</strong> at the bottom of the screen</td>
<td>Click on <strong>Edit</strong></td>
</tr>
<tr>
<td></td>
<td>Select the Query server, set it to <strong>Observer</strong></td>
<td>Select the Query server, set it to <strong>Observer</strong></td>
</tr>
<tr>
<td></td>
<td>Press <strong>OK</strong></td>
<td>Press <strong>OK</strong></td>
</tr>
<tr>
<td>31.</td>
<td>Restart SDS application</td>
<td>Navigate to <strong>Main Menu -&gt; Status &amp; Manage -&gt; Server</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Status &amp; Manage</strong></td>
<td><strong>Network Elements</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Server</strong></td>
<td><strong>HA</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Database</strong></td>
<td><strong>KPIs</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Processes</strong></td>
<td><strong>Tasks</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Files</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the recovered Query server and click on <strong>Restart</strong>.</td>
</tr>
<tr>
<td>32.</td>
<td>Stop Replication to the C-Level Servers of this</td>
<td>DSR Only, if SDS, Skip This Step</td>
</tr>
<tr>
<td></td>
<td><strong>NOAM VIP GUI:</strong></td>
<td><strong>DSR only, DSR Skip This Step</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Stop Replication</strong></td>
<td><strong>Stop Replication</strong></td>
</tr>
<tr>
<td></td>
<td>to the C-Level Servers of this</td>
<td>to the C-Level Servers of this</td>
</tr>
</tbody>
</table>
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prior to continuing this procedure, replication to C Level servers at the SOAM site being recovered <strong>MUST</strong> be inhibited.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Failure to inhibit replication to the working c-level servers will result in their database being destroyed!</strong></td>
<td></td>
</tr>
<tr>
<td><strong>If the spare SOAM is also present in the site and lost:</strong> Execute Appendix E. Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)</td>
<td></td>
</tr>
<tr>
<td><strong>If the spare SOAM is NOT deployed in the site:</strong> Execute Appendix C. Inhibit A and B Level Replication on C-Level Servers to inhibit replication to working C Level servers before continuing.</td>
<td></td>
</tr>
</tbody>
</table>

#### 33. **NOAM VIP GUI:** Recover Active SOAM Server
- Install the SOAM servers
- **DSR:**
  - Execute procedure “Configure the SOAM Servers”, steps 1-3, and 5-9 from reference [8]
  - **Note:** If you are using NetBackup, also execute step 12 of procedure “Configure the SOAM Servers” from reference [8]
- **SDS:**
  - Execute procedure “Configure the SDS DP SOAM Servers”, steps 1-3, and 5-8 from reference [8]

#### 34. **NOAM VIP GUI:** Set HA on SOAM Server
- Navigate to **Status & Manage -> HA**
### Procedure 2: Recovery Scenario 2

#### Click on **Edit** at the bottom of the screen

Select the SOAM server, set it to **Active**

<table>
<thead>
<tr>
<th>Zombie SOAM1</th>
<th>The.m</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active</strong></td>
<td></td>
</tr>
<tr>
<td>Zombie SOAM2</td>
<td>The.m</td>
</tr>
<tr>
<td>Standby</td>
<td></td>
</tr>
<tr>
<td>Spare</td>
<td></td>
</tr>
<tr>
<td>Observer</td>
<td></td>
</tr>
<tr>
<td>OOS</td>
<td></td>
</tr>
</tbody>
</table>

Press **OK**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>35.</td>
<td><strong>NOAM VIP GUI:</strong> Restart DSR application</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;Status &amp; Manage-&gt;Server</strong>, select the recovered SOAM server and click on <strong>Restart</strong>.</td>
</tr>
<tr>
<td>36.</td>
<td><strong>NOAM VIP GUI:</strong> Upload the backed up SOAM Database file (DSR Only)</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;Status &amp; Manage-&gt;Files</strong></td>
</tr>
<tr>
<td></td>
<td><strong>DSR Only, if SDS, Skip This Step</strong></td>
</tr>
</tbody>
</table>
Procedure 2: Recovery Scenario 2

Select the Active SOAM server tab. The following screen will appear. Click on Upload as shown below and select the file “SO Provisioning and Configuration” file backed up after initial installation and provisioning.

1. Click on Browse and locate the backup file
2. Check This is a backup file Box
3. Click on Open as shown below.

Click on the Upload button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.

37. Recovered SOAM GUI: Login (DSR Only)  DSR Only, SDS Skip This Step

Establish a GUI session on the recovered SOAM server. Open the web browser and enter a URL of:

http://<Recovered_SOAM_IP_Address>

Login as the guiadmin user:
### Procedure 2: Recovery Scenario 2

#### 38. Recovered SOAM GUI:
- Verify the Archive Contents and Database Compatibility (DSR Only)

DSR Only, if SDS, Skip This Step

Click on **Main Menu->Status & Manage->Database**

Select the **Active SOAM** server and click on the **Compare**.

The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 36**, of this procedure.

**Database Compare**

- Select archive to compare on server: 7
- Archive: backup\backup\DSR.2cm

Verify that the output window matches the screen below.
Procedure 2: Recovery Scenario 2

### Database Archive Compare

The selected database came from ZombiesOCM on 1

- **Archive Contents**: Configuration data
- **Database Compatibility**: The databases are compatible.

**Note**: Archive Contents and Database Compatibilities must be the following:

- **Archive Contents**: Configuration data
- **Database Compatibility**: The databases are compatible.

**Note**: The following is expected output for Topology Compatibility Check since we are restoring from existing backed up database 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.

<table>
<thead>
<tr>
<th>39.</th>
<th><strong>Recovered SOAM GUI</strong>: Restore the Database (DSR Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>DSR Only, if SDS, Skip This Step</strong></td>
</tr>
</tbody>
</table>

Select the **Active SOAM** server, and click on **Restore** as shown below.

The following screen will be displayed. Select the proper backup provisioning and configuration file.

### Database Compare

Select archive to compare on sen

<table>
<thead>
<tr>
<th>Archive</th>
<th>backup/backup.dsr.Z</th>
</tr>
</thead>
</table>

Click **OK** Button. The following confirmation screen will be displayed.

If you get an error for Node Type Compatibility, that is expected. If no other errors are displayed, select the **Force** checkbox as shown above and click **OK** to proceed with the DB restore.
Procedure 2: Recovery Scenario 2

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Database Restore Confirm</strong></td>
</tr>
<tr>
<td></td>
<td>Compatible archive.</td>
</tr>
<tr>
<td></td>
<td>The selected database came from Zombi.</td>
</tr>
<tr>
<td></td>
<td>Archive Contents</td>
</tr>
<tr>
<td></td>
<td>Configuration data</td>
</tr>
<tr>
<td></td>
<td>Database Compatibility</td>
</tr>
<tr>
<td></td>
<td>The databases are compatible.</td>
</tr>
</tbody>
</table>

**Note:** After the restore has started, the user will be logged out of XMI SOAM GUI since the restored Topology is old data. The provisioning will be disabled after this step.

**Note (For DSR 8.0 Recovery ONLY):** If the spare SOAM is in another network and is unreachable, a workaround must be executed to ensure a successful database restore. Follow the below workaround for this scenario.

**Workaround** - If the spare SOAM is unreachable and ping (from recovered SOAM server to spare SOAM server) hangs (as evidenced by "ps -ef | grep ping" showing the same ping process and its child for more than 10 seconds), kill the hung ping processes and the restore will proceed.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>40.</strong></td>
<td><strong>Recovered SOAM GUI:</strong></td>
</tr>
<tr>
<td></td>
<td>Monitor and Confirm database restoral (DSR Only)</td>
</tr>
<tr>
<td></td>
<td>DSR Only, if SDS, Skip This Step</td>
</tr>
<tr>
<td></td>
<td>Wait for 5-10 minutes for the System to stabilize with the new topology:</td>
</tr>
<tr>
<td></td>
<td>Monitor the Info tab for “Success”. This will indicate that the restore is complete and the system is stabilized.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not pay attention to alarms until all the servers in the system are completely restored.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Configuration and Maintenance information will be in the same state it was backed up during initial backup.</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>41.</strong></td>
<td><strong>NOAM VIP GUI:</strong></td>
</tr>
<tr>
<td></td>
<td>Login</td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td><img src="http://%3CPrimary_NOAM_VIP_IP_Address%3E" alt="http://&lt;Primary_NOAM_VIP_IP_Address&gt;" /></td>
</tr>
<tr>
<td></td>
<td>Login as the <strong>guiadmin</strong> user:</td>
</tr>
</tbody>
</table>
## Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>42.</td>
<td>NOAM VIP GUI: Recover the Remaining SOAM Servers</td>
</tr>
<tr>
<td></td>
<td><strong>DSR:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>43.</td>
<td>NOAM VIP GUI: Start replication on the recovered SOAMs</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>44.</th>
<th><strong>NOAM VIP GUI:</strong> Set HA on Recovered standby SOAM Server</th>
</tr>
</thead>
</table>

- Navigate to **Status & Manage -> HA**
- Click on **Edit** at the bottom of the screen
- Select the recovered standby SOAM server, set it to **Active**
- Press **OK**

<table>
<thead>
<tr>
<th>45.</th>
<th><strong>NOAM VIP GUI:</strong> Restart DSR application</th>
</tr>
</thead>
</table>

- Navigate to **Main Menu->Status & Manage->Server**, 

Click on the Allow Replication button as shown below on the recovered SOAM servers.

Verify that the replication on all SOAMs servers is allowed. This can be done by checking 'Repl status' column of respective server.
Procedure 2: Recovery Scenario 2

Select the recovered standby SOAM server and click on **Restart**.

### NOAM VIP GUI:
**Start Replication on Working C-Level Servers (DSR Only)**

<table>
<thead>
<tr>
<th>46.</th>
<th>NOAM VIP GUI: Start Replication on Working C-Level Servers (DSR Only)</th>
<th>DSR Only, if SDS, Skip This Step</th>
</tr>
</thead>
</table>

**Un-Inhibit (Start) Replication to the **working** C-Level Servers which belongs to the same site as of the failed SOAM servers.**

**If the spare SOAM is also present in the site and lost:** Execute Appendix F. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)

**If the spare SOAM is NOT deployed in the site:** Execute Appendix D. Un-Inhibit A and B Level Replication on C-Level Servers

Navigate to **Status & Manage -> Database**

If the **“Repl Status”** is set to “Inhibited”, click on the **Allow Replication** button as shown below using the following order, otherwise if none of the servers are inhibited, skip this step and continue with the next step:

- Active NOAM Server
- Standby NOAM Server
- Active SOAM Server
- Standby SOAM Server
- Spare SOAM Server *(if applicable)* – Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only
- Active DR NOAM Server
Procedure 2: Recovery Scenario 2

- Standby DR NOAM Server
- MP/IPFE Servers
- SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare) – Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only

Verify that the replication on all the working servers is allowed. This can be done by examining the Repl Status table as seen below:

<table>
<thead>
<tr>
<th>OAM Repl Status</th>
<th>SIG Repl Status</th>
<th>Repl Status</th>
<th>Repl Audit Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NotApplicable</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
<tr>
<td>Normal</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
<tr>
<td>Normal</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
<tr>
<td>Normal</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
</tbody>
</table>

47. (DSR Only) **Activate PCA Feature**

If you have PCA installed in the system being recovered, execute the procedures “PCA Activation on Stand By NOAM network” on recovered StandBy NOAM Server and “PCA Activation on Active SOAM network” on recovered Active SOAM Server from [7] to re-activate PCA.

48. **NOAM VIP GUI: Recover the C-Level Server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs)**

Recover C-Level Servers:

**DSR:**

Execute procedure “Configure the MP Servers”, Steps 1, 9-13 from reference [8]

**Note:** Execute steps 14-16 of procedure “Configure the MP Servers” from reference [8] if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.

**SDS:**

Execute procedure “Configure the SDS DP Servers”, Steps 1, 5-8 from reference [8].

Repeat this step for any remaining failed MP servers.

49. **NOAM VIP GUI: Set HA on all C-Level Servers**

Navigate to **Status & Manage -> HA**

- Click on **Edit** at the bottom of the screen

For each recovered C-Level whose Max Allowed HA Role is set to OOS, set it to **Active**.
### Procedure 2: Recovery Scenario 2

**50. NOAM VIP GUI:**
Restart DSR Application on recovered C-Level Servers.

Navigate to Main Menu->Status & Manage->Server

- Status & Manage
  - Network Elements
  - Server
  - HA
  - Database
  - KPIs
  - Processes

Select the recovered C-Level servers and click on **Restart**.

**51. NOAM VIP GUI:**
Start replication on all C-Level Servers (DSR Only)

DSR Only, if SDS, Skip This Step

Un-Inhibit *(Start)* Replication to the **ALL** C-Level Servers

Navigate to **Status & Manage -> Database**

- Status & Manage
  - Network Elements
  - Server
  - HA
  - Database
  - KPIs
  - Processes

If the "Repl Status" is set to "Inhibited", click on the Allow Replication button as shown below using the following order:

- Active NOAM Server
- Standby NOAM Server
- Active SOAM Server
- Standby SOAM Server
Procedure 2: Recovery Scenario 2

- Spare SOAM Server *(if applicable)* - Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only
- Active DR NOAM Server
- Standby DR NOAM Server
- MP/IPFE Servers
- SBRS *(if SBR servers are configured, start with the active SBR, then standby, then spare)* - Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only

Verify that the replication on all the working servers is allowed. This can be done by examining the Repl Status table as seen below:

<table>
<thead>
<tr>
<th>OAM Repl Status</th>
<th>SIG Repl Status</th>
<th>Repl Status</th>
<th>Repl Audit Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NotApplicable</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
<tr>
<td>Normal</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
<tr>
<td>Normal</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
<tr>
<td>Normal</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
</tbody>
</table>

52. ACTIVE NOAM: Perform key exchange between the active-NOAM and recovered servers.

Establish an SSH session to the Active NOAM, login as *adムusr*.

Execute the following command to perform a keyexchange from the active NOAM to each recovered server:

```
$ keyexchange adムusr@<Recovered Server Hostname>
```

**Note:** If an export server is configured, perform this step.

53. ACTIVE NOAM: Activate Optional Features

Establish an SSH session to the active NOAM, login as *adムusr*.

**Note For PCA Activation:**

If you have PCA installed in the system being recovered, execute the procedure “PCA Activation on Stand By NOAM server” on recovered Standby NOAM Server and procedure “PCA Activation on Active SOAM server” on recovered Active SOAM Server from [6] to re-activate PCA.

**Note:** If not all SOAM sites are recovered at this point, then you should repeat activation for each *new* SOAM site that comes online.

**Note:** If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.

Refer to **Section 1.5 Optional Features** to activate any features that were previously activated.

**Note:** While running the activation script, the following error message (and
Procedure 2: Recovery Scenario 2

Corresponding messages) output may be seen, this can safely be ignored:

```
iload31000{S/W Fault}
```

54. **NOAM VIP GUI:**

Fetch and Store the database Report for the Newly Restored Data and Save it

Navigate to **Main Menu -> Status & Manage -> Database**

The following screen is displayed:

**Main Menu: Status & Manage -> Database [Report]**

```
dsr Database Status Report
-------------------------------------------------------------
From: Active Network CARP on host ZombieNOAM1
Report Version: 5.0.0.0.0-50.9.0
User: guisain

General
-------
Hostname : ZombieNOAM1
Database Birthday : 2016-07-11 11:21:50 EDT
AppWorks Database Version : 6.0
Application Database Version :
Capacities and Utilization
----------------------------
Disk Utilization 9.4%: 588M used of 7.0G total, 6.0G available
Memory Utilization 0.0%: used of total, 0M available
```

Click on **Save** and save the report to your local machine.

55. **ACTIVE NOAM:**

Verify Replication Between Servers.

Login to the Active NOAM via SSH terminal as **admusr**.

Execute the following command:

```
$ sudo irepstat -m
```

Output like below shall be generated:
Procedure 2: Recovery Scenario 2

-- Policy 0 ActStb [DbReplication] --
---------
Oahu-DAMP-1 -- Active
  BC From Oahu-SOAM-2 Active 0 0.50 0.15%cpu 25B/s A-me
  CC To Oahu-DAMP-2 Active 0 0.10 0.14%cpu 25B/s A-me
Oahu-DAMP-2 -- Stby
  BC From Oahu-SOAM-2 Active 0 0.50 0.11%cpu 31B/s A=C3642.212
  CC From Oahu-DAMP-1 Active 0 0.10 0.14 1.16%cpu 31B/s A=C3642.212
Oahu-IPFE-1 -- Active
  BC From Oahu-SOAM-2 Active 0 0.50 0.03%cpu 24B/s A=C3642.212
Oahu-IPFE-2 -- Active
  BC From Oahu-SOAM-2 Active 0 0.50 0.03%cpu 28B/s A=C3642.212
Oahu-NOAM-1 -- Stby
  AA From Oahu-NOAM-2 Active 0 0.25 0.03%cpu 23B/s
Oahu-NOAM-2 -- Active
  AA To Oahu-NOAM-1 Active 0 0.25 1%R 0.04%cpu 61B/s
  AB To Oahu-SOAM-2 Active 0 0.50 1%R 0.05%cpu 75B/s
Oahu-SOAM-1 -- Stby
  BB From Oahu-SOAM-2 Active 0 0.50 0.03%cpu 27B/s
Oahu-SOAM-2 -- Active
  AB From Oahu-NOAM-2 Active 0 0.50 0.03%cpu 24B/s
  BB To Oahu-SOAM-1 Active 0 0.50 1%R 0.04%cpu 32B/s
  BC To Oahu-IPFE-1 Active 0 0.50 1%R 0.04%cpu 21B/s
  BC To Oahu-SS7MP-2 Active 0 0.50 1%R 0.04%cpu 21B/s
irepstat ( 40 lines) (h)elp (m)erged

56. NOAM VIP GUI: Verify the Database states

Click on Main Menu->Status and Manager->Database

Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below:
Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Network Element</th>
<th>Server</th>
<th>Role</th>
<th>OAM Max HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieDRNOAM</td>
<td>ZombieDRNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM2</td>
<td>Network OAM&amp;P</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM2</td>
<td>System OAM</td>
<td>NA</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM1</td>
<td>System OAM</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM</td>
<td>ZombieDRNOAM2</td>
<td>Network OAM&amp;P</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieOAMP2</td>
<td>MP</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSS7MP2</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombiePFE1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombiePFE2</td>
<td>MP</td>
<td>Active</td>
</tr>
</tbody>
</table>

57. **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”.

<table>
<thead>
<tr>
<th>Hostname</th>
<th>OAM HA Role</th>
<th>Application HA Role</th>
<th>Max Allowed HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieNOAM1</td>
<td>Active</td>
<td>NA</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM2</td>
<td>Standby</td>
<td>NA</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM1</td>
<td>Active</td>
<td>NA</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM2</td>
<td>Standby</td>
<td>NA</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM1</td>
<td>Active</td>
<td>NA</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM2</td>
<td>Standby</td>
<td>NA</td>
<td>Standby</td>
</tr>
</tbody>
</table>

58. **SOAM GUI:**
Enable Provisioning

Click on **Main Menu->Status & Manage->Database**
## Procedure 2: Recovery Scenario 2

### Enable Provisioning

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

![Enable Provisioning Button](image)

A confirmation window will appear, press **OK** to enable Provisioning.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>59.</td>
<td><strong>SOAM VIP GUI:</strong> Verify the Local Node Info (DSR Only)</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;Diameter-&gt;Configuration-&gt;Local Node</strong></td>
</tr>
<tr>
<td></td>
<td>Verify that all the local nodes are shown.</td>
</tr>
<tr>
<td>60.</td>
<td><strong>SOAM VIP GUI:</strong> Verify the Peer Node Info (DSR Only)</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;Diameter-&gt;Configuration-&gt;Peer Node</strong></td>
</tr>
</tbody>
</table>
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 61.  | **SOAM VIP GUI:** Verify the Connections Info (DSR Only)  
      *Navigate to Main Menu->Diameter->Configuration->Connections*  
      Verify that all the peer nodes are shown. |
|      | **MP Servers:** Disable SCTP Auth Flag (DSR Only)  
      *For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [8]*  
      Execute this procedure on all Failed MP Servers. |
|      | **SOAM VIP GUI:** Enable Connections if needed (DSR Only)  
      *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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>64.</strong></td>
<td><strong>SOAM VIP GUI:</strong> Enable Optional Features (DSR Only)</td>
</tr>
<tr>
<td></td>
<td>DSR Only, SDS Skip This Step</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu -&gt; Diameter -&gt; Maintenance -&gt; Applications</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image.png" alt="Application Menu" /></td>
</tr>
<tr>
<td></td>
<td>Select the optional feature application configured in step 72 Click the <strong>Enable</strong> button.</td>
</tr>
<tr>
<td><strong>65.</strong></td>
<td><strong>SOAM VIP GUI:</strong> Re-enable Transports if Needed (DSR Only)</td>
</tr>
<tr>
<td></td>
<td>DSR Only, SDS Skip This Step</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;Transport Manager -&gt; Maintenance -&gt; Transport</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image.png" alt="Transport Menu" /></td>
</tr>
<tr>
<td></td>
<td>Select each transport and click on the <strong>Enable</strong> button</td>
</tr>
<tr>
<td><strong>66.</strong></td>
<td><strong>SOAM VIP GUI:</strong> Re-enable MAPIWF application if needed (DSR Only)</td>
</tr>
<tr>
<td></td>
<td>DSR Only, SDS Skip This Step</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;SS7/Sigtran-&gt;Maintenance-&gt;Local SCCP Users</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image.png" alt="SS7/Sigtran Menu" /></td>
</tr>
<tr>
<td></td>
<td>Click on the <strong>Enable</strong> button corresponding to MAPIWF Application Name.</td>
</tr>
</tbody>
</table>
### Procedure 2: Recovery Scenario 2

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verify that the SSN Status is Enabled.</strong></td>
<td></td>
</tr>
</tbody>
</table>

67. **SOAM VIP GUI:** Re-enable links if needed (DSR Only)

- Navigate to **Main Menu->SS7/Sigtran->Maintenance->Links**
  - **SS7/Sigtran**
  - **Configuration**
  - **Maintenance**
  - **Local SCCP Users**
  - **Remote Signaling Points**
  - **Remote MTP3 Users**
  - **Linksets**
  - **Links**

  Click on **Enable** button for each link.

- **DSR Only, SDS Skip This Step**

68. **SOAM VIP GUI:** Examine All Alarms

- Navigate to **Main Menu->Alarms & Events->View Active**
  - **Alarms & Events**
    - **View Active**
    - **View History**
    - **View Trap Log**

  Examine all active alarms and refer to the on-line help on how to address them.
  
  If needed contact **Appendix M. My Oracle Support (MOS).**

69. **NOAM VIP GUI:** Examine All Alarms

- Login to the NOAM VIP if not already logged in.

- Navigate to **Main Menu->Alarms & Events->View Active**

  - **Alarms & Events**
    - **View Active**
    - **View History**
    - **View Trap Log**

  Examine all active alarms and refer to the on-line help on how to address them.

  If needed contact **Appendix M. My Oracle Support (MOS).**
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 70. | **NOAM VIP:** Verify all servers in Topology are accessible (RADIUS Only)  

If the RADIUS key has never been revoked, skip this step (if RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)

Establish an SSH session to the NOAM VIP. Login as `admusr`.

Execute following commands to check if all the servers in the Topology are accessible:

```
$ cd /usr/TKLC/dpi/bin/
$ ./sharedKrevo -checkAccess
```

Example Output:

```
sharedKrevo binary: sharedKrevo -checkAccess:
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
ifconfig: No such file or directory
```

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 71. | **NOAM VIP:** Copy key file to all the servers in Topology (RADIUS Only)  

If the RADIUS key has never been revoked, skip this step (if RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)

Execute following commands to check if existing Key file on Active NOAM (The NOAM which is intact and was not recovered) server is valid:

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

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

Execute following command to copy the key file to all the servers in the Topology:

```
$ ./sharedKrevo -synchronize
```
## Procedure 2: Recovery Scenario 2

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> If any errors are present, stop and contact Appendix M. My Oracle Support (MOS)</td>
<td></td>
</tr>
<tr>
<td><strong>72.</strong></td>
<td><strong>Backup and Archive All the Databases from the Recovered System</strong></td>
</tr>
<tr>
<td></td>
<td>Execute <strong>Appendix A.</strong> Database Backup to back up the Configuration databases:</td>
</tr>
<tr>
<td><strong>73.</strong></td>
<td><strong>Recover IDIH (If Configured)</strong></td>
</tr>
<tr>
<td></td>
<td>If any components of IDIH were affected, refer to <strong>Section 7.0</strong> to perform the disaster recovery on IDIH.</td>
</tr>
</tbody>
</table>
5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact)

For a partial server outage with an SOAM server intact and available; NOAM servers are recovered using recovery procedures of base hardware and software and then executing a database restore to the active NOAM server using a NOAM database backup file obtained from external backup sources such as customer servers or NetBackup. All other servers are recovered using recovery procedures of base hardware and software. Database replication from the active NOAM/active SOAM server will recover the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures’ detailed steps are in Procedure 3. The major activities are summarized as follows:

Recover Active NOAM server by recovering base hardware, software and the database.

- Recover the base hardware.
- Recover the software.
- Recover the database

Recover NOAM servers by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.

Recover Query Server (if needed) by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.

Recover any failed SOAM and MP/DP servers by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.
- Database is already intact at one SOAM server and does not require restoration at the other SOAM and MP/DP servers.

Recover IDIH if necessary
## Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step #</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Workarounds</td>
</tr>
<tr>
<td>2.</td>
<td>Gather Required Materials</td>
</tr>
<tr>
<td>3.</td>
<td>Replace Failed Equipment</td>
</tr>
</tbody>
</table>
| 4.     | Recover PMAC TVOE Host (If Required): Configure BIOS Settings and Update Firmware | 1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:
   - HP DL380 Gen8: “Configure HP Gen 8 Server BIOS Settings”
   2. Verify and/or upgrade server firmware by executing procedure “Upgrade Rack Mount Server Firmware” from reference [8] |
| 5.     | Recover PMAC and PMAC TVOE Host: Backup Available | This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step.
   1. Restore the TVOE backup by executing Appendix G. Restore TVOE Configuration from Backup Media on ALL failed rack mount servers
   2. Restore the PMAC backup by executing Appendix H. Restore PMAC from Backup |

Proceed to Step 7
## Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td><strong>Recover PMAC and PMAC TVOE Host:</strong> Backup Not Available</td>
<td>This step assumes that TVOE and PMAC backups are <strong>NOT</strong> available, if the TVOE and PMAC have already been restored, <strong>skip this step</strong>&lt;br&gt;1. Execute procedure “Install and Configure TVOE on First RMS (PMAC Host)” from reference [8]&lt;br&gt;2. Execute section “Install PMAC” from reference [8]&lt;br&gt;3. Execute section “Initialize the PMAC Application” from reference [8]&lt;br&gt;&lt;br&gt;<strong>Proceed to Next Step</strong></td>
</tr>
<tr>
<td>7.</td>
<td><strong>Recover Failed Cisco 4948 Aggregation Switches</strong> (HP DL380 Only)</td>
<td><strong>Oracle X5-2/Netra X5-2/X6-2/HP DL380 GEN 9 SKIP THIS STEP</strong>&lt;br&gt;Recover failed Cisco 4948 aggregation switches, if needed:&lt;br&gt; Backup configuration files available: Refer to Appendix B. Recovering/Replacing Failed Cisco 4948 Aggregation Switches to recover failed Cisco 4948 aggregation switches&lt;br&gt;Backup configuration files <strong>NOT</strong> available: Execute section “Configure Cisco 4948E-F Aggregation Switches (HP DL 380 Gen 8 Only)” from reference [8]</td>
</tr>
<tr>
<td>8.</td>
<td><strong>Configure PMAC</strong> (No Backup)</td>
<td>If PMAC backup was <strong>NOT</strong> restored in step 5, execute this step. Otherwise <strong>Skip this Step</strong>.&lt;br&gt;Execute sections “Configure PMAC Server (NetBackup Only)” and “Add RMS to the PMAC Inventory” from reference [8]</td>
</tr>
<tr>
<td>9</td>
<td><strong>Install/Configure Additional Rack Mount Servers</strong> (Backups available)</td>
<td>This step assumes that TVOE backups are available, if backups are <strong>NOT</strong> available, <strong>skip this step</strong>.&lt;br&gt;1. Execute procedure “Install TVOE on Additional Rack Mount Servers” from reference [8]&lt;br&gt;2. Restore the TVOE backup by executing Appendix E. Restore TVOE Configuration from Backup Media on <strong>ALL</strong> failed rack mount servers</td>
</tr>
<tr>
<td>10</td>
<td><strong>Install/Configure Additional Rack Mount Servers</strong> (Backups <strong>NOT</strong> available)</td>
<td>This step assumes that TVOE backups are <strong>NOT</strong> available, if backups are available, execute the previous step.&lt;br&gt;1. Execute procedure “Install TVOE on Additional Rack Mount Servers” from reference [8]&lt;br&gt;2. Execute “Configure TVOE on Additional Rack Mount Servers” from reference [8]</td>
</tr>
</tbody>
</table>
**Procedure 3: Recovery Scenario 3**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Description</th>
</tr>
</thead>
</table>
| 11   | **Configure BIOS Settings and Update Firmware on Additional Rack Mount Servers** | 1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:  
   - HP DL380 Gen8: “Configure HP Gen 8 Server BIOS Settings”  
   2. Verify and/or upgrade server firmware by executing procedure “Upgrade Rack Mount Server Firmware” from reference [8] |
| 12   | **Determine VM Placement and Socket Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen9 Only)** | HP DL380 GEN 8 SKIP THIS STEP  
Determine the VM placement and Pinning for proper VM placement and pinning. Refer 12 for workbook reference |
| 13   | **Deploy Redundant PMAC (if required)** | Refer to procedure “Deploy Redundant PMAC (Optional)” to re-deploy and configure any redundant PMACs previously configured. |
| 14   | **PMAC: Determine if an fdconfig file exists from the initial deployment.** | Determine whether the fdconfig backup file exists:  

```
[admusr@melbourne-pmac-1 ~]$ ll /usr/TKLC/smac/etc/fdc/
```

Examine the results and verify whether the rms config file <hostname>.cfg exists  
Note: There may be multiple fdconfig backup files here with respect to each RMS. Select the respective one according to the RMS. |
| 15   | **If fdc backup file does NOT exist** | Execute this step ONLY If the fdconfig backup file does NOT exist:  
If the fdconfig file does NOT exist: Create the needed file(s) by executing section “Virtual Machine/Network Fast Deployment” from reference [8]  
**WARNING:**  
It is very important to ensure the file(s) created only affect the TVOE server(s) and its Guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.  
Skip to step 24 if this step was executed |
Procedure 3: Recovery Scenario 3

| Step | PMAC [If fdconfig backup file exists]: Load ISOs into PMAC if not done already | Execute this step ONLY If the fdconfig backup file exists and located at step 14:  
If the DSR, SDS, and TPD ISOs are NOT loaded in to the PMAC: Execute procedures 14 of section “Virtual Machine/Network Fast Deployment” from reference [8]  
If already loaded into PMAC, skip this step. |
Procedure 3: Recovery Scenario 3

17

PMAC
[If fdc backup file exists ]:
Edit/Update Configuration File

Execute this step ONLY If the fdconfig backup file exists and located at step 14:

Edit the fdconfig file to include only the required/failed servers.

Note: Comment out configuration items that are not needed.

Note: It is recommended that a separate configuration file be created for EACH rack mount server being deployed.

Note: Cabinet ID in the config file needs to match the cabinet already defined in PM&C

The following items are mandatory:

- siteName
- tpdIso
- dsrIso (if DSR VMs are being configured)
- sdlso (if SDS VMs are being configured)
- NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured)
- XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured)
- XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured)
- DSRNOAM1XMIIIPADDRESS (if DSRNOAM1 is being configured)
- DSRNOAM2XMIIIPADDRESS (if DSRNOAM2 is being configured)
- DSRDRNOAM1XMIIIPADDRESS (if DSRDRNOAM1 is being configured)
- DSRDRNOAM2XMIIIPADDRESS (if DSRDRNOAM2 is being configured)
- SDSNOAM1XMIIIPADDRESS (if SDSNOAM1 is being configured)
- SDSNOAM2XMIIIPADDRESS (if SDSNOAM2 is being configured)
- SDSDRNOAM1XMIIIPADDRESS (if SDSDRNOAM1 is being configured)
- SDSDRNOAM2XMIIIPADDRESS (if SDSDRNOAM2 is being configured)

Note: Refer to Appendix R: VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8]

Note: Comment out SDS and DSR profile items if corresponding products are not used.

Note: [Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9]: Refer to Appendix Q.3: Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8]

Note: The VM names should not be modified in the .cfg file. The names are fixed and will be prefixed in the siteName.

Note: The VM locations should not be changed from their ‘RMSx’ format. Each RMS should correspond with a separate Rack Mount Server.

WARNING:

It is very important to ensure the file(s) created only affect the TVOE server(s) and its Guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC [If fdc backup file exists]:</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>Copy the located backed up fdc file to the RMS directory</td>
</tr>
</tbody>
</table>

**Execute this step ONLY If the fdconfig backup file exists and located at step 14:**

Copy the located fdconfig backup file to the RMS directory:

```
$ cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file> /usr/TKLC/smac/etc/RMS/
```
### Procedure 3: Recovery Scenario 3

| 19 | PMAC [If fdc backup file exists]: Execute the config.sh script |

Execute this step ONLY if the fdconfig backup file exists and located at step 14:

Execute config.sh against the modified back up config file defined above:

**Note:** If the below command is executed on multiple cfg files, it will overwrite the existing xml file. It is recommended to rename the xml file before running the below command again.

```
$ sudo ./config.sh <config file>
```

Sample Output:

```
Validating cfg file...
Successful validation of cfg file.
Added Cabinet 101 to Fast Deployment File.
Added Zombie TVOE1 to Fast Deployment File.
Added Zombie TVOE2 to Fast Deployment File.
Added xml1(bond0.4) to Fast Deployment File.
Added im1(bond0.3) to Fast Deployment File.
Added reg(bond1.16) to Fast Deployment File.
Added xsi1(bond1.6) to Fast Deployment File.
Added xsi2(bond1.7) to Fast Deployment File.
Added xsi3(bond1.8) to Fast Deployment File.
Added xsi4(bond1.9) to Fast Deployment File.
Added xsi5(bond1.11) to Fast Deployment File.
Added xsi6(bond1.12) to Fast Deployment File.
Added xsi7(bond1.13) to Fast Deployment File.
Added xsi8(bond1.14) to Fast Deployment File.
Added xsi9(bond1.15) to Fast Deployment File.
Added xsi10(bond1.16) to Fast Deployment File.
Added xsi11(bond1.17) to Fast Deployment File.
Added xsi12(bond1.18) to Fast Deployment File.
Added xsi13(bond1.19) to Fast Deployment File.
Added xsi14(bond1.20) to Fast Deployment File.
Added xsi15(bond1.21) to Fast Deployment File.
Added xsi16(bond1.22) to Fast Deployment File.
Added Zombie DSRRNOAM1 to Fast Deployment File.
Added Zombie DSRRNOAM2 to Fast Deployment File.
Added Zombie DSRRNNAME to Fast Deployment File.
Added Zombie_1SRRNOAM1 to Fast Deployment File.
Added Zombie_1SRRNOAM2 to Fast Deployment File.
Added Zombie_SUITEAM1 to Fast Deployment File.
Added Zombie_SUITEAM2 to Fast Deployment File.

Validating Fast Deployment File......
Configuration file validation successful.
```

```
SUCCESS: OPERATION SUCCESS!!
```
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>20</th>
<th><strong>PMAC</strong>&lt;br&gt; [If fdc backup file exists]: Execute Fast Deployment</th>
</tr>
</thead>
</table>
|    | **Execute this step ONLY If the fdconfig backup file exists and located at step 14:**<br>With the file generated from the config.sh script, execute the following command to start fast deployment:<br><br>$ screen<br>$ sudo fdconfig config --file=<fd_config.xml><br><br**Note:** This is a long duration command. If the screen command was run prior to executing the fdconfig, perform a “screen -dr” to resume the screen session in the event of a terminal timeout etc.
**Procedure 3: Recovery Scenario 3**

**PMAC GUI**
- If fdc backup file exists:
  - Monitor the configuration

**Execute this step ONLY If the fdconfig backup file exists and located at step 14:**

If not already done so, establish a GUI session on the PMAC server.

Navigate to **Main Menu -> Task Monitoring**

![Main Menu - Task Monitoring](image)

Monitor the configuration to completion:

- **Note:** Should a failure occur with fdconfig, logs can be accessed in /var/TKLC/log/fdconfig/fdconfig.log

```
[admusr@melbourne-pmac-1 fdconfig]$ sudo fdconfig dumpsteps --file=deploy_melbourne_20170329T202458_701b.fdcdb
Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb"
Here are the steps that were generated

------------ begin ------------

Dump of DB steps:
NUM PHS DLY INFRA ID SVRTYPE CMD ELEMENT PRE STATE TO BGTS COMMAND TEXT
--- --- --- --- --- ---------- ----------- ---------------------------
--- --- --- --- --- ---------- ----------- ---------------------------
1 1 0 pmac Fast_Deployment 0 21 0 Complete 300 0 Check PM&C is available
2 1 0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet
3 1 0 pmac Fast_Deployment 0 3 melbourne_RMS3 1 Skipped 900 0 Add Rms
4 2 0 pmac Fast_Deployment 1

Run Below command to restart the fdconfig after a failure has occurred and has been resolved:

```
$ sudo fdconfig restart --file=deploy_melbourne_20170329T202458_701b.fdcdb
```
Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Execute this step ONLY If the fdconfig backup file exists and located at step 14:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Repeat steps 14-21 for each rack mount server configuration file located at step 14, if required.</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Execute this step ONLY If the fdconfig backup file exists and located at step 14:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Copy the updated fdc file to the fdc backup directory:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$ sudo cp /usr/TKLC/smac/etc/RMS/&lt;fdc_file&gt;/usr/TKLC/smac/etc/fdc/</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change permissions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/&lt;fdc_file&gt;</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Perform CPU Pinning</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure VM CPU socket pinning on each TVOE host to optimize performance by executing procedure “CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen9 Only)” from reference [8]</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Obtain Latest Database Backup and Network Configuration Data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Obtain most recent “RADIUS shared secret encryption key” file DpiKf.bin.encr from external backup sources (Only when the RADIUS Key Revocation MOP has been executed on the system)</td>
<td></td>
</tr>
</tbody>
</table>

From required materials list in Section 3.1 Required Materials: use site survey documents and Network Element report (if available), to determine network configuration data.
<table>
<thead>
<tr>
<th></th>
<th>Procedure 3: Recovery Scenario 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td><strong>Execute DSR Installation Procedure for the First NOAM</strong>&lt;br&gt;Verify the networking data for Network Elements&lt;br&gt;Note: Use the backup copy of network configuration data and site surveys (Step 2)&lt;br&gt;Note: SDS disaster recovery actions can and should be worked simultaneously, doing so would allow faster recovery of the complete solution (i.e. stale DB on DP servers will not receive updates until SDS-SOAM servers are recovered. The following steps will be written to accommodate both DSR and SDS disaster recovery steps.&lt;br&gt;<strong>IMPORTANT:</strong> While creating the first NOAMs in this step, it is important that the server hostname is the same as one of the NOAM hostnames used prior to the disaster.&lt;br&gt;&lt;br&gt;<strong>DSR:</strong>&lt;br&gt;1. Configure the first NOAM server by executing procedure “Configure First NOAM NE and Server” from reference [8]&lt;br&gt;2. Configure the NOAM server group by executing procedure “Configure the NOAM Server Group” from reference [8]&lt;br&gt;&lt;br&gt;<strong>SDS:</strong>&lt;br&gt;1. Configure the first SDS NOAM server by executing procedure “Configure First SDS NOAM NE and Server” from reference [8]&lt;br&gt;2. Configure the SDS NOAM server group by executing procedure “Configure the SDS NOAM Server Group” from reference [8]</td>
</tr>
</tbody>
</table>
Procedure 3: Recovery Scenario 3

27

NOAM GUI:
Login

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

Oracle System Login

Log In
Enter your username and password to log in
Username: |
Password: |

Welcome to the Oracle System Login.
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.
Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.
Procedure 3: Recovery Scenario 3

**NOAM GUI:**
Upload the Backed up Database File

**DSR Only, if SDS, Skip to Step 32**

Browse to Main Menu->Status & Manage->Files

Select the Active NOAM server. The following screen will appear:

1. Click on **Browse** and locate the backup file
2. Check **This is a backup file** box
3. Click on **Open** as shown below.

Click on **Upload** as shown below and select the file “NO Provisioning and Configuration:” file backed up after initial installation and provisioning.

Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.
Procedure 3: Recovery Scenario 3

29

**NOAM GUI:**
Disable Provisioning

**DSR Only, if SDS, Skip to Step 32**

Click on **Main Menu->Status & Manage->Database**

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

![Disable Provisioning Button](image)

A confirmation window will appear, press **OK** to disable Provisioning.
Procedure 3: Recovery Scenario 3

30

**NOAM GUI:**
Verify the Archive Contents and Database Compatibility

**DSR Only, if SDS, Skip to Step 32**

Select the *Active NOAM* server and click on the **Compare**.

The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 28** of this procedure.

Verify that the output window matches the screen below.

**Note:** You will get a database mismatch regarding the Topology Compatibility and possibly User compatibility (due to authentication) These warnings are expected. If these are the only mismatches, proceed, otherwise stop and contact Appendix M. My Oracle Support (MOS) and ask for assistance.

**Note:** Archive Contents and Database Compatibilities must be the following:

**Archive Contents:** Configuration data

**Database Compatibility:** The databases are compatible.

**Note:** The following is expected Output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one NOAM:

**Topology Compatibility**
THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.

**Note:** We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility.

If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.
Procedure 3: Recovery Scenario 3

**ACTIVE NOAM:**

- Restore the Database

**DSR Only, If SDS, Skip to Step 32**

From **Main Menu->Status & Manage->Database**

Select the **Active NOAM** server, and click on **Restore** as shown below.

![Select archive to Restore on server: Zombie]

Archive * backup/Backup.dsr.ZombieNO

[Ok | Cancel]

The following screen will be displayed. Select the proper back up provisioning and configuration file.

![Database Restore Confirm]

Incompatible archive selected

The selected database came from ZombieNO

Archive Contents
Configuration data

Database Compatibility
The databases are compatible.

Force Restore? [✓ Force | Force restore]

[Ok | Cancel]

**Note:** After the restore has started, the user will be logged out of XMI NO GUI since the restored Topology is old data.
<table>
<thead>
<tr>
<th>Step</th>
<th>SDS NOAM:</th>
<th>SDS Only, if DSR, Skip this step</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>Transfer SDS Configuration and Provisioning backup Database Files</td>
<td>Using the IP of the recovered SDS NOAM, transfer the uncompressed backup database files to the <code>/var/TKLC/db/filemgmt</code> directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Linux:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. From the command line of a Linux machine use the following command to copy the configuration backup file to the SDS NOAM guest:</td>
</tr>
<tr>
<td></td>
<td></td>
<td># scp &lt;path_to_configuration_db_file&gt; admusr@&lt;SDS_NOAM_IP&gt;/var/TKLC/db/filemgmt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. From the command line of a Linux machine use the following command to copy the provisioning backup file to the SDS NOAM guest:</td>
</tr>
<tr>
<td></td>
<td></td>
<td># scp &lt;path_to_provisioning_db_file&gt; admusr@&lt;SDS_NOAM_IP&gt;/var/TKLC/db/filemgmt</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> where <code>&lt;path_to_db_file&gt;</code> is the path to the backup database file on the local system and <code>&lt;SDS_NOAM_IP&gt;</code> is the recovered SDS NOAM IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Windows:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use WinSCP to copy the backup database files into the <code>/var/TKLC/db/filemgmt</code> directory. Please refer to [9] procedure Using WinSCP to copy the backup image to the customer system.</td>
</tr>
<tr>
<td>33</td>
<td>Login</td>
<td>SDS Only, if DSR, Skip this step</td>
</tr>
<tr>
<td></td>
<td>Establish an SSH session to the SDS active NOAM XMI IP address, login as <code>admusr</code>.</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>Stop running applications</td>
<td>SDS Only, if DSR, Skip this step</td>
</tr>
<tr>
<td></td>
<td>Issue the following command to stop running applications. Leave database running:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$ sudo prod.stop --ignore-cap</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This step may take several minutes to complete.</td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Command</th>
</tr>
</thead>
</table>
| 35   | SDS NOAM: Stop running applications | Restore the configuration DB by executing the following command:  

```bash
$ sudo idb.restore -n -t /var/TKLC/db/filemgmt -v  
<full path to configuration archive file name>
```

| 36   | SDS NOAM: Stop running applications | Restore the configuration DB by executing the following command:  

```bash
$ sudo idb.restore -n -t /var/TKLC/db/filemgmt -v  
<full path to provisioning archive file name>
```

| 37   | SDS NOAM: Stop running applications | Start the SDS application by executing the following command:  

```bash
$ sudo prod.start
```
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td><strong>NOAM VIP GUI:</strong> 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: &lt;br&gt;&lt;br&gt;<strong>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</strong> &lt;br&gt;&lt;br&gt;Login as the <em>guiadmin</em> user:</td>
</tr>
<tr>
<td>39</td>
<td><strong>NOAM VIP GUI:</strong> Wait for 5-10 minutes for the System to stabilize with the new topology: &lt;br&gt;&lt;br&gt;Monitor the Info tab for <strong>&quot;Success&quot;</strong>. This will indicate that the restore is complete and the system is stabilized. &lt;br&gt;&lt;br&gt;Following alarms <strong>must</strong> be ignored for NOAM and MP/DP Servers until all the Servers are configured: &lt;br&gt;&lt;br&gt;Alarms with Type Column as <strong>“REPL”</strong>, <strong>“COLL”</strong>, <strong>“HA”</strong> (with mate NOAM), <strong>“DB”</strong> (about Provisioning Manually Disabled) &lt;br&gt;&lt;br<strong>Note:</strong> Do not pay attention to alarms until all the servers in the system are completely restored. &lt;br&gt;&lt;br<strong>Note:</strong> The Configuration and Maintenance information will be in the same state it was backed up during initial backup.</td>
</tr>
</tbody>
</table>
**Procedure 3: Recovery Scenario 3**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td><strong>Active NOAM:</strong> Set Failed Servers to OOS</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu -&gt; Status &amp; Manage -&gt; HA</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Main Menu Screenshot" /></td>
</tr>
<tr>
<td></td>
<td>Select <strong>Edit</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Modifying HA attributes</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Edit Screen" /></td>
</tr>
<tr>
<td></td>
<td>Set the Max Allowed HA Role drop down box to <strong>OOS</strong> for the failed servers.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Ok</strong></td>
</tr>
<tr>
<td>41</td>
<td><strong>NOAM VIP GUI:</strong> Recover Standby NOAM</td>
</tr>
<tr>
<td></td>
<td>Install the second NOAM server:</td>
</tr>
<tr>
<td></td>
<td><strong>DSR:</strong></td>
</tr>
<tr>
<td></td>
<td>Execute procedure “Configure the Second NOAM Server”, steps 1, 3-6 from reference [8]</td>
</tr>
<tr>
<td></td>
<td><strong>SDS:</strong></td>
</tr>
<tr>
<td></td>
<td>Execute procedure “Configure the Second SDS NOAM Server”, steps 1, 3-6 from reference [8]</td>
</tr>
<tr>
<td>42</td>
<td><strong>Install NetBackup Client (Optional)</strong></td>
</tr>
<tr>
<td></td>
<td>If NetBackup is used execute procedure “Install NetBackup Client (Optional)” from reference [8]</td>
</tr>
</tbody>
</table>
Procedure 3: Recovery Scenario 3

43

**NOAM VIP GUI:**
Set HA on Standby NOAM

Navigate to **Status & Manage -> HA**

- [Diagram]
  - Status & Manage
    - Network Elements
    - Server
    - HA
    - Database
    - KPIs
    - Processes
    - Tasks
    - Files

Click on **Edit** at the bottom of the screen

Select the standby NOAM server, set it to **Active**

[Diagram]

Press **OK**

44

**NOAM VIP GUI:**
Restart DSR application

Navigate to **Main Menu->Status & Manage->Server.**

[Diagram]

Select the recovered standby NOAM server and click on **Restart**.
<table>
<thead>
<tr>
<th>Active NOAM: Correct the RecognizedAuthority table</th>
<th>Establish an SSH session to the active NOAM, login as <strong>admusr</strong>. Execute the following command:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>$ sudo top.setPrimary</strong></td>
</tr>
<tr>
<td></td>
<td>- Using my cluster: A1789</td>
</tr>
<tr>
<td></td>
<td>- Updating A1789.022: &lt;DSR_NOAM_B_hostname&gt;</td>
</tr>
<tr>
<td></td>
<td>- Updating A1789.144: &lt;DSR_NOAM_A_hostname&gt;</td>
</tr>
</tbody>
</table>
### Procedure 3: Recovery Scenario 3

#### NOAM VIP GUI:
Perform Keyexchange with Remote Import Server

| 46 | SDS Only, DSR Skip This Step |

1) Navigate to **Main Menu -> SDS -> Configuration -> Options**

2) Uncheck the **Remote Import Enabled Box**:

3) Click **Apply**

**Note:** Re-navigate to **Main Menu -> SDS -> Configuration -> Options** to clear Success banner.

4) Re-Enter the **Remote Import Password**:

5) Click **Apply**

**Note:** Re-navigate to **Main Menu -> SDS -> Configuration -> Options** to clear Success banner.

6) Check the **Remote Import Enabled Box**:
**Procedure 3: Recovery Scenario 3**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 47   | **NOAM VIP GUI:** Repeat for Remote Export Server  
Repeate **Step 46** for the remote Export Server  
SDS Only, DSR Skip This Step |
| 48   | **NOAM VIP GUI:** Perform Keyexchange with Export Server  
Navigate to **Main Menu -> Administration -> Remote Servers -> Data Export**  
- Administration  
- General Options  
- Access Control  
- Software Management  
- Remote Servers  
  - LDAP Authentication  
  - SNMP Trapping  
  - Data Export  
  - DNS Configuration  
Click on **SSH Key Exchange** at the bottom of the screen  
Enter the Password and press **OK** |
| 49   | **NOAM VIP GUI:** Recover Query Servers  
SDS Only, DSR Skip This Step  
Execute procedure “Configuring SDS Query Servers”, steps 1, 4-7 from reference [8] |
## Procedure 3: Recovery Scenario 3

### 50
**SDS NOAM VIP GUI:** Set HA on Query Server

**SDS Only, DSR Skip This Step**

Navigate to **Status & Manage -> HA**

- **Status & Manage**
  - Network Elements
  - Server
  - HA
  - Database
  - KPIs
  - Processes
  - Tasks
  - Files

Click on **Edit** at the bottom of the screen

Select the Query server, set it to **Observer**

Press **OK**

### 51
**SDS NOAM VIP GUI:** Restart SDS application

**SDS Only, DSR Skip This Step**

Navigate to **Main Menu->Status & Manage->Server**

- **Status & Manage**
  - Network Elements
  - Server
  - HA
  - Database
  - KPIs
  - Processes

Select the recovered Query server and click on **Restart**.
### Procedure 3: Recovery Scenario 3

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

![Status & Manage -> HA](image)
# Procedure 3: Recovery Scenario 3

## NOAM VIP GUI: Restart DSR application

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>54</td>
<td>Navigate to <strong>Main Menu-&gt;Status &amp; Manage-&gt;Server</strong>. Select the recovered standby SOAM server and click on <strong>Restart</strong>.</td>
</tr>
</tbody>
</table>

*DSR Only*

## Activate PCA Feature

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>55</td>
<td>If you have PCA installed in the system being recovered, execute the procedure &quot;PCA Activation on Active NOAM network&quot; on recovered Active NOAM Server and procedure &quot;PCA Activation on Stand By SOAM network&quot; on recovered Standby SOAM from [7] to re-activate PCA.</td>
</tr>
</tbody>
</table>

## NOAM VIP GUI: Recover the C-Level Server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 56   | Recover C-Level Servers:  

**DSR:**  
Execute procedure “Configure the MP Servers”, Steps 1, 9-13 from reference [8]  

**Note:** Execute steps 14-16 of procedure “Configure the MP Servers” from reference [8] if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.  

**SDS:**  
Execute procedure “Configure the SDS DP Servers”, Steps 1, 5-8 from reference [8]  

Repeat this step for any remaining failed MP servers.
Procedure 3: Recovery Scenario 3

NOAM VIP GUI: Set HA on all C-Level Servers

Navigate to Status & Manage -> HA

- Status & Manage
  - Network Elements
  - Server
  - HA
  - Database
  - KPIs
  - Processes

Click on Edit at the bottom of the screen

For each server whose Max Allowed HA Role is set to OOS, set it to Active

- ZombieDAMP1
  - Active

- ZombieDAMP2
  - OOS

Press OK

NOAM VIP GUI: Restart DSR Application on recovered C-Level Servers.

Navigate to Main Menu->Status & Manage->Server

- Status & Manage
  - Network Elements
  - Server
  - HA
  - Database
  - KPIs
  - Processes

Select the recovered C-Level servers and click on Restart.
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 59   | **ACTIVE NOAM:**  
Perform key exchange between the active-NOAM and recovered servers.  
Execute the following command to perform a keyexchange from the active NOAM to each recovered server:  
\[ \$ \texttt{keyexchange admusr@<Recovered Server Hostname>} \]  
**Note:** If an export server is configured, perform this step. | |
| 60   | **ACTIVE NOAM:**  
Activate Optional Features  
*DSR Only, if SDS, Skip This Step*  
Establish an SSH session to the active NOAM, login as **admusr**.  
**Note For PCA Activation:**  
If you have PCA installed in the system being recovered, execute the procedure “**PCA Activation on Active NOAM server**” on recovered Active NOAM Server and procedure “**PCA Activation on Stand By SOAM server**” on recovered Standby SOAM from [6] to re-activate PCA.  
**Note:** If not all SOAM sites are recovered at this point, then you should repeat activation for each *new* SOAM site that comes online.  
**Note:** If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.  
Refer to **Section 1.5 Optional Features** to activate any features that were previously activated.  
**Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:  
\[ \texttt{iload\#31000{S/W Fault}} \] | |
Procedure 3: Recovery Scenario 3

NOAM VIP GUI: Fetch and Store the database Report for the Newly Restored Data and Save it

Navigate to Main Menu -> Status & Manage -> Database

Select the active NOAM server and click on the Report button at the bottom of the page.

The following screen is displayed:

Main Menu: Status & Manage -> Database [Report]

Click on Save and save the report to your local machine.
Procedure 3: Recovery Scenario 3

ACTIVE NOAM:
Verify Replication Between Servers.

Login to the Active NOAM via SSH terminal as admusr.

Execute the following command:

```
$ sudo irepstat -m
```

Output like below shall be generated:

```
-- Policy 0 ActStb [DbReplication] -----------------------------------
----------
Oahu-DAMP-1 -- Active
    BC From Oahu-SOAM-2 Active 0 0.50 ^0.15%cpu 25B/s A=me
    CC To  Oahu-DAMP-2 Active 0 0.10  0.14%cpu 25B/s A=me
Oahu-DAMP-2 -- Stby
    BC From Oahu-SOAM-2 Active 0 0.50 ^0.11%cpu 31B/s A=C3642.212
    CC From Oahu-DAMP-1 Active 0 0.10  1.16%cpu 31B/s A=C3642.212
Oahu-IPFE-1 -- Active
    BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 24B/s A=C3642.212
Oahu-IPFE-2 -- Active
    BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 28B/s A=C3642.212
Oahu-NOAM-1 -- Stby
    AA From Oahu-NOAM-2 Active 0 0.25 ^0.03%cpu 23B/s
Oahu-NOAM-2 -- Active
    AA To  Oahu-NOAM-1 Active 0 0.25  1%R 0.04%cpu 61B/s
    AB To  Oahu-SOAM-2 Active 0 0.50  1%R 0.05%cpu 75B/s
Oahu-SOAM-1 -- Stby
    BB From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 27B/s
Oahu-SOAM-2 -- Active
    AB From Oahu-NOAM-2 Active 0 0.50 ^0.03%cpu 24B/s
    BB To  Oahu-SOAM-1 Active 0 0.50  1%R 0.04%cpu 32B/s
    BC To  Oahu-IPFE-1 Active 0 0.50  1%R 0.04%cpu 21B/s
    BC To  Oahu-SS7MP-2 Active 0 0.50  1%R 0.04%cpu 21B/s
irepstat ( 40 lines) (h)eip (m)erged
```
Procedure 3: Recovery Scenario 3

Verifying Database states

Click on Main Menu->Status and Manager->Database

- Status & Manage
  - Network Elements
  - Server
  - HA
  - Database
  - KPIs
  - Processes

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:

<table>
<thead>
<tr>
<th>Network Element</th>
<th>Server</th>
<th>Role</th>
<th>OAM Max HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieDRNOAM</td>
<td>ZombieDRNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM2</td>
<td>Network OAM&amp;P</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM1</td>
<td>System OAM</td>
<td>N/A</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM2</td>
<td>System OAM</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM</td>
<td>ZombieDRNOAM2</td>
<td>Network OAM&amp;P</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM2</td>
<td>MP</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSS7MP2</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSS7MP1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombiePFE1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombiePFE2</td>
<td>MP</td>
<td>Active</td>
</tr>
</tbody>
</table>
Procedure 3: Recovery Scenario 3

64

**NOAM VIP GUI:** Verify the HA Status

Click on **Main Menu->Status and Manage->HA**

![Image of HA status menu]

Select the row for all of the servers
Verify that the “HA Role” is either “Active” or “Standby”.

<table>
<thead>
<tr>
<th>Hostname</th>
<th>OAM HA Role</th>
<th>Application HA Role</th>
<th>Max Allowed HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Standby</td>
</tr>
</tbody>
</table>

65

**NOAM GUI:** Enable Provisioning

Click on **Main Menu->Status & Manage->Database**

![Image of provisioning menu]

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

![Image of enable provisioning button]

A confirmation window will appear, press OK to enable Provisioning.
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>SOAM VIP GUI: Verify the Local Node Info (DSR Only)</th>
<th>DSR Only, SDS Skip This Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>66</td>
<td>Navigate to Main Menu-&gt;Diameter-&gt;Configuration-&gt;Local Node</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verify that all the local nodes are shown.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>SOAM VIP GUI: Verify the Peer Node Info (DSR Only)</th>
<th>DSR Only, SDS Skip This Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>67</td>
<td>Navigate to Main Menu-&gt;Diameter-&gt;Configuration-&gt;Peer Node</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verify that all the peer nodes are shown.</td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 68   | **SOAM VIP GUI:** Verify the Connections Info (DSR Only) | **DSR Only, SDS Skip This Step**
|      | Navigate to **Main Menu->Diameter->Configuration->Connections** |
|      | Verify that all the connections are shown. |
| 69   | **MP Servers:** Disable SCTP Auth Flag (DSR Only) | **DSR Only, SDS Skip This Step**
|      | For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [12] |
|      | Execute this procedure on all Failed MP Servers. |
| 70   | **SOAM VIP GUI:** Enable Connections if needed (DSR Only) | **DSR Only, SDS Skip This Step**
|      | Navigate to **Main Menu->Diameter->Maintenance->Connections** |
|      | Select each connection and click on the **Enable** button. Alternatively you can enable all the connections by selecting the **EnableAll** button. |
|      | Verify that the Operational State is Available. |
|      | **Note:** If a Disaster Recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution |
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>71</td>
<td><strong>SOAM VIP GUI:</strong> Enable Optional Features (DSR Only)</td>
</tr>
<tr>
<td></td>
<td><strong>DSR Only, SDS Skip This Step</strong></td>
</tr>
<tr>
<td></td>
<td>Navigate to <code>Main Menu -&gt; Diameter -&gt; Maintenance -&gt; Applications</code></td>
</tr>
<tr>
<td></td>
<td>- Maintenance</td>
</tr>
<tr>
<td></td>
<td>- Route Lists</td>
</tr>
<tr>
<td></td>
<td>- Route Groups</td>
</tr>
<tr>
<td></td>
<td>- Peer Nodes</td>
</tr>
<tr>
<td></td>
<td>- Connections</td>
</tr>
<tr>
<td></td>
<td>- Egress Throttle Groups</td>
</tr>
<tr>
<td></td>
<td>- Applications</td>
</tr>
<tr>
<td></td>
<td>Select the optional feature application configured in <strong>step 60</strong></td>
</tr>
<tr>
<td></td>
<td>Click the <strong>Enable</strong> button.</td>
</tr>
<tr>
<td></td>
<td>![Enable, Disable, Pause Updates buttons]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>71</td>
<td><strong>SOAM VIP GUI:</strong> Re-enable Transports if Needed (DSR Only)</td>
</tr>
<tr>
<td></td>
<td><strong>DSR Only, SDS Skip This Step</strong></td>
</tr>
<tr>
<td></td>
<td>Navigate to <code>Main Menu -&gt; Transport Manager -&gt; Maintenance -&gt; Transport</code></td>
</tr>
<tr>
<td></td>
<td>![Transport Manager, Configuration, Maintenance, Transport buttons]</td>
</tr>
<tr>
<td></td>
<td>Select each transport and click on the <strong>Enable</strong> button</td>
</tr>
<tr>
<td></td>
<td>![Enable, Disable, Block buttons]</td>
</tr>
<tr>
<td></td>
<td>Verify that the Operational Status for each transport is Up.</td>
</tr>
</tbody>
</table>
Procedure 3: Recovery Scenario 3

73

SOAM VIP GUI:
Re-enable MAPIWF application if needed (DSR Only)

DSR Only, SDS Skip This Step

Navigate to Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users

- SS7/Sigtran
  - Configuration
  - Maintenance
    - Local SCCP Users
    - Remote Signaling Points
    - Remote MTP3 Users
    - Linksets
    - Links

Click on the Enable button corresponding to MAPIWF Application Name.

Enable  Disable

Verify that the SSN Status is Enabled.

74

SOAM VIP GUI:
Re-enable links if needed (DSR Only)

DSR Only, SDS Skip This Step

Navigate to Main Menu->SS7/Sigtran->Maintenance->Links

- SS7/Sigtran
  - Configuration
  - Maintenance
    - Local SCCP Users
    - Remote Signaling Points
    - Remote MTP3 Users
    - Linksets
    - Links

Click on Enable button for each link.

Enable  Disable

Verify that the Operational Status for each link is Up.
Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>75</th>
<th>NOAM VIP: Verify all servers in Topology are accessible (RADIUS Only)</th>
</tr>
</thead>
</table>

If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)

Establish an SSH session to the NOAM VIP. Login as `admusr`.

Execute following commands to check if all the servers in the Topology are accessible:

```
$ ./usr/TXL/dpi/bin/sharedKrevo -checkAccess
```

**Output Example:**

```
1450112012: [INFO] 'SCAM-2' is accessible.
FIPS integrity verification test failed.
The authenticity of host 'ipfe (10.240.146.16)' can't be established.
RSH key fingerprint is 8a:7f:0d:6e:86:fa:8b:0c:4b:0d:fa:72:4e:ec:82.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ipfe,10.240.146.16' (RSA) to the list of known hosts .

1450112010: [INFO] 'IPFE' is accessible.
FIPS integrity verification test failed.
The authenticity of host 'ipfe (10.240.146.24)' can't be established.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ipfe,10.240.146.24' (RSA) to the list of known hosts .

1450112017: [INFO] 'MP-2' is accessible.
FIPS integrity verification test failed.
The authenticity of host 'mp-2 (10.240.146.24)' can't be established.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mp-2,10.240.146.24' (RSA) to the list of known hosts .

1450112020: [INFO] 'MP-1' is accessible.
```

**Note:** If any of the servers are not accessible, stop and contact Appendix M. My Oracle Support (MOS)
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>76</td>
<td><strong>SOAM VIP:</strong> Copy key file to all the servers in Topology (RADIUS Only)</td>
</tr>
<tr>
<td></td>
<td>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</td>
</tr>
<tr>
<td></td>
<td>Establish an SSH session to any of the Active SOAM which remained intact and operational (Need to Login to Active SOAM server which was not recovered or did not need recovery). Login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td>Execute following commands to check if existing Key file on Active SOAM server is valid:</td>
</tr>
</tbody>
</table>
|      | ```
|      | $ cd /usr/TKLC/dpi/bin/
|      | $ ./sharedKrevo -validate
|      | ```
|      | **Expected Output:** |
|      | /usr/TKLC/dpi/ |
|      | **Note:** If output of above command shows that existing key file is not valid, contact Appendix M. My Oracle Support (MOS) |
|      | Establish an SSH session to the active SOAM, login as **admusr**. |
|      | Execute following command to copy the key file to Active NOAM: |
|      | ```
|      | $ cd /usr/TKLC/dpi/bin/
|      | $ ./sharedKrevo -copyKey -destServer <Active NOAM server name>
|      | ```
### Procedure 3: Recovery Scenario 3

#### NOAM VIP: Copy key file to all the servers in Topology (RADIUS Only)

- If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)

  Establish an SSH session to any of the Active NOAM. Login as admusr.

  Execute following command to copy the key file to all the servers in the Topology:

  ```bash
  $ ./sharedKrevo -synchronize
  $ ./sharedKrevo -updateData
  ```

#### SOAM VIP GUI: Examine All Alarms

- Navigate to Main Menu->Alarms & Events->View Active

  ![View Active]

  Examine all active alarms and refer to the on-line help on how to address them.

  If needed contact Appendix M. My Oracle Support (MOS).
## Procedure 3: Recovery Scenario 3

| 79 | **NOAM VIP GUI:** Examine All Alarms | Login to the NOAM VIP if not already logged in. Navigate to **Main Menu->Alarms & Events->View Active**  

- **Alarms & Events**  
  - View Active  
  - View History  
  - View Trap Log  

  Examine all active alarms and refer to the on-line help on how to address them.  
  If needed contact **Appendix M. My Oracle Support (MOS)**. |

| 80 | **Backup and Archive All the Databases from the Recovered System** | Execute **Appendix A. Database Backup** to back up the Configuration databases: |

| 81 | **Recover IDIH (If Configured)** | If any components of IDIH were affected, refer to **Section 7.0** to perform the disaster recovery on IDIH. |

| 82 | **SNMP Workaround** | Refer to **Appendix J. SNMP Configuration** to configure SNMP as a workaround in the following cases:  

1) If SNMP is not configured in DSR/SDS  
2) If SNMP is already configured and **SNMPv3** is selected as enabled version |
5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)

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

Recover **Standby NOAM** server by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.

Recover **Query Server (if needed)** by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.

Recover **Standby SOAM** server by recovering base hardware and software.

- Recover the base hardware.
- Recover the software.

Recover IDIH if necessary
### Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Workarounds</th>
<th>Gather Required Materials</th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
</table>
| 1.     | Refer to Appendix I. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure. Refer to Appendix J. SNMP Configuration to configure SNMP as a workaround in the following cases: 1) If SNMP is not configured in DSR/SDS 2) If SNMP is already configured and SNMPv3 is selected as enabled version | Gather the documents and required materials listed in Section 3.1 Required Materials | 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:  

<table>
<thead>
<tr>
<th>http://&lt;Primary NOAM VIP IP Address&gt;</th>
<th>Login as the guiadmin user:</th>
</tr>
</thead>
</table>
### Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>4.</th>
<th>Active NOAM: Set Failed Servers to OOS</th>
<th>Navigate to <strong>Main Menu -&gt; Status &amp; Manage -&gt; HA</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Oracle System Login" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Log In</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter your username and password to log in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Username: <img src="image" alt="Enter username" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password: <img src="image" alt="Enter password" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Change password" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Log In" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Welcome to the Oracle System Login.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the <a href="#">Oracle Software Web Browser Support Policy</a> for details.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unauthorized access is prohibited.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates." /></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other names may be trademarks of their respective owners.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Copyright" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2010, 2016, Oracle and/or its affiliates. All rights reserved.</td>
</tr>
</tbody>
</table>

Select **Edit**
Procedure 4: Recovery Scenario 4

4. **Modifying HA attributes**

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Max Allowed HA Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieNOAM1</td>
<td>Active</td>
<td>The maximum des</td>
</tr>
<tr>
<td>ZombieNOAM2</td>
<td>Active Standby Spare Observer</td>
<td>OOS</td>
</tr>
<tr>
<td>ZombieDRNOAM1</td>
<td></td>
<td>The maximum des</td>
</tr>
</tbody>
</table>

Set the Max Allowed HA Role drop down box to **OOS** for the failed servers.

Select **Ok**

5. **Replace Failed Equipment**

- HW vendor to replace the failed equipment

6. **Recover PMAC TVOE Host (If Required):**

   - Configure BIOS Settings and Update Firmware
   1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:
      - **HP DL380 Gen8:** “Configure HP Gen 8 Server BIOS Settings”
      - **Oracle X5-2/Netra X5-2/X6-2:** “Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings”
      - **HP DL380 Gen9:** “Configure HP Gen9 Server BIOS Settings”
   2. Verify and/or upgrade server firmware by executing procedure “Upgrade Rack Mount Server Firmware” from reference [8]

7. **Recover PMAC and PMAC TVOE Host:**

   - Backup Available
   1. If the PMAC is located on the failed rack mount server(s), execute this step. Otherwise skip to step 10.

   This step assumes that TVOE and PMAC backups are available, if backups are **NOT** available, skip this step.
   1. Restore the TVOE backup by executing **Appendix G. Restore TVOE Configuration from Backup Media**
   2. on **ALL** failed rack mount servers, restore the PMAC backup by executing **Appendix H. Restore PMAC from Backup**
**Procedure 4: Recovery Scenario 4**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>Recover PMAC and PMAC TVOE Host: Backup Not Available</td>
</tr>
<tr>
<td></td>
<td>If the PMAC is located on the failed rack mount server(s), execute this step. Otherwise skip to step 10.</td>
</tr>
<tr>
<td></td>
<td>This step assumes that TVOE and PMAC backups Are NOT available, if the TVOE and PMAC have already been restored, <strong>skip this step</strong></td>
</tr>
<tr>
<td></td>
<td>1. Execute section “Install and Configure TVOE on First RMS (PMAC Host)” from reference [8]</td>
</tr>
<tr>
<td></td>
<td>2. Execute section “Install PMAC” from reference [8]</td>
</tr>
<tr>
<td></td>
<td>3. Execute section “Initialize the PMAC Application” from reference [8]</td>
</tr>
<tr>
<td></td>
<td><strong>Proceed to Next Step</strong></td>
</tr>
<tr>
<td>9.</td>
<td>Configure PMAC (No Backup)</td>
</tr>
<tr>
<td></td>
<td>If PMAC backup was <strong>NOT</strong> restored in <strong>step 7</strong>, execute this step. Otherwise <strong>Skip this Step</strong>.</td>
</tr>
<tr>
<td></td>
<td>Execute sections “Configure PMAC Server (NetBackup Only)” and “Add RMS to the PMAC Inventory” from reference [8]</td>
</tr>
<tr>
<td>10.</td>
<td>Install/Configure Additional Rack Mount Servers</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If TVOE backups are available refer Appendix G. Restore TVOE Configuration from Backup Media otherwise execute this below step</td>
</tr>
<tr>
<td></td>
<td>If TVOE backups were <strong>NOT</strong> performed on any additional rack mount servers or are not available, execute this step. Otherwise <strong>Skip this Step</strong></td>
</tr>
<tr>
<td></td>
<td>1. Execute procedure “Install TVOE on Additional Rack Mount Servers” from reference [8]</td>
</tr>
<tr>
<td></td>
<td>2. Execute “Configure TVOE on Additional Rack Mount Servers” from reference [8]</td>
</tr>
<tr>
<td></td>
<td>3. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:</td>
</tr>
<tr>
<td></td>
<td>• HP DL380 Gen8: “Configure HP Gen 8 Server BIOS Settings”</td>
</tr>
<tr>
<td></td>
<td>• Oracle X5-2/Netra X5-2/X6-2: “Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings”</td>
</tr>
<tr>
<td></td>
<td>• HP DL380 Gen9: “Configure HP Gen9 Server BIOS Settings”</td>
</tr>
<tr>
<td></td>
<td><strong>HP DL380 GEN 8 SKIP THIS STEP</strong></td>
</tr>
<tr>
<td></td>
<td>Determine the VM placement and Pinning for proper VM placement and pinning. Refer 12 for workbook reference</td>
</tr>
</tbody>
</table>
### Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.</td>
<td>Deploy Redundant PMAC (if required)</td>
<td>Refer to procedure “Deploy Redundant PMAC (Optional)” to re-deploy and configure any redundant PMACs previously configured.</td>
</tr>
</tbody>
</table>
| 13.  | PMAC: Determine if an fdconfig file exists from the initial deployment. | Determine whether the fdconfig backup file exists: 

```bash
[admusr@melbourne-pmac-1 ~]$ ll /usr/TKLC/smac/etc/fdc/
```

Examine the results and verify whether the rms config file `<hostname>.cfg` exists

Note: There may be multiple fdconfig backup files here with respect to each RMS. Select the respective one according to the RMS. |
| 14.  | If FDCONFIG backup file does NOT exist: | Execute this step ONLY If the fdconfig backup file does NOT exist: 
If the fdconfig file does NOT exist: Create the needed file(s) by executing section “Virtual Machine/Network Fast Deployment” from reference [8] 

**WARNING:** It is very important to ensure the file(s) created only affect the TVOE server(s) and its Guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service. |
| 15.  | PMAC [If fdc backup file exists]: Load ISOs into PMAC if not done already | Execute this step ONLY If the fdconfig backup file exists and located at step 13: 
If the DSR, SDS, and TPD ISOs are NOT loaded into the PMAC: Execute procedures 14 of section “Virtual Machine/Network Fast Deployment” from reference [8] 

If already loaded into PMAC, skip this step. |
| 16.  | PMAC [If fdc backup file exists]: Edit/Update Configuration File | Execute this step ONLY If the fdconfig backup file exists and located at step 13: 

Edit the fdconfig file to include only the required/failed servers. 

**Note:** Comment out configuration items that are not needed. 

**Note:** It is recommended that a separate configuration file be created for EACH rack mount server being deployed. 

Note: Cabinet ID in the config file needs to match the cabinet **already defined in PM&C**

The following items are mandatory: 
- `siteName` |
Procedure 4: Recovery Scenario 4

- tpdIso
- dsrlso (if DSR VMs are being configured)
- sdsISO (if SDS VMs are being configured)
- NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured)
- XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured)
- XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured)
- DSRNOAM1XMIPADDRESS (if DSRNOAM1 is being configured)
- DSRNOAM2XMIPADDRESS (if DSRNOAM2 is being configured)
- DSRDRNOAM1XMIPADDRESS (if DSRDRNOAM1 is being configured)
- DSRDRNOAM2XMIPADDRESS (if DSRDRNOAM2 is being configured)
- SDSNOAM1XMIPADDRESS (if SDSNOAM1 is being configured)
- SDSNOAM2XMIPADDRESS (if SDSNOAM2 is being configured)
- SDSDRNOAM1XMIPADDRESS (if SDSDRNOAM1 is being configured)
- SDSDRNOAM2XMIPADDRESS (if SDSDRNOAM2 is being configured)

**Note:** Refer to **Appendix R: VM Automation Profile Values** for DSR and SDS profile values with the configuration file from reference [8]

**Note:** Comment out SDS and DSR profile items if corresponding products are not used.

**Note:** [Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9]: Refer to **Appendix Q.3: Non-HA Lab Node VM Automation Profile Values** for DSR and SDS profile values with the configuration file from reference [8]

**Note:** The VM names should not be modified in the .cfg file. The names are fixed and will be prefixed in the siteName.

**Note:** The VM locations should not be changed from their ‘RMSx’ format. Each RMS should correspond with a separate Rack Mount Server.

**WARNING:** It is very important to ensure the file(s) created only affect the TVOE server(s) and its Guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.

17. **PMAC**
   **[If fdc backup file exists]:**
   Copy the located backedup fdc file to the RMS directory
   
   **Execute this step ONLY If the fdconfig backup file exists and located at step 13:**
   Copy the located fdconfig backup file to the RMS directory:

   ```bash
   $ cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file>
   /usr/TKLC/smac/etc/RMS/
   ```

18. **PMAC[If fdc backup file exists**
   **Execute this step ONLY If the fdconfig backup file exists and located at step 13:**
Procedure 4: Recovery Scenario 4

1. Execute the config.sh script

Execute config.sh against the modified back up config file defined above:

**Note:** If the below command is executed on multiple cfg files, it will overwrite the existing xml file. It is recommended to rename the xml file before running the below command again.

```
$ sudo ./config.sh <config file>
```

Sample Output:

```
Validating config file...
```

19. PMAC

**[If fdc backup file]**

Execute this step ONLY if the fdconfig backup file exists and located at step 13:

With the file generated from the config.sh script, execute the following
Procedure 4: Recovery Scenario 4

If fdc backup file exists:

Execute Fast Deployment

- Execute Fast Deployment command to start fast deployment:

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

**Note:** This is a long duration command. If the screen command was run prior to executing the fdconfig, perform a “screen -dr” to resume the screen session in the event of a terminal timeout etc.

PMAC GUI

[If fdc backup file exists]:

- Monitor the Configuration

20. PMAC GUI

[If fdc backup file exists]:

- Monitor the configuration to completion:

```
If not already done so, establish a GUI session on the PMAC server.

Navigate to **Main Menu -> Task Monitoring**

- **Status and Manage**
  - **Task Monitoring**
  - **Help**
  - **Legal Notices**
  - **Logout**

**Note:** Should a failure occur with fdconfig, logs can be accessed in /var/TKLC/log/fdconfig/fdconfig.log

```
[admusr@melbourne-pmac-1 fdconfig]$ sudo fdconfig dumpsteps --file=deploy_melbourne_20170329T202458_701b.fdcdb
Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb"
Here are the steps that were generated
```

---------- begin ---------
## Procedure 4: Recovery Scenario 4

### Dump of DB steps:

<table>
<thead>
<tr>
<th>NUM</th>
<th>PHS</th>
<th>DLY</th>
<th>INFRA</th>
<th>ID</th>
<th>SVRTYPE</th>
<th>CMD</th>
<th>ELEMENT</th>
<th>PRE STATE</th>
<th>TO</th>
<th>STATE</th>
<th>TEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>pmac</td>
<td>Fast_Deployment</td>
<td>1</td>
<td>Run Below command to restart the fdconfig after a failure has occurred and has been resolved:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>pmac</td>
<td>Fast_Deployment</td>
<td>1</td>
<td>$ sudo fdconfig restart -- file=deploy_melbourne_20170329T202458_701b.fdcdb</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>pmac</td>
<td>Fast_Deployment</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>0</td>
<td>pmac</td>
<td>Fast_Deployment</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PMAC**

- **[If fdc backup file exists]:**
  - Repeat for each Rack mount server configuration file

21. **PMAC**

   **Execute this step ONLY If the fdconfig backup file exists and located at step 13:**

   - Repeat **steps 13-20** for each rack mount server/configuration file located at step 13, if required.

22. **PMAC**

   **Execute this step ONLY If the fdconfig backup file exists and located at step 13:**

   - Issue the following commands:
     - Copy the updated fdc file to the fdc backup directory:
       ```bash
       $ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> /usr/TKLC/smac/etc/fdc/
       ```
     - Change permissions:
       ```bash
       $ sudo chmod 777 /usr/TKLC/smac/etc/fdc/<fdc_file>
       ```
### Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 23. | **Perform CPU Pinning**  
Configure VM CPU socket pinning on each TVOE host to optimize performance by executing procedure “CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only)” from reference [8] |
| 24. | **NOAM VIP GUI: Login**  
If the failed server(s) are NOT OAM type, skip to step 34  
Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  

http://<Primary_NOAM_VIP_IP_Address>  
Login as the guiadmin user: |
| 25. | **NOAM VIP GUI: Recover Standby NOAM (If needed)**  
Install the second NOAM server if needed:  
**DSR:**  
Execute procedure “Configure the Second NOAM Server”, steps 1, 3-6 from reference [8]  
**SDS:**  
Execute procedure “Configure the Second SDS NOAM Server”, steps 1, 3-6 from reference [8] |
### Procedure 4: Recovery Scenario 4

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>Install NetBackup Client (Optional)</td>
<td>If NetBackup is used execute procedure “Install NetBackup Client (Optional)” from reference [8]</td>
</tr>
</tbody>
</table>
| 27 | NOAM VIP GUI: Set HA on Standby NOAM | Navigate to Status & Manage -> HA  

![Status & Manage](image)

Click on Edit at the bottom of the screen  
Select the standby NOAM server, set it to Active  
Press OK |
| 28 | NOAM VIP GUI: Restart DSR application | Navigate to Main Menu->Status & Manage->Server,  

![Status & Manage](image)  
Select the recovered standby NOAM server and click on Restart. |
### Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>No.</th>
<th>Active NOAM: Correct the RecognizedAuthority table</th>
<th>NOAM VIP GUI: Recover Query Servers</th>
<th>SDS NOAM VIP GUI: Set HA on Query Server</th>
<th>SDS NOAM VIP GUI: Restart SDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>29.</td>
<td>Establish an SSH session to the active NOAM, login as <strong>admusr</strong>. Execute the following command:</td>
<td>SDS Only, DSR Skip This Step</td>
<td>SDS Only, DSR Skip This Step</td>
<td>SDS Only, DSR Skip This Step</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo top.setPrimary</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Using my cluster: A1789</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Updating A1789.022: <code>&lt;DSR_NOAM_B_hostname&gt;</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Updating A1789.144: <code>&lt;DSR_NOAM_A_hostname&gt;</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30.</td>
<td>SDS Only, DSR Skip This Step</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Execute procedure “Configuring SDS Query Servers”, steps 1, 4-7 from reference [8]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31.</td>
<td>SDS Only, DSR Skip This Step</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Status &amp; Manage -&gt; HA</strong> Click on <strong>Edit</strong> at the bottom of the screen</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select the Query server, set it to <strong>Observer</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Press <strong>OK</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Application</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>33.</td>
<td>Navigate to Main Menu-&gt;Status &amp; Manage-&gt;Server</td>
<td>Select the recovered Query server and click on Restart.</td>
<td></td>
</tr>
<tr>
<td>34.</td>
<td>NOAM VIP GUI: Recover SOAM Servers</td>
<td>Recover the SOAM servers (Standby, Spare-Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only)</td>
<td>DSR: Execute procedure “Configure the SOAM Servers”, steps 1-3, and 5-9 from reference [8]. <strong>Note:</strong> If you are using NetBackup, also execute step 12 of procedure “Configure the SOAM Servers” from reference [8]. SDS: Execute procedure “Configure the SDS DP SOAM Servers”, steps 1-3, and 5-8 from reference [8].</td>
</tr>
<tr>
<td>34.</td>
<td>NOAM VIP GUI: Set HA on Standby SOAM</td>
<td>Navigate to Status &amp; Manage -&gt; HA</td>
<td>Click on Edit at the bottom of the screen</td>
</tr>
</tbody>
</table>
### Procedure 4: Recovery Scenario 4

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| Select the SOAM server, set it to **Active**<br><br>![SOAM Server Selection](image)
|   |   |   |
| **Press OK**<br><br>![Press OK](image)
|   |   |   |
| **35. NOAM VIP GUI:**<br>Restart DSR application<br><br>Navigate to **Main Menu->Status & Manage->Server,**<br>Select the recovered SOAM server and click on **Restart.**
|   |   |   |
| **36. (PCA Only) Activate PCA Feature**<br>If you have PCA installed in the system being recovered, execute the procedure “**PCA Activation on Stand By NOAM network**” on recovered StandBy NOAM Server and procedure “**PCA Activation on Stand By SOAM network**” on recovered StandBy SOAM Server from [7] to re-activate PCA.
|   |   |   |
| **37. NOAM VIP GUI:** Recover the C-Level Server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs<br><br>**DSR:** Execute procedure “**Configure the MP Servers**”, Steps 1, 9-13 from reference [8]<br><br>**Note:** Execute steps 14-16 of “**Configure the MP Servers**”, from reference [8] if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.
**Procedure 4: Recovery Scenario 4**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>38.</strong></td>
<td><strong>NOAM VIP GUI:</strong> Set HA on all C-Level Servers</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Status &amp; Manage -&gt; HA</strong></td>
</tr>
<tr>
<td></td>
<td>Click on <strong>Edit</strong> at the bottom of the screen</td>
</tr>
<tr>
<td></td>
<td>For each server whose Max Allowed HA Role is set to OOS, set it to <strong>Active</strong></td>
</tr>
<tr>
<td></td>
<td>Press <strong>OK</strong></td>
</tr>
</tbody>
</table>

**SDS (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only):**

- Execute procedure **“Configure the SDS DP Servers”**, Steps 1, 5-8 from reference [8]
- Repeat this step for any remaining failed MP servers.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>39.</strong></td>
<td><strong>NOAM VIP GUI:</strong> Restart DSR Application on recovered C-Level Servers</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;Status &amp; Manage-&gt;Server</strong></td>
</tr>
<tr>
<td></td>
<td>Select the recovered C-Level servers and click on <strong>Restart</strong>.</td>
</tr>
</tbody>
</table>
### Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| 40.  | ACTIVE NOAM: Perform key exchange between the active NOAM and recovered servers. | Establish an SSH session to the Active NOAM, login as **admusr**. Execute the following command to perform a key exchange from the active NOAM to each recovered server:  

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

**Note:** If an export server is configured, perform this step.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| 41.  | ACTIVE NOAM: Activate Optional Features | DSR Only, if SDS, Skip This Step  
Establish an SSH session to the active NOAM, login as **admusr**.  

**Note For PCA Activation:**  
If you have PCA installed in the system being recovered, execute the procedure “PCA Activation on Stand By NOAM server” on recovered StandBy NOAM Server and procedure “PCA Activation on Stand By SOAM server” on recovered StandBy SOAM Server from [6] to re-activate PCA.  

**Note:** If not all SOAM sites are recovered at this point, then you should repeat activation for each *new* SOAM site that comes online.  

**Note:** If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.  
Refer to [Section 1.5 Optional Features](#) to activate any features that were previously activated.  
**Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:  

```
iload#31000{S/W Fault}
```

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| 42.  | MP Servers: Disable SCTP Auth Flag (DSR Only) | DSR Only, SDS Skip This Step  
For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [8]  
Execute this procedure on all Failed MP Servers.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| 43.  | NOAM VIP GUI: Fetch and Store the database Report for | Navigate to **Main Menu -> Status & Manage -> Database**
Procedure 4: Recovery Scenario 4

Select the active NOAM server and click on the Report button at the bottom of the page.

The following screen is displayed:

Main Menu: Status & Manage -> Database [Report]

Click on Save and save the report to your local machine.

44. ACTIVE NOAM: Verify Replication Between Servers.

Login to the Active NOAM via SSH terminal as admusr.

Execute the following command:

```bash
$ sudo irepstat -m
```

Output like below shall be generated:

```
-- Policy 0 ActStb [DbReplication] ****************************
```
Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>Oahu-DAMP-1 -- Active</th>
<th>Oahu-DAMP-2 -- Stby</th>
</tr>
</thead>
<tbody>
<tr>
<td>BC From Oahu-SOAM-2</td>
<td>0 0.50 ^0.15%cpu 25B/s A=me</td>
</tr>
<tr>
<td>CC To Oahu-DAMP-2</td>
<td>0 0.10 0.14%cpu 25B/s A=me</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Oahu-IPFE-1 -- Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>BC From Oahu-SOAM-2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Oahu-NOAM-1 -- Stby</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA From Oahu-NOAM-2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Oahu-SS7MP-2 Active</th>
<th>0 0.50 1%R 0.04%cpu 21B/s</th>
</tr>
</thead>
</table>

irepstat (40 lines) (h)elp (m)erged

45. NOAM VIP GUI: Verify the Database states

Click on **Main Menu->Status and Manager->Database**

- Status & Manage
  - Network Elements
  - Server
  - HA
  - Database
  - KPIs
  - Processes

Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below:
Procedure 4: Recovery Scenario 4

**46. NOAM VIP GUI: Verify the HA Status**

Click on **Main Menu->Status and Manage->HA**

Select the row for all of the servers

Verify that the "HA Role" is either "Active" or "Standby".

**47. SOAM VIP GUI: Verify the Local Node Info (DSR Only)**

Navigate to **Main Menu->Diameter->Configuration->Local Node**
### Procedure 4: Recovery Scenario 4

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>48.</td>
<td><strong>SOAM VIP GUI:</strong> Verify the Peer Node Info (DSR Only)</td>
</tr>
<tr>
<td></td>
<td><strong>DSR Only, SDS Skip This Step</strong></td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;Diameter-&gt;Configuration-&gt;Peer Node</strong></td>
</tr>
</tbody>
</table>

Verify that all the local nodes are shown.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>49.</td>
<td><strong>SOAM VIP GUI:</strong> Verify the Connections Info (DSR Only)</td>
</tr>
<tr>
<td></td>
<td><strong>DSR Only, SDS Skip This Step</strong></td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;Diameter-&gt;Configuration-&gt;Connections</strong></td>
</tr>
</tbody>
</table>

Verify that all the peer nodes are shown.
### Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 50.  | **SOAM VIP GUI:** Enable Connections if needed (DSR Only) | **DSR Only, SDS Skip This Step**
|      | Verify that all the connections are shown. |
|      | Navigate to **Main Menu -> Diameter -> Maintenance -> Connections** |
|      | Select each connection and click on the **Enable** button. Alternatively you can enable all the connections by selecting the **EnableAll** button. |
|      | Verify that the Operational State is Available. |
|      | **Note:** If a Disaster Recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution. |
| 51.  | **SOAM VIP GUI:** Enable Optional Features (DSR Only) | **DSR Only, SDS Skip This Step**
|      | Navigate to **Main Menu -> Diameter -> Maintenance -> Applications** |
|      | Select the optional feature application configured in **step 60** |
|      | Click the **Enable** button. |
| 52.  | **SOAM VIP GUI:** Re-enable Transports if Needed (DSR Only) | **DSR Only, SDS Skip This Step**
|      | Navigate to **Main Menu -> Transport Manager -> Maintenance -> Transport** |
Procedure 4: Recovery Scenario 4

Select each transport and click on the Enable button.

Verify that the Operational Status for each transport is Up.

53.
SOAM VIP GUI: Re-enable MAPIWF application if needed (DSR Only)

DSR Only, SDS Skip This Step

Navigate to Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users

Click on the Enable button corresponding to MAPIWF Application Name.

Verify that the SSN Status is Enabled.

54.
SOAM VIP GUI: Re-enable links if needed (DSR Only)

DSR Only, SDS Skip This Step

Navigate to Main Menu->SS7/Sigtran->Maintenance->Links

Click on Enable button for each link.
### Procedure 4: Recovery Scenario 4

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 55. **NOAM VIP:** Verify all servers in Topology are accessible (RADIUS Only) | If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)

Establish an SSH session to the NOAM VIP. Login as **admusr**.

Execute following commands to check if all the servers in the Topology are accessible:

```
$ cd /usr/TKLC/dpi/bin/
$ ./sharedKrevo --checkAccess
```

**Example Output:**

```
[admusr@NOAM-2 bin]$ ./sharedKrevo --checkAccess
FIPS integrity verification test failed.
1450723084: [INFO] 'NOAM-1' is accessible.
FIPS integrity verification test failed.
1450723084: [INFO] 'NOAM-2' is accessible.
FIPS integrity verification test failed.
1450723085: [INFO] 'IDPE' is accessible.
FIPS integrity verification test failed.
1450723085: [INFO] 'MF-2' is accessible.
FIPS integrity verification test failed.
1450723086: [INFO] 'MF-1' is accessible.
[admusr@NOAM-2 bin]$  
```

**Note:** If any of the servers are not accessible, stop and contact Appendix M. My Oracle Support (MOS)

| 56. **NOAM VIP:** Copy key file to all the servers in Topology (RADIUS Only) | If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)

Execute following commands to check if existing Key file on Active NOAM server is valid:

```
$ ./sharedKrevo --validate
```
Procedure 4: Recovery Scenario 4

If output of above command shows that existing key file is not valid then contact Appendix M. My Oracle Support (MOS)

Execute following command to copy the key file to all the servers in the Topology :

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

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

SOAM VIP GUI:  Navigate to Main Menu->Alarms & Events->View Active

Examine All Alarms
## Procedure 4: Recovery Scenario 4

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Examine** all active alarms and refer to the on-line help on how to address them.
- If needed contact Appendix M. My Oracle Support (MOS).

### 58. NOAM VIP GUI: Examine All Alarms

- Login to the NOAM VIP if not already logged in.
- Navigate to **Main Menu->Alarms & Events->View Active**

### 59. Restart oampAgent if Needed

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

### 60. Backup and Archive All the Databases from the Recovered System

- Execute Appendix A. Database Backup to back up the Configuration databases:

### 61. Recover IDIH (If Configured)

- If any components of IDIH were affected, refer to **Section 7.0** to perform the disaster recovery on IDIH.
5.1.5 Recovery Scenario 5 (Both NOAM servers failed with DR-NOAM available)

For a partial outage with both NOAM servers failed but a DR NOAM available, the DR NOAM is switched from secondary to primary then recovers the failed NOAM servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures’ detailed steps are in Procedure 5. The major activities are summarized as follows:

Switch DR NOAM from secondary to primary

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

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

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

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

Recover IDIH if necessary
### Procedure 5: Recovery Scenario 5

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Workarounds</th>
<th>Gather Required Materials</th>
<th>Switch DR NOAM to Primary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✅</td>
<td>lector to Appendix I. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.</td>
<td>Refer Document DSR / SDS 8.x NOAM Failover User's Guide [13]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refer to Appendix J. SNMP Configuration to configure SNMP as a workaround in the following cases:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) If SNMP is not configured in DSR/SDS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) If SNMP is already configured and SNMPv3 is selected as enabled version</td>
</tr>
<tr>
<td>2</td>
<td>✅</td>
<td>Gather the documents and required materials listed in Section 3.1 Required Materials.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>✅</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 M. My Oracle Support (MOS) and ask for assistance.
Procedure 5: Recovery Scenario 5

| 4 | Recover System | If ALL SOAM servers have failed, execute Procedure 2
|   |               | If ALL NOAM servers have failed, execute the following steps:
|   |               | 1) Procedure 4: Steps 4-14
|   |               | 2) Perform a key exchange between the newly active NOAM and the recovered NOAM PMAC:
|   |               | From a terminal window connection on the active NOAM as the admusr user, exchange SSH keys for admusr between the active NOAM and the recovered NOAM’s PMAC server using the key exchange utility, using the management IP address for the PMAC server.
|   |               | When prompted for the password, enter the password for the admusr user of the PMAC server.
|   |               | $ keyexchange admusr@<Recovered_Servers_PMAC_IP Address>
|   |               | Note: if key exchange fails, edit /home/admusr/.ssh/known_hosts and remove blank lines, and retry the key exchange commands.
|   |               | 3) Use the PMAC GUI to determine the control network IP address of the recovered VMs. From the PMAC GUI, navigate to Main Menu -> Software -> Software Inventroy
|   |               | Perform a key exchange between the recovered PMAC and the recovered guests:
|   |               | From a terminal window connection on the recovered PMAC as the admusr user, exchange SSH keys for admusr between the PMAC and the recovered VM guests using the key exchange utility, using the control network IP addresses for the VM guests.
|   |               | When prompted for the password, enter the password for the admusr user of the VM guest.
|   |               | $ keyexchange admusr@<Recovered_VM_control_IP Address>
|   |               | Note: if key exchange fails, edit /home/admusr/.ssh/known_hosts and remove blank lines, and retry the key exchange commands.
|   |               | 4) Procedure 4: 15-19 (To be performed for each NOAM)
Procedure 5: Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td><strong>Perform Key exchange between Active NOAM and Recovered NOAMs</strong>&lt;br&gt;Perform a keyexchange between the newly active NOAM and the recovered NOAM servers:&lt;br&gt;From a terminal window connection on the active NOAM as the <code>admusr</code> user, exchange SSH keys for <code>admusr</code> between the active NOAM and the recovered NOAM servers using the keyexchange utility, using the host names of the recovered NOAMs.&lt;br&gt;When prompted for the password, enter the password for the <code>admusr</code> user of the recovered NOAM servers.&lt;br&gt;$ keyexchange admusr@&lt;Recovered_NOAM Hostname&gt;</td>
</tr>
<tr>
<td>6</td>
<td><strong>NOAM VIP GUI: Recover Standby/Spare SOAM and C-Level Servers</strong>&lt;br&gt;If necessary, refer to Procedure 3 to recover any standby or Spare SOAMs as well as any C-Level servers.</td>
</tr>
<tr>
<td>7</td>
<td><strong>Recovered NOAM servers: Activate Optional Features</strong>&lt;br&gt;DSR Only, if SDS, Skip This Step&lt;br&gt;Map-Diameter Interworking (MAP-IWF) and/or Policy and Charging Application (PCA) Only&lt;br&gt;Activate the features Map-Diameter Interworking (MAP-IWF) and Policy and Charging Application (PCA) as follows:&lt;br&gt;<strong>For PCA:</strong>&lt;br&gt;1. Establish SSH sessions to the all the recovered NOAM servers and login as admusr. Refer [7] and execute procedure “PCA Activation on Standby NOAM server” on all recovered NOAM Servers to re-activate PCA.&lt;br&gt;<strong>For MAP-IWF:</strong>&lt;br&gt;1. Establish SSH session to the recovered active NOAM, login as <code>admusr</code>. Refer [5] to activate Map-Diameter Interworking (MAP-IWF)&lt;br&gt;Note: While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:&lt;br&gt;<code>iload#31000{S/W Fault}</code>&lt;br&gt;Note: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.</td>
</tr>
</tbody>
</table>
## Procedure 5: Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 8    | **DR-NOAM VIP:** Copy key file to recovered NOAM servers in Topology (RADIUS Only) | DSR Only, if SDS, Skip This Step  
If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)  
Establish an SSH session to any of the Active DR NOAM which is intact and operational. Login as admusr.
Execute following commands to check if existing Key file on Active DR NOAM server is valid:  
```
$ cd /usr/TKLC/dpi/bin/
$ ./sharedKrevo –validate
```
Note: If errors are present, stop and contact Appendix M. My Oracle Support (MOS)  
If key file is valid, Execute following commands to copy Key file from Active DR NOAM server to recovered NOAMs:
```
$ ./sharedKrevo -copyKey -destServer <First NOAM>
$ ./sharedKrevo -copyKey -destServer <Second NOAM>
``` |
| 9    | **Primary NOAM:** Modify DSR OAM process | Establish an SSH session to the primary NOAM, login as admusr.
Execute the following commands:  
Retrieve the cluster ID of the recovered NOAM:  
```
$ sudo iqt -fClusterID TopologyMapping where "NodeID='"<DR_NOAM_Host_Name>'"
```
```
Server_ID | NodeID | ClusterID  
---|---|---
1 | Oahu-DSR-NOAM-2 | A1055
```
Execute the following command to start the DSR OAM process on the recovered NOAM:  
```
$ echo "<clusterID>|DSROAM_Proc|Yes" | iload -ha -xun -fcluster -fresource -foptional HaClusterResourceCfg
``` |
| 10   | **Switch DR NOAM Back to Secondary** | Once the system has been recovered:  
### Procedure 5: Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>11</strong></td>
<td><strong>NOAM VIP:</strong> Verify all servers in Topology are accessible (RADIUS Only) <strong>DSR Only, if SDS, Skip This Step</strong>&lt;br&gt; If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)&lt;br&gt; Establish an SSH session to the NOAM VIP. Login as <em>admusr</em>.&lt;br&gt; Execute following command to check if all the servers in the Topology are accessible:&lt;br&gt; <code>bash&lt;br&gt;$ cd /usr/TKLC/dsr/bin/&lt;br&gt;$ ./sharedKrevo -checkAccess&lt;br&gt;</code>&lt;br&gt; <strong>Note:</strong> If any of the servers are not accessible, stop and contact Appendix M. My Oracle Support (MOS)</td>
</tr>
<tr>
<td><strong>12</strong></td>
<td><strong>NOAM VIP:</strong> Copy key file to all the servers in Topology (RADIUS Only) <strong>DSR Only, if SDS, Skip This Step</strong>&lt;br&gt; Establish an SSH session to the Active NOAM, login as <em>admusr</em>.&lt;br&gt; Execute following command to copy the key file to all the servers in the Topology:&lt;br&gt; <code>bash&lt;br&gt;$ ./sharedKrevo -synchronize&lt;br&gt;$ ./sharedKrevo -updateData&lt;br&gt;</code>&lt;br&gt; <strong>Note:</strong> If errors are present, stop and contact Appendix M. My Oracle Support (MOS)</td>
</tr>
<tr>
<td><strong>13</strong></td>
<td><strong>Recovered Servers:</strong> Verify Alarms&lt;br&gt; Navigate to Main Menu -&gt; Alarms &amp; Events -&gt; View Active&lt;br&gt; [View Alarms &amp; Events]&lt;br&gt; [View Active]&lt;br&gt; [View History]&lt;br&gt; [View Trap Log]&lt;br&gt; Verify the recovered servers are not contributing to any active alarms (Replication, Topology misconfiguration, database impairments, NTP, etc.)</td>
</tr>
<tr>
<td><strong>14</strong></td>
<td><strong>Recover IDIH (If Configured)</strong>&lt;br&gt; If any components of IDIH were affected, refer to Section 7.0 to perform the disaster recovery on IDIH.</td>
</tr>
</tbody>
</table>
5.1.6 Recovery Scenario 6 (Database Recovery)

5.1.6.1 Recovery Scenario 6: Case 1

For a partial outage with

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

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

**Note:** Corrupt databases on the SOAM will replicate to all SOAMs in its Network Element (Active, Standby, and Spare). It may be necessary to perform this recovery procedure on ALL SOAMs.

**Procedure 6: Recovery Scenario 6 (Case 1)**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Workarounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Refer to Appendix I. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.</td>
</tr>
</tbody>
</table>
Procedure 6: Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Login as the <strong>guiadmin</strong> user:</td>
</tr>
</tbody>
</table>

![Oracle System Login](image)

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the [Oracle Software Web Browser Support Policy](https://www.oracle.com) for details.

Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.
### Procedure 6: Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 3    | **Active NOAM:**  
Set Failed Servers to OOS |
|      | Navigate to **Main Menu** - > **Status & Manage** - > **HA**  
Select **Edit**  
**Modifying HA attributes**  
|      | **[Image of HA attributes table]** |
|      | Set the Max Allowed HA Role drop down box to **OOS** for the failed servers.  
Select **Ok** |
| 4    | **Server Being Recovered:**  
Login |
| 5    | **Server Being Recovered:**  
Change runlevel to 3  
Execute the following command to bring the system to runlevel 3.  
```bash  
$ sudo init 3  
```
| 6    | **Server Being Recovered:**  
Recover System  
Execute the following command and follow the instructions appearing the console prompt  
```bash  
$ sudo /usr/TKLC/appworks/sbin/backout_restore  
```
| 7    | **Server Being Recovered:**  
Change runlevel to 4  
Execute the following command to bring the system back to runlevel 4.  
```bash  
$ sudo init 6  
```
Procedure 6: Recovery Scenario 6 (Case 1)

Server Being Recovered: Verify the server

Execute the following command to verify if the processes are up and running

```
$ sudo pm.getprocs
```

Example Output:

```
A 5139 omha Up 12/21 13:16:28 1 omha
A 5140 omplalarms Up 12/21 13:16:28 1 omplalarms
A 5143 cassmpaa Up 12/21 13:16:28 1 cassmpaa -S 1.3.6.1.4.1.3
23.5.3.28.1
A 5145 omcpss Up 12/21 13:16:28 1 omcpss
A 9999 eclipseHelp Up 12/21 13:16:28 1 eclipseHelp
A 9999 libsave Up 12/21 13:16:28 1 libsave -l10 -MB20 -S40 -
DE20 -W1 -S2
A 9999 libunlock Up 12/21 13:16:28 1 libunlock -f
A 9999 lstatmerge Up 12/21 13:16:28 1 lstatmerge
A 9999 lntmerge Up 12/21 13:16:28 1 lntmerge
A 9999 lntrelUp Up 12/21 13:16:28 1 lntrelUp
A 9999 omnAgent Up 12/21 13:16:28 1 omnAgent
A 9999 pm.watchdog Up 12/21 13:16:28 1 pm.watchdog
A 9999 rsclerk Up 12/21 13:16:28 1 rsclerk -r 6000
A 9999 re_portmap Up 12/21 13:16:28 1 re_portmap -d100
A 9999 staticclerk Up 12/21 13:16:28 1 staticclerk -s 0
A 9999 vmmgr Up 12/21 13:16:28 1 vmmgr
A 9999 -1 Astatelnst Done 12/21 13:16:28 1 Astatelnst
A 9999 -1 auditFlask Done 12/21 13:16:28 1 auditPeriodicTask
A 9999 -1 auditTasks Done 12/21 13:16:28 1 auditDeamonTasks
A 9999 -1 guiRegMapload Done 12/21 13:16:28 1 guiRegMapload
A 9999 -1 madminloads Done 12/21 13:16:28 1 madminloads
```
Procedure 6: Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Set Failed Servers to Active</th>
<th>Navigate to Status &amp; Manage -&gt; HA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Click on Edit at the bottom of the screen</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the failed server, set it to <strong>Active</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Modifying HA attributes</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Hostname</strong></td>
</tr>
<tr>
<td>9</td>
<td>ZombieNOAM1</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td>ZombieNOAM2</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td>ZombieDRNOAM1</td>
<td>Standby</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Press OK</strong></td>
</tr>
</tbody>
</table>
### Procedure 6: Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP:</th>
<th>DSR Only, if SDS, Skip This Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Verify all servers in Topology are accessible (RADIUS Only)</td>
<td>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</td>
</tr>
</tbody>
</table>

Establish an SSH session to the NOAM VIP. Login as `admusr`

Execute following commands to check if all the servers in the Topology are accessible:

```bash
$ cd /usr/TKLC/dpi/bin/
$ ./sharedKrevo -checkAccess
```

```
[admusr@NOAM-2 bin]$ ./sharedKrevo -checkAccess
FIPS integrity verification test failed.
1450723797: [INFO] 'NOAM-1' is accessible.
FIPS integrity verification test failed.
1450723797: [INFO] 'SOAM-1' is accessible.
FIPS integrity verification test failed.
1450723797: [INFO] 'SCAN-2' is accessible.
FIPS integrity verification test failed.
1450723798: [INFO] 'IFPE' is accessible.
FIPS integrity verification test failed.
1450723798: [INFO] 'MF-2' is accessible.
FIPS integrity verification test failed.
1450723798: [INFO] 'MF-1' is accessible.
```

[admusr@NOAM-2 bin]$
**Procedure 6: Recovery Scenario 6 (Case 1)**

<table>
<thead>
<tr>
<th>NOAM VIP:</th>
<th>DSR Only, if SDS, Skip This Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy key file to all the servers in Topology (RADIUS Only)</td>
<td>If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)</td>
</tr>
</tbody>
</table>

Execute following commands to check if existing Key file on Active NOAM (The NOAM which is intact and was not recovered) server is valid:

```
$ ./sharedKrevo -validate
```

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

Execute following command to copy the key file to all the servers in the Topology:

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

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

**Note:** If any errors are present, stop and contact Appendix M. My Oracle Support (MOS)
## Procedure 6: Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th></th>
<th>Backup and Archive All the Databases from the Recovered System</th>
<th>Execute Appendix A. Database Backup to back up the Configuration databases:</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.1.6.2 Recovery Scenario 6: Case 2

For a partial outage with

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

Procedure 7: Recovery Scenario 6 (Case 2)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This procedure performs recovery if database got corrupted in the system and system is in the state to get replicated.</td>
<td></td>
</tr>
<tr>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
<td></td>
</tr>
<tr>
<td>If this procedure fails, contact Appendix M. My Oracle Support (MOS) and ask for assistance.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Workarounds</th>
<th>Refer to Appendix I. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.</th>
</tr>
</thead>
</table>
Procedure 7: Recovery Scenario 6 (Case 2)

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

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:

![Oracle System Login]

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

Unauthorized access is prohibited.

---

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.
Procedure 7: Recovery Scenario 6 (Case 2)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><strong>Active NOAM:</strong> Set Failed Servers to OOS</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu -&gt; Status &amp; Manage -&gt; HA</strong></td>
</tr>
<tr>
<td></td>
<td>Select <strong>Edit</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Modifying HA attributes</strong></td>
</tr>
<tr>
<td></td>
<td>![Image of HA attributes table]</td>
</tr>
<tr>
<td></td>
<td>Set the Max Allowed HA Role drop down box to <strong>OOS</strong> for the failed servers.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Ok</strong></td>
</tr>
<tr>
<td>4</td>
<td><strong>Server in Question:</strong> Login</td>
</tr>
<tr>
<td></td>
<td>Establish an SSH session to the server in question. Login as <strong>admusr</strong></td>
</tr>
<tr>
<td>5</td>
<td><strong>Server in Question:</strong> Take Server out of Service</td>
</tr>
<tr>
<td></td>
<td>Execute the following command to take the server out of service.</td>
</tr>
</tbody>
</table>
|      | ```
|      | $ sudo bash -l
|      | $ sudo prod.clobber
|      | ``` |
| 6    | **Server in Question:** Take Server to DbUp State and Start the Application |
|      | Execute the following commands to take the server to Dbup and start the DSR application: |
|      | ```
|      | $ sudo bash -l
|      | $ sudo prod.start
|      | ``` |
## Procedure 7: Recovery Scenario 6 (Case 2)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 7    | **NOAM VIP GUI:**  Set Failed Servers to Active  
|      | Navigate to **Status & Manage -> HA**  
|      | ![Status & Manage HA menu](image)  
|      | Click on *Edit* at the bottom of the screen  
|      | Select the failed server, set it to **Active**  
|      | ![Modifying HA attributes](image)  
|      | Press **OK**  
|      | **Server in Question:**  Verify the Server State  
|      | Execute the following commands to verify the processes are up and running:  
|      | `$ sudo pm.getprocs`  
|      | Execute the following command to verify if replication channels are up and running:  
|      | `$ sudo irepstat`  
|      | Execute the following command to verify if merging channels are up and running:  
|      | `$ sudo inetmstat` |
### Procedure 7: Recovery Scenario 6 (Case 2)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td><strong>NOAM VIP GUI:</strong> Restart DSR application  &lt;br&gt; Navigate to Main Menu-&gt;Status &amp; Manage-&gt;Server,  &lt;br&gt; Select each recovered server and click on Restart.</td>
</tr>
</tbody>
</table>
| 10   | **NOAM VIP:** Verify all servers in Topology are accessible (RADIUS Only)  <br> **DSR Only, if SDS, Skip This Step**  <br> If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)  <br> Establish an SSH session to the NOAM VIP. Login as admusr.  <br> Execute following commands to check if all the servers in the Topology are accessible:  <br> ```bash  <br>$ cd /usr/TKLC/dpi/bin/  
$ ./sharedKrevo -checkAccess  <br>``` |
Procedure 7: Recovery Scenario 6 (Case 2)

**NOAM VIP:**
Copy key file to all the servers in Topology (RADIUS Only)

**DSR Only, if SDS, Skip This Step**
If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)

Execute following commands to check if existing Key file on Active NOAM (The NOAM which is intact and was not recovered) server is valid:

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

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

Execute following command to copy the key file to all the servers in the Topology:

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

```
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450727731: [INFO] Synced key to IPS
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450727731: [INFO] Synced key to IPS
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450727731: [INFO] Synced key to IPS
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450727731: [INFO] Synced key to IPS
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450727731: [INFO] Synced key to IPS
[admusr@NOAM-2 bin]$ [admusr@NOAM-2 bin]$ ./sharedKrevo -updateData
```

```
[admusr@NOAM-1 bin]$ ./sharedKrevo -updateData
1450203518: [INFO] Updating data on server 'NOAM-1'
1450203519: [INFO] Data updated to 'NOAM-1'
1450203520: [INFO] Updating data on server 'SOAM-2'
1450203521: [INFO] Data updated to 'SOAM-2'
1450203522: [INFO] 1 rows updated on 'SOAM-2'
```

**Note:** If any errors are present, stop and contact Appendix M. My Oracle Support (MOS)
### Procedure 7: Recovery Scenario 6 (Case 2)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td><strong>Backup and Archive All the Databases from the Recovered System</strong></td>
</tr>
</tbody>
</table>

Execute Appendix A. Database Backup to back up the Configuration databases:
6.0 Resolving User Credential Issues after Database Restore

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

6.1 Restoring a Deleted User

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

These users were removed prior to creation of the backup and archive file. They will be reintroduced by system restoration of that file.
## 6.2 Keeping a Restored user

### Procedure 8: Keep Restored User

<table>
<thead>
<tr>
<th>Step #</th>
<th>Before Restoration: Notify Affected Users Before Restoration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step #</th>
<th>After Restoration: Login to the NOAM VIP</th>
</tr>
</thead>
</table>
| 2      | Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  

```
http://<Primary_NOAM_VIP_IP_Address>
```

Login as the `guiadmin` user:
Procedure 8: Keep Restored User

3

After Restoration:
Reset User Passwords

Navigate to Administration -> Access Control -> Users

Select the user

Click the Change Password button

Enter a new password

NOTE: The password must be between 8 and 16 characters.
The password must also contain 3 of these 4 types of characters:
numeric, lowercase alpha, uppercase alpha, special character (!@#$%^&*?)

Click the Continue button
### 6.3 Removing a Restored User

#### Procedure 9: Remove the Restored User

<table>
<thead>
<tr>
<th>STEP #</th>
<th>After Restoration: Login to the NOAM VIP</th>
<th>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:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Login as the guiadmin user:</td>
<td>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</td>
</tr>
</tbody>
</table>

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 M. My Oracle Support (MOS) and ask for assistance.
Procedure 9: Remove the Restored User

<table>
<thead>
<tr>
<th></th>
<th>After Restoration: Delete User</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

**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. They will be deleted by system restoration of that file.

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

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Before Restoration: Notify Affected Users Before Restoration</th>
<th>Perform this procedure to remove users that will be restored by system restoration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.</td>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
</tr>
</tbody>
</table>

If this procedure fails, contact Appendix M. My Oracle Support (MOS) and ask for assistance.
Procedure 10: Restoring an Archive that does not Contain a Current User

### 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:

```plaintext
http://<Primary_NOAM_VIP_IP_Address>
```

Login as the `guiadmin` user:

![Oracle System Login]

---

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.
Procedure 10: Restoring an Archive that does not Contain a Current User

<table>
<thead>
<tr>
<th>3</th>
<th><strong>Before Restoration:</strong> Record user settings</th>
</tr>
</thead>
</table>

Navigate to **Administration -> Access Control -> Users**

Under each affected user, record the following:
- Username,
- Account status
- Remote Auth
- Local Auth
- Concurrent Logins Allowed
- Inactivity Limit
- Comment
- Groups
### Procedure 10: Restoring an Archive that does not Contain a Current User

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><strong>After Restoration:</strong> 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:</td>
</tr>
</tbody>
</table>

```
http://<Primary_NOAM_VIP_IP_Address>
```

Login as the *guiadmin* user:  

![Oracle System Login](image)

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

Unauthorized access is prohibited.

*Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*

*Copyright © 2010, 2015, Oracle and/or its affiliates. All rights reserved.*
Procedure 10: Restoring an Archive that does not Contain a Current User

| 5 | **After Restoration:** Recreate affected user |

Navigate to **Administration -> Access Control -> Users**

Click **Insert**

Recreate the user using the data collected in **Step 3.**

**Adding new user**

- **Username:**
- **Group:**
- **Authentication Options:**
- **Access Options:**
- **Access Allowed:**
- **Maximum Concurrent Logins:**
- **Session Inactivity Limit:**
- **Comment:**

Click **Ok**
### Procedure 10: Restoring an Archive that does not Contain a Current User

<table>
<thead>
<tr>
<th>Step</th>
<th>After Restoration:</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Repeat for Additional Users</td>
<td>Repeat Step 5 to recreate additional users.</td>
</tr>
<tr>
<td>7</td>
<td>Reset the Passwords</td>
<td>See Procedure 8 for resetting passwords for a user.</td>
</tr>
</tbody>
</table>
7.0 IDIH Disaster Recovery

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

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

```xml
</infrastructures>
<servers>

..........................................................
<tvoeguest id="ORA">
    <infrastructure>localPMAC</infrastructure>
    </postdeploy>
    </scripts>
</tvoeguest>
..........................................................

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

**Disaster Recovery Scenarios:**

<table>
<thead>
<tr>
<th>Disaster Recovery Scenario</th>
<th>fdconfig file to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server containing Oracle database server</td>
<td>Install fdconfig xml</td>
</tr>
<tr>
<td>Server containing Application Server</td>
<td>Upgrade/Disaster Recovery xml</td>
</tr>
<tr>
<td>Server containing Mediation Server</td>
<td>Upgrade/Disaster Recovery xml</td>
</tr>
</tbody>
</table>
**Procedure 11: IDIH Disaster Recovery Preparation**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>PMAC GUI: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open web browser and enter: <code>http://&lt;PMAC_Mgmt_Network_IP&gt;</code></td>
</tr>
</tbody>
</table>

Login as *pmacadmin* user:

![Oracle System Login](image)

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 M. My Oracle Support (MOS) and ask for assistance.
<table>
<thead>
<tr>
<th></th>
<th>PMAC GUI: Verify necessary IDIH images are available</th>
<th>Oracle Guest: Establish an SSH session to the Oracle guest, login as <strong>admusr</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2</strong></td>
<td>Navigate to Main Menu -&gt; Software -&gt; Manage Software Images</td>
<td>Execute the following command to perform a database health check:</td>
</tr>
<tr>
<td></td>
<td>Verify the current IDIH TVOE, TPD, Oracle, Application and Mediation images are listed.</td>
<td><strong>$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i</strong></td>
</tr>
<tr>
<td></td>
<td>Verify these values match the name in the <code>&lt;software&gt; &lt;/software&gt;</code> section in the hostname-upgrade_xx-xx-xx.xml file.</td>
<td>Output:</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the necessary software images are not available please follow the instructions from reference [8].</td>
<td><img src="image-url" alt="Database Health Check Output" /></td>
</tr>
</tbody>
</table>
Procedure 12: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
</table>
| **1**  | PMAC GUI: Login

Open web browser and enter:

```plaintext
http://<PMAC_Mgmt_Network_IP>
```

Login as **pmacadmin** user:

![Oracle System Login](image)

If this procedure fails, contact Appendix M. My Oracle Support (MOS) and ask for assistance.
### Procedure 12: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Details</th>
</tr>
</thead>
</table>
| 2    | Remove existing Application Server | Navigate to **Main Menu -> VM Management**  
  - Software  
    - Software Inventory  
    - Manage Software Images  
    - VM Management  
  Select the application guest,  
  Click on the **Delete** button. |
| 3    | Remove existing Mediation Server | Navigate to **Main Menu -> VM Management**  
  - Software  
    - Software Inventory  
    - Manage Software Images  
    - VM Management  
  Select the Mediation guest,  
  Click on the **Delete** button. |
| 4    | PMAC: Establish SSH session and Login | Establish an SSH session to the PMAC, login as **admusr**. |
## Procedure 12: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

| Step | PMAC: Re-install the Mediation and Application Servers | Execute the following command (Enter your upgrade file):
|------|--------------------------------------------------------|--------------------------------------------------------------------------------|
| 5    | $ cd /var/TKLC/smac/guest-dropin
$sudo fdconfig config --file=<hostname-upgrade_xx-xx-xxx>.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.

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC GUI: Monitor the Configuration</th>
</tr>
</thead>
</table>
| 6    | If not already done so, establish a GUI session on the PMAC server. Navigate to **Main Menu -> Task Monitoring**

- Status and Manage
  - Task Monitoring
  - Help
  - Legal Notices
  - Logout

Monitor the IDIH configuration to completion.
Alternatively, you can monitor the `fdconfig` status through the command line after executing the `fdconfig` command:

**Example:**

```
$ admusr@bertie:~/TKLC/smac/guest-dropin
run Config
Request to start a new configuration
Running d-ray_04-21-15 configuration
Configuration file processing complete

Created a deployment database file: deploy_d-ray_20150511T033944_030c.fdcdb
Preparing to run the configuration steps
PMAC has no in progress tasks
Cabinet is already provisioned, skipping: 1
RMS is already provisioned, skipping: 10.250.36.27
Server discovery complete: [RMS ip: 10.250.36.27]
Hostname for [RMS ip: 10.250.36.27] already set to d-ray skipping
```
Procedure 12: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Perform CPU Pinning</td>
</tr>
</tbody>
</table>

Configure VM CPU socket pinning on each TVOE host to optimize performance by executing procedure “CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only)” steps 1-3 from reference [8].

Establish an SSH session to the TVOE host of the recovered VM, login as admusr.

Perform the following command to list the current VMs configured:

```
$ sudo virsh list
```

Reboot the recovered VM by executing the following command:

```
$ sudo virsh reboot <virsh ID>
```

Repeat for each recovered VM.
Appendix A. Database Backup

Procedure 13: Database Backup

The intent of this procedure is to back up the provision and configuration information from an NOAM or SOAM server after the disaster recovery is complete.

**Note:** SOAM database on SDS is not required.

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

If this procedure fails, contact Appendix M. My Oracle Support (MOS) and ask for assistance.

<table>
<thead>
<tr>
<th>STEP #</th>
<th>NOAM/SOAM VIP: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server.</td>
</tr>
<tr>
<td></td>
<td>Open the web browser and enter a URL of:</td>
</tr>
<tr>
<td></td>
<td>http://&lt;Primary_NOAM/SOAM_VIP_IP_Address&gt;</td>
</tr>
<tr>
<td></td>
<td>Login as the guiadmin user:</td>
</tr>
</tbody>
</table>

```
Welcome to the Oracle System Login.
This application is designed to work with most modern HTML5 compliant browsers and uses both Javascript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.
Other names may be trademarks of their respective owners.
Copyright © 2010, 2015. Oracle and/or its affiliates. All rights reserved.
```
Procedure 13: Database Backup

2

NOAM/SOAM VIP: Backup Configuration Data for the System

Navigate to Main Menu -> Status & Manage -> Database

Select the Active NOAM Server and Click on Backup button

Make sure that the checkboxes next to “Configuration” is checked.

Database Backup

Enter a filename for the backup and press OK
**Procedure 13: Database Backup**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 3 | **NOAM/SOAM VIP:** Verify the backup file existence.  
Navigate to **Main Menu -> Status & Manage -> Files**  
Select the Active NOAM or SOAM tab.  
The files on this server will be displayed. Verify the existence of the backup file. |
| 4 | **NOAM/SOAM VIP:** Download the file to a local machine.  
From the previous step, choose the backup file.  
Select the **Download** button  
Select **OK** to confirm the download. |
### Procedure 13: Database Backup

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 5    | **Upload the Image to Secure Location**  
**Transfer the backed up image saved in the previous step to a secure location where the Server Backup files are fetched in case of system disaster recovery.** |
| 6    | **Backup Active SOAM**  
**Repeat Steps 2 through 5 to back up the Active SOAM** |
| 7    | **Take Secured backup of key file (RADIUS Only)**  
**DSR Only, if SDS, Skip This Step**  
**If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator)**  
Login to ssh shell of Active NOAM server using user admusr  
Take secure backup of updated key file “RADIUS shared secret encryption key” for disaster scenarios.  
Execute following command to encrypt the key file before being backed up to secure customer setup:  
\[
\text{
$ ./sharedKrevo -encr$
}
\]  
Execute following command to copy the encrypted key file to secure customer setup:  
\[
\text{
$ sudo scp /var/TKLC/db/filemgmt/DpiKf.bin.encr user@<customer IP>:<path of customer setup>
}
\]  
**Note:** Access to backed up key file must be strictly controlled by the operator. If the operator wishes to further encrypt this key file using operator specified encryption techniques, the operator is recommended to do so, however the operator shall be responsible to decrypt this file using operator specific decryption techniques and copy the resulting DpiKf.bin.encr file securely to the file management folder if the key file needs to be restored for disaster recovery. Once the key file is backed up to the operator provided server and path, it is the responsibility of the operator to ensure access to the backed up key file is extremely selective and restricted |
Appendix B. Recovering/Replacing Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 8 Only)

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

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

<table>
<thead>
<tr>
<th>S T E P #</th>
<th>The intent of this procedure is to recover a failed Aggregation (4948E / 4948E-F) Switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prerequisites for this procedure are:</td>
</tr>
<tr>
<td></td>
<td>- A copy of the networking xml configuration files</td>
</tr>
<tr>
<td></td>
<td>- A copy of HP Misc Firmware DVD or ISO</td>
</tr>
<tr>
<td></td>
<td>- IP address and hostname of the failed switch</td>
</tr>
<tr>
<td></td>
<td>- Rack Mount position of the failed switch</td>
</tr>
<tr>
<td></td>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
</tr>
<tr>
<td></td>
<td>If this procedure fails, contact Appendix M. My Oracle Support (MOS) and ask for assistance.</td>
</tr>
</tbody>
</table>

1. **Recover failed Aggregation Switches: Cisco 4948E/4948E-F**

   Login to the PMAC via SSH as `admusr`

   Remove the old SSH key of the switch from the PMAC by executing the following command from a PMAC command shell:

   ```
   sudo ssh-keygen -R <4948_switch_ip>
   ```

   **Note:** You will need a copy of the HP Misc Firmware DVD or ISO *(or firmware file obtained from the appropriate hardware vendor)* and of the original networking xml files custom for this installation. These will either be stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.

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

   Older platform init files may not work on platform 7.2 systems. Copy the switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy 'switch1A_4948_4948E_init.xml'.

   **After creating the init file Refer to procedure “Replace a failed 4948/4948E/4948E-F switch (PM&C Installed) (netConfig)” to replace a failed Aggregation switch. - Refer [2] for the applicable platform configuration reference.**

   The templates can be found by the following method:

   From the PMAC CLI
   ```
   1. df | grep -I DSR
   ```

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

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

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

4. Locate the DSR_NetConfig_Templates.zip
   
   1. Example:

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

5. Unzip the DSR_NetConfig_Templates.zip file and retrieve the required switch init file
### Procedure 14: Recovering a Failed Aggregation Switch (Cisco 4948E/4948E-F) - HP DL380 Only

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>$ unzip DSR_NetConfig_Templates.zip</code></td>
</tr>
<tr>
<td>6.</td>
<td>Edit the desired file with site specific details. The existing file from original deployment &quot;/usr/TKLC/smac/etc/switch/xml&quot; can be used as a reference.</td>
</tr>
<tr>
<td>7.</td>
<td>Copy the new init file to the &quot;/usr/TKLC/smac/etc/switch/xml&quot; dir.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>$ cp &lt;switch_xml_file&gt; /usr/TKLC/smac/etc/switch/xml/</code></td>
</tr>
</tbody>
</table>
Appendix B. Recovering/Replacing Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 8 Only)

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

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

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Active NOAM: Login</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check off (√) each step as it is completed. Boxes have been provided for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>this purpose under each step number.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If this procedure fails, contact Appendix M. My Oracle Support (MOS) and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ask for assistance.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Active NOAM: Inhibit replication on all C level Servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Execute the following command:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>```</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$ for i in $(iqt -p -z -h -fHostName NodeInfo where &quot;nodeId like 'C*' and siteId='&quot;$siteId&quot;'); do iset -f inhibitRepPlans='A B' NodeInfo where &quot;nodeName='$i'&quot;; done</td>
<td></td>
</tr>
<tr>
<td></td>
<td>```</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** SOAM Site NE name of the site can be found out by logging into the Active NOAM GUI and going to Configuration->Server Groups screen.

Please see the screenshot below for more details. E.g. if ServerSO1 belongs to the site which is being recovered then siteId will be SO_HPC03.
Procedure 15: Inhibit A and B Level Replication on C-Level Servers

After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP/DP is disabled.

Verification of replication inhibition on MP/DPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP/DP servers for the selected site e.g. Site SO_HPC03 shall be set as ‘A B’:

Perform the following command:

$ iqt NodeInfo

Expected output:

<table>
<thead>
<tr>
<th>nodeId</th>
<th>nodeName</th>
<th>hostName</th>
<th>nodeCapability</th>
<th>inhibitRepPlans</th>
<th>siteId</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1386.099</td>
<td>NO1</td>
<td>NO1</td>
<td>Active</td>
<td></td>
<td>NO_HPC03</td>
</tr>
<tr>
<td>B1754.109</td>
<td>SO1</td>
<td>SO1</td>
<td>Active</td>
<td></td>
<td>SO_HPC03</td>
</tr>
<tr>
<td>C2254.131</td>
<td>MP2</td>
<td>MP2</td>
<td>Active</td>
<td>A B</td>
<td>SO_HPC03</td>
</tr>
<tr>
<td>C2254.233</td>
<td>MP1</td>
<td>MP1</td>
<td>Active</td>
<td>A B</td>
<td>SO_HPC03</td>
</tr>
</tbody>
</table>
### Appendix D. Un-Inhibit A and B Level Replication on C-Level Servers

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Active NOAM:</strong> Login</td>
<td>Login to the Active NOAM server via SSH as <code>admusr</code> user.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Active NOAM:</strong> Un-Inhibit replication on all C level Servers</td>
<td>Execute the following command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ for i in </code>$(iqt -p -z -h -fhostName NodeInfo where &quot;nodeId like 'C*' and siteId='&lt;SOAM_Site_NE_namee&gt;'&quot;); do iset -finhibitRepPlans='' NodeInfo where &quot;nodeName='$i'&quot;; done`</td>
</tr>
</tbody>
</table>

**Note:** SOAM Site NE name of the site can be found out by logging into the Active NOAM GUI and going to **Configuration->Server Groups** screen.

Please see the screenshot below for more details. E.g. if ServerSO1 belongs to the site which is being recovered then siteId will be SO_HPC03.

![Screenshot](image.png)
Procedure 16: Un-Inhibit A and B Level Replication on C-Level Servers

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

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>The intent of this procedure is to inhibit A and B level replication on all C Level servers of this site when Active, Standby and Spare SOAMs are lost.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
</tr>
<tr>
<td></td>
<td>If this procedure fails, contact Appendix M. My Oracle Support (MOS) and ask for assistance.</td>
</tr>
<tr>
<td></td>
<td><strong>Active NOAM:</strong> Login</td>
</tr>
</tbody>
</table>
Procedure 15: Inhibit A and B Level Replication on C-Level Servers

| Active NOAM: Inhibit replication on all C level Servers |

Execute the following command:

```bash
$ for i in $(sudo Imysql.client -B -N -e "
SELECT DISTINCT CS.hostname
FROM appworks.Server CS, appworks.Server PS,
appworks.Server2SG C2SG, appworks.Server2SG P2SG,
appworks.ServerGroup CSG, appworks.ServerGroup PSG,
comcol.ClusterInfo CCI, comcol.ClusterInfo PCI,
comcol.ClusterGroupInfo
WHERE CS._h_Server_ID = C2SG._h_Server_ID
AND C2SG._h_SG_ID = CSG._h_SG_ID
AND CSG.clusterId = CCI.clusterId
AND CCI.groups = comcol.ClusterGroupInfo.groupId
AND comcol.ClusterGroupInfo.parentGroup = PCI.groups
AND PCI.clusterId = PSG.clusterId
AND PSG.ServerGroupName='SOAM_SG_NAME';
");
do iset -finhibitRepPlans='A B' NodeInfo where
"nodeName='$i'"; done
```

**Note:** SOAM_SG_NE name of the Server Group can be found out by logging into the Active NOAM GUI and going to **Configuration->Server Groups** screen.

Please see the screenshot below for more details. E.g. if SOAM1 belongs to the site which is being recovered then then server group will be SO_SG.
Appendix F. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Active NOAM:</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Verify Replication has been Inhibited.</td>
</tr>
</tbody>
</table>

After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP/DP is disabled.

Verification of replication inhibition on MP/DPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP/DP servers for the selected server group e.g. Server group SO_SG shall be set as ‘A B’:

Perform the following command:

```
$ iqt NodeInfo
```

<table>
<thead>
<tr>
<th>nodeId</th>
<th>nodeName</th>
<th>hostName</th>
<th>nodeCapability</th>
<th>inhibitRepPlans</th>
<th>siteId</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1386.099</td>
<td>NO1</td>
<td>NO1</td>
<td>Active</td>
<td>NO_HPC03</td>
<td></td>
</tr>
<tr>
<td>B1754.109</td>
<td>SO1</td>
<td>SO1</td>
<td>Active</td>
<td>SO_HPC03</td>
<td></td>
</tr>
<tr>
<td>C2254.131</td>
<td>MP2</td>
<td>MP2</td>
<td>Active</td>
<td>A B</td>
<td>SO_HPC03</td>
</tr>
<tr>
<td>C2254.233</td>
<td>MP1</td>
<td>MP1</td>
<td>Active</td>
<td>A B</td>
<td>SO_HPC03</td>
</tr>
</tbody>
</table>

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

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

**ST E P #1**

The intent of this procedure is to Un-inhibit A and B level replication on all C Level servers of this site when Active, Standby and Spare SOAMs are lost

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

If this procedure fails, contact Appendix M. My Oracle Support (MOS) and ask for assistance.

<table>
<thead>
<tr>
<th>Step</th>
<th>Active NOAM:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Login</td>
</tr>
</tbody>
</table>

Login to the Active NOAM server via SSH as admusr user.
Procedure 16: Un-Inhibit A and B Level Replication on C-Level Servers

<table>
<thead>
<tr>
<th></th>
<th>Active NOAM: Un-Inhibit replication on all C level Servers</th>
<th>Execute the following command:</th>
</tr>
</thead>
</table>

**Note:** \textit{SOAM\_SG\_NAME} name of the site can be found out by logging into the Active NOAM GUI and going to \textbf{Configuration->Server Groups} screen.

Please see the screenshot below for more details. E.g. if ServerSO1 belongs to the site which is being recovered then server group will be SO\_SG.
Procedure 16: Un-Inhibit A and B Level Replication on C-Level Servers

3

Active NOAM:
Verify Replication has been un-Inhibited.

After executing above steps to un-inhibit replication on MP/DP(s), no alarms on GUI would be raised informing that replication on MP/DP is disabled.

Verification of replication un-inhibition on MP/DPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP/DP servers for the selected server group e.g. Server group SO_SG shall be set as ' ':

Perform the following command:

```
$ sudo iqt NodeInfo
```

Expected output:

<table>
<thead>
<tr>
<th>nodeId</th>
<th>nodeName</th>
<th>hostName</th>
<th>nodeCapability</th>
<th>inhibitRepPlans</th>
<th>siteId</th>
<th>excludeTables</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1386.099</td>
<td>NO1</td>
<td>NO1</td>
<td>Active</td>
<td></td>
<td></td>
<td>NO_HPC03</td>
</tr>
<tr>
<td>B1754.109</td>
<td>SO1</td>
<td>SO1</td>
<td>Active</td>
<td></td>
<td></td>
<td>SO_HPC03</td>
</tr>
<tr>
<td>C2254.131</td>
<td>MP2</td>
<td>MP2</td>
<td>Active</td>
<td></td>
<td></td>
<td>SO_HPC03</td>
</tr>
<tr>
<td>C2254.233</td>
<td>MP1</td>
<td>MP1</td>
<td>Active</td>
<td></td>
<td></td>
<td>SO_HPC03</td>
</tr>
</tbody>
</table>
# Appendix G. Restore TVOE Configuration from Backup Media

**Procedure 17: Restore TVOE Configuration from Backup Media**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1 | **Install TVOE Application**  
  - If the PMAC is NOT hosted on the failed rack mount server, follow procedure “Install TVOE on Additional Rack Mount Servers” from reference [8]  
  - If the PMAC is hosted on the failed rack mount server, follow procedure “Install and Configure TVOE on First RMS (PMAC Host)” from reference [8] |
| 2 | **Establish network connectivity**  
  - If the PMAC is NOT hosted on the failed rack mount server, skip this step  
  - If the PMAC is hosted on the failed rack mount server, execute procedures “Gather and Prepare Configuration files” and “First RMS Configuration steps 1-4, 22-23”  
  **Note:** The IP address that is configured on the TVOE must be one that will be accessible via the network of the machine that currently holds the TVOE Backup ISO image. This could be a NetBackup Master Server, a Customer PC, etc. |
| 3 | **Restore TVOE Backup ISO image to the TVOE host (NetBackup)**  
  - If using NetBackup to restore the TVOE backup ISO image execute this step, otherwise skip this step  
    1. Execute Appendix “Application NetBackup Client Installation Procedures” from reference [8]  
    2. Interface with the NetBackup Master Server and initiate a restore of the TVOE backup ISO image.  
  **Note:** Once restored, the ISO image will be in `/var/TKLC/bkp/` on the TVOE server. |
## Procedure 17: Restore TVOE Configuration from Backup Media

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 4 | Transfer TVOE Backup ISO image to the TVOE host | Using the IP of the TVOE host, transfer the backup ISO image to the TVOE.  
**Linux:**  
From the command line of a Linux machine use the following command to copy the backup ISO image to the TVOE host:  
\[
\text{# scp <path_to_image> tvoexfer@<TVOE_IP>:backup/}
\]

**Note:** where `<path_to_image>` is the path to the backup ISO image on the local system and `<TVOE_IP>` is the TVOE IP address.  

**Note:** If the IP is an IPv4 address then `<TVOE_IP>` will be a normal dot-decimal notation (e.g. “10.240.6.170”).  

**Note:** If the IP is an IPv6 link local address then `<TVOE_IP>` will be need to be scoped such as “[fe80::21e:bff:fe76:5e1c%control]” where `control` is the name of the interface on the machine that is initiating the transfer and it must be on the same link as the interface on the TVOE host.  

**IPv4 Example:**  
\[
\text{# scp /path/to/image.iso tvoexfer@10.240.6.170:backup/}
\]

**IPv6 Example:**  
\[
\text{# scp /path/to/image.iso tvoexfer@[fe80::21e:bff:fe76:5e1c%control]:backup/}
\]

**Windows:**  
Use WinSCP to copy the Backup ISO image into the backup directory within the tvoexfer user’s home directory. Please refer to [9] procedure Using WinSCP to copy the backup image to the customer system. |
| 5 | TVOE Server: Login | Establish an SSH session to the TVOE server, login as `admusr`. |
### Procedure 17: Restore TVOE Configuration from Backup Media

<table>
<thead>
<tr>
<th></th>
<th>Restore TVOE Backup ISO image</th>
<th>Restore the TVOE backup ISO by executing the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td></td>
<td><code>$ sudo su - platcfg</code></td>
</tr>
</tbody>
</table>

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

Select the desired archive:

```
Select Backup Media: [/var/IRLS/kmr/0am-VOE-1-plat-app-201809041314.iso]
```

Select OK

Select **Restore Backup Archive**

Confirm restore:
## Procedure 17: Restore TVOE Configuration from Backup Media

<table>
<thead>
<tr>
<th></th>
<th>Monitor TVOE Backup process</th>
<th>Wait for the restore to complete.</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** This will typically take less than 5 minutes

Restore complete:
**Procedure 17: Restore TVOE Configuration from Backup Media**

<table>
<thead>
<tr>
<th>TVOE Server: Exit Restore Backup Menu</th>
<th>Exit the Restore Backup Menu</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Restore Backup Menu" /></td>
<td><img src="image2" alt="Exit Backup Menu" /></td>
</tr>
</tbody>
</table>

- In the Restore Backup Menu, select Exit Restore Backup Menu.
- Use arrow keys to move between options, <Enter> selects, <F12> Main Menu.
Procedure 17: Restore TVOE Configuration from Backup Media

<table>
<thead>
<tr>
<th>Procedure</th>
<th>TVOE Server: Restart</th>
<th>Restart the TVOE server</th>
</tr>
</thead>
</table>

1. **TVOE Server: Restart**

2. **Restart the TVOE server**

   - **Select Yes to Restart**
   - **Confirm Restart**
### Procedure 17: Restore TVOE Configuration from Backup Media

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td><strong>TVOE Server:</strong> Wait for restart to successfully complete.</td>
</tr>
</tbody>
</table>
| 11   | **TVOE Server:** Verify storage pools are active. <br> Login as admusr. <br> Execute the following command to verify all storage pools are listed and are in the active state: <br>  
```  
$ sudo virsh -c "qemu:///system" pool-list
```

Note: If any storage pools are missing or inactive, contact Appendix M. My Oracle Support (MOS)
### Procedure 17: Restore TVOE Configuration from Backup Media

| 12 | **TVOE Server:** Enable HIDS (Optional) | **Note:** Enabling HIDS is optional. This step should be skipped if HIDS is not required to be enabled.  
When enabling HIDS, the baseline should be updated as well so the restored files aren’t incorrectly reported as being tampered with. The following commands should be run from the TVOE host remote console to enable HIDS and update the baseline: |
|----|--------------------------------------|---|
|    | **$ /usr/TKLC/plat/bin/hidsMgr --initialize**  
LOG: HIDS monitoring has been Initialized  
HIDS baseline has been initialized |    |
|    | **$ /usr/TKLC/plat/bin/hidsMgr --enable**  
HIDS monitoring has successfully been enabled  
New State: ENABLED |    |
|    | **$ /usr/TKLC/plat/bin/hidsMgr --update --all**  
HIDS baseline has successfully been updated |    |
### Procedure 17: Restore TVOE Configuration from Backup Media

| 13 | **TVOE Server:** Verify Alarms | Execute the following to verify alarms:
|    |                             | `$ sudo su - platcfg`

Select Diagnostics

![Diagnostics Menu](image1)

Select Alarm Manager

![Alarm Manager](image2)

Select Show Alarm Status

![Show Alarm Status](image3)

If any failures are reported, contact Appendix M. My Oracle Support (MOS)
**Procedure 17: Restore TVOE Configuration from Backup Media**

<table>
<thead>
<tr>
<th></th>
<th>TVOE (Optional): Delete the files from /var/TKLC/upgrade</th>
<th>If the original DSR release is pre 8.0 &amp; performing <em>Network Fast Deployment from</em>[^8], execute the below step:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>After the TVOE configuration is restored, delete the following scripts/supporting files which are copied to /var/TKLC/upgrade/ folder from the DSR ISO:</td>
</tr>
</tbody>
</table>
|   |                                                          | tuned_tvoe.tar  
|   |                                                          | irqtune.sh  
|   |                                                          | cpuset.py  
|   |                                                          | FDCONFIG will re-create these files with necessary permissions. |
## Appendix H. Restore PMAC from Backup

### Procedure 18: Restore PMAC from Backup Media

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Deploy the PMAC Guest</td>
<td>Execute section &quot;Install PMAC&quot; from reference [8]</td>
</tr>
<tr>
<td>2</td>
<td>PMAC: Login</td>
<td>Establish an SSH session to the PMAC server, login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Restore PMAC Backup image to the PMAC host</td>
<td>From the remote backup location, copy the backup file to the deployed PMAC. There are too many possible backup scenarios to cover them all here. The example below is a simple scp from a redundant PM&amp;C backup location. If using IPv6 addresses, command requires shell escapes, e.g. <code>admusr@[&lt;ipV6addr&gt;]:/&lt;file&gt;</code></td>
</tr>
<tr>
<td>4</td>
<td>PMAC: Verify no Alarms are present</td>
<td>Verify no alarms are present by executing the following command: <code>sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</code></td>
</tr>
</tbody>
</table>

**Note:** The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PMAC prior to the restoration of the data.

**Prerequisite:** TVOE management server has been restored. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact Appendix M. My Oracle Support (MOS) and ask for assistance.
### Procedure 18: Restore PMAC from Backup Media

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 5    | Restore the PMAC Data from Backup | Restore the PMAC data from backup by executing the following command:  
```bash
$ sudo /usr/TKLC/smac/bin/pmacadm restore
```

PM&C Restore been successfully initiated as task ID 1

To check the status of the background task, issue the following command:
```bash
$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks
```

**Note:** The result will eventually display *PMAC Restore successful.*

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 6    | PMAC GUI: Login       | Open web browser and navigate to the PMAC GUI, Login as *PMACadmin* user:  
```bash
https://<pmac_network_ip>
```
## Procedure 18: Restore PMAC from Backup Media

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td><strong>PMAC GUI:</strong> Verify Restore Task completed</td>
<td>Navigate to <strong>Task Monitoring</strong>&lt;br&gt;Verify the restore background task completed successfully.&lt;br&gt;Note: After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior, ISO images will be added in the next step.</td>
</tr>
<tr>
<td>8</td>
<td><strong>PMAC GUI:</strong> Verify System Inventory</td>
<td>Navigate to <strong>Main Menu ➔ System Inventory</strong>&lt;br&gt;Verify previously provisioned cabinets are present</td>
</tr>
<tr>
<td>9</td>
<td><strong>PMAC:</strong> Verify PMAC</td>
<td>Perform a system health check on the PMAC&lt;br&gt;$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus&lt;br&gt;This command should return no output on a healthy system.&lt;br&gt;$ sudo /usr/TKLC/smac/bin/sentry status&lt;br&gt;All Processes should be running, displaying output similar to the following:&lt;br&gt;PM&amp;C Sentry Status&lt;br&gt;------------------&lt;br&gt;sentryd started: Mon Jul 23 17:50:49 2012&lt;br&gt;Current activity mode: ACTIVE&lt;br&gt;Process PID Status StartTS NumR&lt;br&gt;------------------&lt;br&gt;-------&lt;br&gt;smacTalk 9039 running Tue Jul 24 12:50:29 2012 2&lt;br&gt;smacMon 9094 running Tue Jul 24 12:50:29 2012 2&lt;br&gt;hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2&lt;br&gt;snmpEventHandler 9176 running Tue Jul 24 12:50:29 2012 2&lt;br&gt;Fri Aug 3 13:16:35 2012&lt;br&gt;Command Complete.</td>
</tr>
</tbody>
</table>
Procedure 18: Restore PMAC from Backup Media

|   10 | **PMAC**: Add ISO images to the PMAC | Re-add any needed ISO images to the PMAC by executing procedure “Load DSR, SDS (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Only), and TPD ISOs to the PMAC Server” from reference [8] for ALL ISO images as required. |
## Procedure 19: Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Deploy the PMAC Guest</strong>&lt;br&gt;Execute section &quot;Install PM&amp;C&quot; from reference [9]&lt;br&gt;&lt;br&gt;<strong>Note:</strong> This procedure is for restoring from a NetBackup server, so specify the appropriate options when deploying PM&amp;C for use with NetBackup.</td>
</tr>
<tr>
<td>2</td>
<td><strong>PMAC TVOE Host: Login</strong>&lt;br&gt;Establish an SSH session to the PMAC TVOE Host, login as <strong>admusr</strong>.</td>
</tr>
</tbody>
</table>
| 3      | **PMAC TVOE Host: Login to PMAC Guest Console**<br>On the TVOE host, execute the following command:<br><br>$ sudo virsh list<br><br>This will produce a listing of currently running virtual machines.  

```
[admusr@Oahu-TVOE-1 ~]$ sudo virsh list
Id       Name          State
1        Oahu-PMAC    running
```

Find the VM name for your PMAC and note its ID number in the first column. |
| 4      | **Connect to console of the VM using the VM number obtained in Step 3.**<br>On the TVOE host, execute:<br><br>$ sudo virsh console <PMAC-VMID>  

Where **PMAC-VMID** is the VM ID you obtained in Step 3:  

```
[admusr@Oahu-TVOE-1 ~]$ sudo virsh console 1
Connected to domain Oahu-PMAC
Escape character is "".
Oracle Linux Server release 6.7
Kernel 2.6.32-578.8.1.el6pre17.0.3.0.0-86.37.0.x86_64 on an x86_64
Oahu-PMAC login: 
```

You are now connected to the PMAC guest console.  

If you wish to return to the TVOE host, you can exit the session by pressing **CTRL + ]**. |
## Procedure 19: Restore PMAC from Backup Server

### PMAC: Prepare PMAC guest to transfer the appropriate backup from Backup Server. Disable iptables, and enable the TPD platcfg backup configuration menus.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 5 | $ sudo /sbin/service iptables stop  
iptables: Flushing firewall rules: [OK ]  
iptables: Setting chains to policy ACCEPT: filter [OK ]
|   | $ sudo /usr/TKLC/smac/etc/services/netbackup start  
Modified menu NBConfig  
-- show  
Set the following menus: NBConfig to visible=1
|   | Modified menu NBInit  
-- show  
Set the following menus: NBInit to visible=1
|   | Modified menu NBDeInit  
-- show  
Set the following menus: NBDeInit to visible=1
|   | Modified menu NBInstall  
-- show  
Set the following menus: NBInstall to visible=1
|   | Modified menu NBVerifyEnv  
-- show  
Set the following menus: NBVerifyEnv to visible=1
|   | Modified menu NBVerify  
-- show  
Set the following menus: NBVerify to visible=1

---

### Run the following commands on the PMAC:

```bash
$ sudo /sbin/service iptables stop
iptables: Flushing firewall rules: [OK ]
iptables: Setting chains to policy ACCEPT: filter [OK ]

$ sudo /usr/TKLC/smac/etc/services/netbackup start
```
**Procedure 19: Restore PMAC from Backup Server**

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC: Verify the TPD platcfg backup menus are visible, then exit the TPD platcfg Utility</th>
<th>Issue the following command to verify the TPD platcfg backup menus are visible:</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td></td>
<td>$ sudo /bin/su - platcfg</td>
</tr>
<tr>
<td></td>
<td>Note: In the example image above of the TPD platcfg utility Main Menu the backup menu is identified as “NetBackup Configuration”.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC: Verify the iptables rules are disabled on the PMAC guest</th>
<th>Verify the iptables rules are disabled on the PMAC guest by executing the following command:</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td></td>
<td>$ sudo /sbin/iptables -nL</td>
</tr>
<tr>
<td></td>
<td>Note: The “Initialize PM&amp;C Application” and “Configure PM&amp;C application” prerequisites can be ignored.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td></td>
<td>Note: The “Initialize PM&amp;C Application” and “Configure PM&amp;C application” prerequisites can be ignored.</td>
</tr>
</tbody>
</table>
## Procedure 19: Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 9 | **Backup Server:** Verify appropriate PMAC backup exists.  
This step will likely be executed by customer IT personnel.  
Log in to the Backup Server as the appropriate user, using the user password.  
Execute the appropriate commands to verify the PMAC backup exists for the desired date.  
(Note: The actions and commands required to verify that the PM&C backups exist and the commands required to perform backup and restore on the Backup Server are the responsibility of the site customer.)  
(Note: It is important to choose the correct backup file to use in the restore. The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PM&C prior to the restoration of the data.) |
| 10 | **Backup Server:** Verify appropriate PMAC backup exists.  
This step will likely be executed by customer IT personnel.  
Log in to the Backup Server as the appropriate user, using the user password.  
Execute the appropriate commands to verify the PMAC backup exists for the desired date.  
Execute the appropriate commands to restore the PM&C Management Server backup for the desired date.  
(Note: The actions, and commands, required to verify the PM&C backups exist, and the commands required to perform backup and restore on the Backup Server are the responsibility of the site customer.) |
| 11 | **PMAC:** Verify no Alarms are present  
Verify no alarms are present by executing the following command:  
```bash  
sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus  
```

Note: The result will eventually display **PMAC Restore successful.** |
| 12 | **Restore the PMAC Data from Backup**  
Restore the PMAC data from backup by executing the following command:  
```bash  
sudo /usr/TKLC/smac/bin/pmacadm restore  
PM&C Restore been successfully initiated as task ID 1  
```

To check the status of the background task, issue the following command:  
```bash  
sudo /usr/TKLC/smac/bin/pmaccli getBgTasks  
```

(Note: The result will eventually display **PMAC Restore successful.** |
## Procedure 19: Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td><strong>PMAC GUI:</strong> Login&lt;br&gt;Open web browser and navigate to the PMAC GUI, Login as <strong>PMACadmin</strong> user: &lt;br&gt;<code>https://&lt;pmac_network_ip&gt;</code>&lt;br&gt;<img src="image" alt="Oracle System Login" /></td>
</tr>
<tr>
<td>14</td>
<td><strong>PMAC GUI:</strong> Verify Restore&lt;br&gt;Task completed&lt;br&gt;Navigate to <strong>Task Monitoring</strong>&lt;br&gt;Verify the restore background task completed successfully. <strong>Note:</strong> After the restore is complete, you should see “Add Enclosure” tasks start for all previously provisioning servers. These should be allowed to complete before continuing.&lt;br&gt;<strong>Note:</strong> After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior, ISO images will be added in the next step.</td>
</tr>
</tbody>
</table>
### Procedure 19: Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td><strong>PMAC GUI:</strong> Verify System Inventory</td>
<td>Navigate to Main Menu -&gt; System Inventory&lt;br&gt;Verify previously provisioned enclosures are present</td>
</tr>
<tr>
<td>16</td>
<td><strong>PMAC:</strong> Verify PMAC</td>
<td>Perform a system health check on the PMAC&lt;br&gt;$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus&lt;br&gt;This command should return no output on a healthy system.&lt;br&gt;$ sudo /usr/TKLC/smac/bin/sentry status&lt;br&gt;All Processes should be running, displaying output similar to the following:&lt;br&gt;PM&amp;C Sentry Status&lt;br&gt;------------&lt;br&gt;sentryd started: Mon Jul 23 17:50:49 2012&lt;br&gt;Current activity mode: ACTIVE&lt;br&gt;Process PID Status StartTS NumR&lt;br&gt;-------------------&lt;br&gt;---------&lt;br&gt;smacTalk 9039 running Tue Jul 24 12:50:29 2012 2&lt;br&gt;smacMon 9094 running Tue Jul 24 12:50:29 2012 2&lt;br&gt;hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2&lt;br&gt;snmpEventHandler 9176 running Tue Jul 24 12:50:29 2012 2&lt;br&gt;Fri Aug 3 13:16:35 2012&lt;br&gt;Command Complete.</td>
</tr>
<tr>
<td>17</td>
<td><strong>PMAC:</strong> Add ISO images to the PMAC</td>
<td>Re-add any needed ISO images to the PMAC by executing procedure “Load Application and TPD ISO onto PMAC Server” from reference [8]</td>
</tr>
</tbody>
</table>
Appendix I. Workarounds for Issues not fixed in this Release

<table>
<thead>
<tr>
<th>Issue</th>
<th>Associated PR/Bug</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSR 8.0 Only: Restore Database from the active SOAM server will fail if the spare SOAM is in another network and is unreachable</td>
<td>23018247</td>
<td>This workaround is only required for DSR 8.0. While restoring the database from the recovered SOAM GUI, if the spare SOAM is in another network and is unreachable, the database restore will fail. <strong>Workaround</strong> - If the spare SOAM is unreachable and ping (from recovered SOAM server to spare SOAM server) hangs (as evidenced by &quot;ps -ef</td>
</tr>
</tbody>
</table>

Appendix J. SNMP Configuration

Procedure 20: SNMP Configuration

This workaround procedure will provide the steps to configure SNMP with 'SNMPv2c and SNMPv3' as the enabled versions for SNMP Traps configuration, as PMAC does not support SNMPv3.

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

If this procedure fails, contact Appendix M. My Oracle Support (MOS), and ask for assistance.

1. **(Workaround)** PRIMARY NOAM VIP GUI: Login

   **NOTE:** This workaround step should be performed only in any of the following cases:
   1) If SNMP is not configured
   2) If SNMP is already configured and SNMPv3 is selected as enabled version

   **Note:** This is a workaround step to configure SNMP with 'SNMPv2c and SNMPv3' as the enabled versions for SNMP Traps configuration, as PMAC does not support SNMPv3.

   Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of:

   `http://<Primary_NOAM_VIP_IP_Address>`

   Login as the **guiadmin** user:
Procedure 20: SNMP Configuration

2.

NOAM VIP GUI:
Configure System-Wide SNMP Trap Receiver(s)

Navigate to Main Menu -> Administration -> Remote Servers -> SNMP Trapping

Select the Server Group tab for SNMP trap configuration:

Fill in the IP address or hostname of the Network Management Station (NMS) you
### Procedure 20: SNMP Configuration

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>244</td>
<td>Set the Enabled Versions as <strong>SNMPv2c and SNMPv3</strong>:</td>
</tr>
<tr>
<td>245</td>
<td><strong>Check Traps Enabled</strong> boxes for the Manager servers being configured:</td>
</tr>
<tr>
<td>246</td>
<td>Enter the <strong>SNMP Community Name</strong>:</td>
</tr>
<tr>
<td>249</td>
<td>Leave all other fields at their default values.</td>
</tr>
<tr>
<td>250</td>
<td>Press <strong>OK</strong></td>
</tr>
</tbody>
</table>

#### 3 NOAMP VIP: Enable Traps from Individual Servers (Optional)

**Note:** By default SNMP traps from MPs are aggregated and then displayed at the active NOAMP. If instead, you wish for every server to send its own traps directly to the NMS, then execute this procedure.

This procedure requires that all servers, including MPs, have an XMI interface on which the customer SNMP Target server (NMS) is reachable.

Navigate to **Main Menu -> Administration -> Remote Servers -> SNMP Trapping**
Procedure 20: SNMP Configuration

Make sure the checkbox next to **Enabled** is checked, if not, check it as shown below.

![Image showing the checkbox for Enabled]

Then click on **Apply** and verify that the data is committed.

<table>
<thead>
<tr>
<th></th>
<th>PMAC: Update the TVOE Host SNMP Community String</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Establish an SSH session to the PMAC, login as <strong>admusr</strong>. Execute the following command to update the TVOE host community string:</td>
</tr>
</tbody>
</table>

```
$ sudo pmaccli setCommStr --AccessType=rw --commStr=<site specific value>
```

**Note:** When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest on the PMAC control network will be updated. All those servers that match the existing Site Specific Community String will not be updated again until the string name is changed.

---

**Appendix K. Restore Provisioning Database**

This procedure will provide the steps to restore SDS Provisioning database.

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

If this procedure fails, contact Appendix M. My Oracle Support (MOS), and ask for assistance.
Log into Primary SDS NOAM GUI using its static IP (not the VIP).

1. Navigate to **Main Menu: Status & Manage -> HA**
2. Click on “Edit”
3. Move the newly recovered standby server to forced standby.

**Main Menu: Status & Manage -> HA [Edit]**

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Max Allowed HA Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rightsvc NOA-b</td>
<td>Active</td>
<td>The maximum allowed HA Role for rightsvc NOA-b</td>
</tr>
<tr>
<td>rightsvc NOA-b</td>
<td>Standby</td>
<td>The maximum allowed HA Role for rightsvc NOA-b</td>
</tr>
<tr>
<td>rightsvc QS</td>
<td>Observer</td>
<td>The maximum allowed HA Role for rightsvc QS</td>
</tr>
</tbody>
</table>

1. Navigate to **Main Menu: Status & Manage -> Database**
2. Select Select Active NOAM and click the Restore button.

**Main Menu: Status & Manage -> Database**

3. Select Provisioning backup file from the list (which was previously placed in /var/TKLC/db/filemgmt/backup directory in Step 5 of Section 2.6.2) and click the OK button.

**Note:** Must use a Provisioning only backup file. Combined backup files containing Configuration & Provisioning data will cause catastrophic...
### Issues which could lead to complete re-installation.

### Main Menu: Status & Manage -> Database [Restore]

#### Database Restore

Select archive to Restore on server: mrownc-sds-NO-a

- backup/backup_sds_righte-sds-NO-a_021512.Auto.tar.gz
- backup/backup_sds_righte-sds-NO-a_021512.Auto.tar.gz
- backup/backup_sds_righte-sds-NO-a_021512.Auto.tar.gz
- backup/backup_sds_righte-sds-NO-a_021512.Auto.tar.gz

#### Archive:

Select the archive to restore.

4. Verify Compatibility and select Ok to restore.

#### Main Menu: Status & Manage -> Database [Restoreconfirm]

#### Database Restore Confirm

The selected database came from righte-sds-NO-a on 03/17/2017 at 11:51PM UTC and contains the following comments: 

- Configuration data
- Database Compatibility

#### Archive Content

Confirm archive "backup/backup_sds_righte-sds-NO-a_021512.Auto.tar.gz" to Restore on server: righte-sds-NO-a.

- [ ] Force
- [ ] Tentative restore on righte-sds-NO-a, double check before.

#### Confirm with:

- Ok
- Cancel

|   | Primary SDS NOAM GUI | Wait 60 seconds for the restore to begin. |
|   | Primary SDS NOAM GUI :Track Progress of Restore | Monitor the "Info" tab under the [Status & Manage → Database] screen and look for the following message:  
Note: - Restore on <Active_NO_hostname> status MAINT_IN_PROGRESS. |
|   | Primary SDS NOAM GUI | Continue to monitor the "Info" tab under the [Status & Manage → Database] screen. |
|   | NOAM GUI:Wait for the restore to complete | screen until the following message is received:  
Success: - Restore on rghnc-sds-NO-b status MAINT_CMD_SUCCESS. Success  

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

1. Navigate to **Main Menu: Status & Manage -> HA**, click Edit.
2. Select the server which was moved to forced standby in **step 2**, change Max HA Role to Active and click OK.

**Main Menu: Status & Manage -> HA [Edit]**

Modifying HA attributes

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Max Allowed HA Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>right-sds-NO-a</td>
<td>Active</td>
<td>The maximum desired HA Role for right-sds-NO-a</td>
</tr>
<tr>
<td>right-sds-NO-b</td>
<td>Active</td>
<td>The maximum desired HA Role for right-sds-NO-b</td>
</tr>
<tr>
<td>right-sds-GS</td>
<td>Observer</td>
<td>The maximum desired HA Role for right-sds-GS</td>
</tr>
</tbody>
</table>

**Appendix L. Recover PDB Relay**

**STEP**

This procedure will provide the steps to re-establish PDB Relay connection.

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

If this procedure fails, contact Appendix M. My Oracle Support (MOS), and ask for assistance.
| # | NOAM VIP console: Determine if pdbrelay is enabled | Execute following command on console of Active NOAM server (accessed via the VIP) and compare the output:

```bash
$iqt -zhp -fvalue ProvOptions where "var='pdbRelayEnabled'"
   TRUE
```

$ Proceed to next step only if the result of above command is true. |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>NOAM VIP GUI: Disable pdbrelay</td>
<td>Uncheck PDB Relay Enabled checkbox under the [SDS --&gt; Configuration --&gt; Options] screen and Apply the change.</td>
</tr>
</tbody>
</table>
| 3 | NOAM VIP console: Emergency Restart (Start from Beginning of Cmd Log) | Execute following command on console:

```bash
$iset -fvalue=0 ProvOptions where "var='pdbRelayMsgLogTimeStamp'"
```
| 4 | NOAM VIP GUI: Enable pdbrelay | Recheck PDB Relay Enabled checkbox under the [SDS --> Configuration --> Options] screen and Apply the change. |

**Appendix M. My Oracle Support (MOS)**

MOS ([https://support.oracle.com](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](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.


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.