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

Copyright © 2019 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates is not responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

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

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

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

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

See more information My Oracle Support (MOS).
Table of Contents

1. Introduction........................................................................................................................................... 6
   1.1 References ........................................................................................................................................ 6
   1.2 Acronyms ........................................................................................................................................ 6
   1.3 Terminology .................................................................................................................................... 7
   1.4 How to Use this Document ........................................................................................................... 8
   1.5 Optional Features .......................................................................................................................... 8

2. General Description .............................................................................................................................. 9
   2.1 Complete Server Outage (All Servers) ......................................................................................... 10
   2.2 Partial Server Outage with One NOAM Server Intact and Both SOAMs Failed ......................... 10
   2.3 Partial Server Outage with Both NOAM Servers Failed and One SOAM Server Intact .......... 10
   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. Procedure Overview ........................................................................................................................... 11
   3.1 Required Materials ......................................................................................................................... 11
   3.2 Disaster Recovery Strategy ............................................................................................................ 12

4. Disaster Recovery Procedure ............................................................................................................. 14
   4.1 Recovery Scenario 1 (Complete Server Outage) ......................................................................... 14
   4.2 Recovery Scenario 2 (Partial Server Outage with One NOAM Server Intact and ALL
       SOAMs Failed) .......................................................................................................................... 56
   4.3 Recovery Scenario 3 (Partial Server Outage with All NOAM Servers Failed and One SOAM Server Intact) .................................................................................................................. 90
   4.4 Recovery Scenario 4 (Partial Server Outage with One NOAM Server and One SOAM
       Server Intact) .......................................................................................................................... 123
   4.5 Recovery Scenario 5 (Both NOAM Servers Failed with DR-NOAM Available) ..................... 147
   4.6 Recovery Scenario 6 (Database Recovery) .................................................................................... 152
       4.6.1 Recovery Scenario 6: Case 1 ................................................................................................. 152
       4.6.2 Recovery Scenario 6: Case 2 ................................................................................................. 158

5. Resolve User Credential Issues after Database Restore ................................................................. 163
   5.1 Restore a Deleted User ................................................................................................................... 163
   5.2 Keep a Restored User .................................................................................................................... 163
   5.3 Remove a Restored User ................................................................................................................. 165
   5.4 Restore a Modified User ............................................................................................................... 166
   5.5 Restore an Archive that Does Not Contain a Current User .......................................................... 166

6. IDIH Disaster Recovery ....................................................................................................................... 171

Appendix A. DSR Database Backup ....................................................................................................... 177
Appendix B. Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only) .................................................................................................................. 181
Appendix C. Inhibit A and B Level Replication on C-level Servers .......................................................... 183
Appendix D. Un-Inhibit A and B Level Replication on C-level Servers ................................................ 184
Appendix E. Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost) .................................................................................. 185
Appendix F. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost) ........................................................................................ 187
Appendix G. Restore TVOE Configuration from Backup Media .................................................................... 189
Appendix H. Restore PMAC from Backup .................................................................................................. 197
Appendix I. Restore Provisioning Database ................................................................................................ 206
Appendix J. Recover PDB Relay ................................................................................................................ 210
Appendix K. SNMP Configuration ............................................................................................................ 211
Appendix L. Backup Directory .................................................................................................................. 214
Appendix M. netConfig backupConfiguration/restoreConfiguration/upgradeFirmware with TPD cipher change .................................................................................................................. 216
Appendix N. My Oracle Support (MOS) ...................................................................................................... 218

List of Tables
Table 1. Acronyms ................................................................................................................................. 6
Table 2. Terminology ............................................................................................................................ 7
Table 3. Optional Features .................................................................................................................. 8
Table 4. Recovery Scenarios ................................................................................................................ 9

List of Figures
Figure 1. Example Procedure Steps Used in This Document ................................................................. 8
Figure 2. Determining Recovery Scenario .......................................................................................... 13

List of Procedures
Procedure 1. Recovery Scenario 1 ........................................................................................................ 15
Procedure 2. Recovery Scenario 2 ........................................................................................................ 57
Procedure 3. Recovery Scenario 3 ........................................................................................................ 91
Procedure 4. Recovery Scenario 4 ........................................................................................................ 124
Procedure 5. Recovery Scenario 5 ........................................................................................................ 147
Procedure 6. Recovery Scenario 6 (Case 1) ........................................................................................ 152
Procedure 7. Recovery Scenario 6 (Case 2) ........................................................................................ 158
Procedure 8. Keep Restored User ........................................................................................................ 163
Procedure 9. Remove the Restored User .......................................................................................... 165
Procedure 10. Restore an Archive That Does Not Contain a Current User ................................. 167
Procedure 11. IDIH Disaster Recovery Preparation ...................................................................... 172
Procedure 12. IDIH Disaster Recovery (Re-Install Mediation and Application Servers) ............. 174
Procedure 13. DSR Database Backup ............................................................................................ 177
Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F) (HP DL380 Gen 9
    Only) ........................................................................................................................................ 181
Procedure 15. Inhibit A and B Level Replication on C-level Servers .............................................. 183
Procedure 16. Un-Inhibit A and B Level Replication on C-level Servers ........................................ 184
Procedure 17. Inhibit A and B Level Replication on C-level Servers .............................................. 185
Procedure 18. Un-Inhibit A and B Level Replication on C-Level Servers ...................................... 187
Procedure 19. Restore TVOE Configuration from Backup Media ................................................... 189
Procedure 20. Restore PMAC from Backup Media ......................................................................... 197
Procedure 21. Restore PMAC from Backup Server ........................................................................ 200
Procedure 22. Restore Provisioning Database .................................................................................. 206
Procedure 23. Recover PDB Relay ................................................................................................. 210
Procedure 24. Configure SNMP .................................................................................................... 211
Procedure 25. Backup Directory .................................................................................................... 214
Procedure 26. Turn off cipher list before backupConfiguration/restoreConfiguration/upgradeFirmware command .............................................................. 216
Procedure 27. Resume cipher list after backupConfiguration/restoreConfiguration/upgradeFirmware command ........................................................................................................ 217
1. Introduction

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

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

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

1.1 References

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

1.2 Acronyms

An alphabetized list of acronyms used in the document.

<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>DSR</td>
<td>Diameter Signaling Router</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>IDIH</td>
<td>Integrated Diameter Intelligence Hub</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>iLO</td>
<td>Integrated Lights Out manager</td>
</tr>
<tr>
<td>IPFE</td>
<td>IP Front End</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>PCA</td>
<td>Policy and Charging Application</td>
</tr>
<tr>
<td>PMAC</td>
<td>Platform Management &amp; Configuration</td>
</tr>
<tr>
<td>RMS</td>
<td>Rack Mounted Server</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage Area Network</td>
</tr>
<tr>
<td>SDS</td>
<td>Subscriber Database Server</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>
</tbody>
</table>

### 1.3 Terminology

An alphabetized list of terms used in the document.

**Table 2. Terminology**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</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>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>
<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>
</tbody>
</table>
1.4 How to Use this Document

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

1. Before beginning a procedure, completely read the instructional text (it displays immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.

2. Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.

3. If a procedural STEP fails to execute successfully or fails to receive the desired output, STOP the procedure. It is recommended to contact My Oracle Support (MOS) for assistance, as described in Appendix N before attempting to continue.

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

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

<table>
<thead>
<tr>
<th>Title/Instructions</th>
<th>Directive/Result Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. □ Change directory</td>
<td>Change to the backup directory.</td>
</tr>
<tr>
<td></td>
<td>$ cd /var/TKLC/backout</td>
</tr>
<tr>
<td>2. □ Verify Network Element data</td>
<td>View the Network Elements configuration data; verify the data; save and print report.</td>
</tr>
<tr>
<td></td>
<td>1. Select Configuration &gt; Network Elements to view Network Elements Configuration screen.</td>
</tr>
</tbody>
</table>

Figure 1. Example Procedure Steps Used in This Document

1.5 Optional Features

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diameter Custom Applications (DCA)</td>
<td>DCA Framework and Application Activation and Deactivation Guide</td>
</tr>
<tr>
<td>Diameter Mediation</td>
<td>DSR Meta Administration Feature Activation Procedure</td>
</tr>
<tr>
<td>Full Address Based Resolution (FABR)</td>
<td>DSR FABR Feature Activation Procedure</td>
</tr>
<tr>
<td>Gateway Location Application (GLA)</td>
<td>DSR GLA Feature Activation Procedure</td>
</tr>
<tr>
<td>Host Intrusion Detection System (HIDS)</td>
<td>DSR Security Guide (Section 3.2)</td>
</tr>
</tbody>
</table>
2. General Description

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map-Diameter Interworking (MAP-IWF)</td>
<td>DSR MAP-Diameter IWF Feature Activation Procedure</td>
</tr>
<tr>
<td>Policy and Charging Application (PCA)</td>
<td>DSR PCA Activation Guide</td>
</tr>
<tr>
<td>Range Based Address Resolution (RBAR)</td>
<td>DSR RBAR Feature Activation Procedure</td>
</tr>
</tbody>
</table>

Table 4. Recovery Scenarios

<table>
<thead>
<tr>
<th>Procedure</th>
<th>State of NOAM and/or SOAM server(s)</th>
</tr>
</thead>
</table>
| Recovery of the entire network from a total outage | • All NOAM servers failed.  
Recovery Scenario 1 (Complete Server Outage) | • All SOAM servers failed.  
• MP servers may or may not have failed. |
| Recovery of one or more servers with at least one NOAM server intact | • At least 1 NOAM server is intact and available.  
Recovery Scenario 2 (Partial Server Outage with One NOAM Server Intact and ALL SOAMs Failed) | • All SOAM servers failed.  
• MP servers may or may not have failed. |
| Recovery of the NOAM pair with one or more SOAM servers intact | • All NOAM servers failed.  
Recovery Scenario 3 (Partial Server Outage with All NOAM Servers Failed and One SOAM Server Intact) | • At least 1 SOAM server out of active, standby, spare is intact and available.  
• MP servers may or may not have failed. |
| Recovery of one or more server with at least one NOAM and one SOAM server intact | • At least 1 NOAM server is intact and available.  
Recovery Scenario 4 (Partial Server Outage with One NOAM Server and One SOAM Server Intact) | • At least 1 SOAM server out of active, standby, spare is intact and available.  
• 1 or more MP servers have failed. |
| Recovery Scenario 5 (Both NOAM Servers Failed with DR-NOAM Available) | • Both NOAM servers failed.  
• DR NOAM is available  
• SOAM servers may or may not be failed.  
• MP servers may or may not be failed. |
| Section Recovery Scenario 6 (Database Recovery) | • Server is intact  
Recovery of one or more server with corrupt databases that cannot be restored using replication from the active parent node. | • Database gets corrupted on the server  
• Latest database backup of the corrupt server is present  
• Replication is inhibited (either manually or because of Comcol upgrade barrier) |
## Procedure | State of NOAM and/or SOAM server(s)
--- | ---
**Section Recovery Scenario 6: Case 1** | • Server is intact  
• Database gets corrupted on the server  
• Replication is occurring to the server with corrupted database

**Section Recovery Scenario 6: Case 2** | • Server is intact  
• Database gets corrupted on the server  
• Latest Database backup of the corrupt server is NOT present  
• Replication is inhibited (either manually or because of Comcol upgrade barrier)

### Note:  For failed aggregation switches (HP DL380 Gen 8 Only), refer to Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only).

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

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

### 2.1 Complete Server Outage (All Servers)

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

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

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

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

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

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

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

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

2.5 Partial Server Outage with Both NOAMs Failed and DR-NOAM Available

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

2.6 Partial Service Outage with Corrupt Database

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

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

3. Procedure Overview

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

3.1 Required Materials

The following items are needed for disaster recovery:

1. A hardcopy of this document and hardcopies of all documents in the reference list.
2. Hardcopy of all NAPD performed at the initial installation and network configuration of this customer’s site. If the NAPD cannot be found, escalate this issue within My Oracle Support (MOS) until the NAPD documents can be located.
3. DSR recent backup files: electronic backup file (preferred) or hardcopy of all DSR configuration and provisioning data.
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.
13. Three (3) target release iDIH Media or target-release ISOs.
15. Latest RADIUS shared secret encryption key file backup (DpiKf.bin.encr).
16. List of activated and enabled features.

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

3.2 Disaster Recovery Strategy

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

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

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

**WARNING**

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

**Recovering Base Hardware:**

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

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

**WARNING**

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

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

- Backup.dsr.DSRNO1.Configuration.NETWORK_OAMP.20180328_021502.AUTO.tar
- Backup.dsr.DSRSO1.Configuration.SYSTEM_OAM.20180328_021502.AUTO.tar
- X7201TVOE-plat-app-201803281022.iso
- backupPmac_20180328_050002.pef5.1.1

4.1 Recovery Scenario 1 (Complete Server Outage)

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

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

- Recover base hardware and software for all rack mount servers
  - Recover the base hardware
  - Recover the virtual machines
  - Recover the software
• Recover PMAC
• Recover active NOAM guest
  • Recover the NOAM database
  • Reconfigure the application
• Recover standby NOAM guest
  • Reconfigure the application
• Recover query server (SDS only) guest
  • Reconfigure the application
• Recover all SOAM and MP/DP guest
  • Recover the SOAM database
  • Reconfigure the application
• Recover 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>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Gather required materials</td>
</tr>
<tr>
<td>2.</td>
<td>Create a backup directory, if needed</td>
</tr>
<tr>
<td>3.</td>
<td>Replace failed equipment</td>
</tr>
<tr>
<td>4.</td>
<td>Recover PMAC and PMAC TVOE Host: Configure BIOS settings and update firmware</td>
</tr>
</tbody>
</table>

This procedure performs recovery if both NOAM servers are failed and all SOAM servers failed. This procedure also covers the C-level server failure.

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

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

1. Gather the documents and required materials listed in the Required Materials section.

2. Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.

3. Work with the hardware vendor to replace the failed equipment.

4. 1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:
   • **HP DL380 Gen8**: Configure HP Gen 8 Server BIOS Settings
   • **Oracle X5-2/Netra X5-2/X6-2/X7-2**: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings
   • **HP DL380 Gen9**: Configure HP Gen9 Server BIOS Settings

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

*Note:* Determine VM placement and pinning by following:

• Section 3.1, item 14; and
• In reference [8], Appendix S VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1 Gbps NICs) and CPU Pinning in HP DL380 Gen 9 (Onboard 1 Gbps NICs) for Pinning Information on HP DL380 Gen 9.
## Procedure 1. Recovery Scenario 1

### 5. Recover PMAC, TVOE Hosts, and Switch: Backups available

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

1. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.
2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup.
3. Proceed to step 7.

### 6. Recover PMAC, TVOE Hosts, and Switch: Backups NOT available

This step assumes TVOE and PMAC backups are NOT available. If the TVOE and PMAC have already been restored, skip this step.

Execute these procedures from reference [8]:
- Install and Configure TVOE on First RMS (PMAC Host)
- Install PMAC
- Initialize the PMAC Application

### 7. Recover failed Cisco 4948 aggregation switches (HP DL380 only)

Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 GEN 9, skip this step. Recover failed Cisco 4948 aggregation switches, if needed:

1. Back up available configuration files. Refer to Appendix C Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only) to recover failed Cisco 4948 aggregation switches.
2. Back up configuration files NOT available. Execute the Configure Cisco 4948E-F Aggregation Switches (HP DL 380 Gen 8 Only) section from reference [8].

### 8. Configure PMAC (no backup)

If PMAC backup was NOT restored in step 5, execute this step; otherwise, skip this step.

Execute these procedures from reference [8]:
- Configure PMAC Server (NetBackup Only)
- Add RMS to the PMAC Inventory

### 9. Install/Configure additional rack mount servers

1. Execute the Install TVOE on Additional Rack Mount Servers procedure from reference [8].
2. If backups are available, restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.
   - If backups are NOT available, execute the Configure TVOE on Additional Rack Mount Servers procedure from reference [8].

### 10. Configure BIOS settings and update firmware on additional rack mount servers

1. Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]:
   - HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings
   - HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings
2. Verify and/or upgrade server firmware by executing the Upgrade Rack Mount Server Firmware procedure from reference [8].
**Procedure 1. Recovery Scenario 1**

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

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC:</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td>Copy the backed up fdc file to the RMS directory</td>
<td>Copy the fdconfig backup file to the RMS directory</td>
</tr>
</tbody>
</table>

- **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)

**Notes:**
- Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].
- Comment out SDS and DSR profile items if corresponding products are not used.
- For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9, refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].
- VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName.
- VM locations should not be changed from their RMSx format. Each RMS should correspond to a separate rack mount server.

**WARNING**

Ensure the file(s) created only affect the TVOE server(s) and guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.
Procedure 1. Recovery Scenario 1

| 18. | PMAC: Execute the config.sh script | Execute `config.sh` against the modified backup config file.

**Note:** If the below command is executed on multiple `cfg` files, it overwrites the existing xml file. Rename the xml file before running the command again.

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

Example output:

```
[admuser@5010441PMAC RMS]$ sudo ./config.sh rms.cfg
Validating cfg file...
Successful validation of cfg file.
Added Cabinet 101 to Fast Deployment File.
Added Zombie_TV01X1 to Fast Deployment File.
Added Zombie_TV02X1 to Fast Deployment File.
Added xml(bond.4) to Fast Deployment File.
Added ini(bond.0.3) to Fast Deployment File.
Added rep(bond.1.10) to Fast Deployment File.
Added xsl1(bond.1.6) to Fast Deployment File.
Added xsl2(bond.1.7) to Fast Deployment File.
Added xsl3(bond.1.8) to Fast Deployment File.
Added xsl4(bond.1.9) to Fast Deployment File.
Added xsl5(bond.1.11) to Fast Deployment File.
Added xsl6(bond.1.12) to Fast Deployment File.
Added xsl7(bond.1.13) to Fast Deployment File.
Added xsl8(bond.1.14) to Fast Deployment File.
Added xsl9(bond.1.15) to Fast Deployment File.
Added xsl10(bond.1.16) to Fast Deployment File.
Added xsl11(bond.1.17) to Fast Deployment File.
Added xsl12(bond.1.18) to Fast Deployment File.
Added xsl13(bond.1.19) to Fast Deployment File.
Added xsl14(bond.1.20) to Fast Deployment File.
Added xsl15(bond.1.21) to Fast Deployment File.
Added xsl16(bond.1.22) to Fast Deployment File.
Added Zombie_DSRRN0M1 to Fast Deployment File.
Added Zombie_DSRRN0M2 to Fast Deployment File.
Added Zombie_DSRRN0M1 to Fast Deployment File.
Added Zombie_DSRRN0M2 to Fast Deployment File.
Validating Fast Deployment File......
Validation configuration file: ".\Zombie_DSRR_Fast_Deployment_06-15-16.xml"
Configuration file validation successful.
Validation complete
Successful Validation of Zombie_DSRR_Fast_Deployment_06-15-16.xml
SUCCESS: OPERATION SUCCESS!!
```

```
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 19.  | **PMAC**: 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 before executing the fdconfig, perform a `screen -dr` to resume the screen session in the event of a terminal timeout, etc.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 20.  | **PMAC GUI**: Monitor the configuration | 1. If not already done, establish a GUI session on the PMAC server.  
2. Navigate to **Task Monitoring**.  
   - Status and Manage  
   - Task Monitoring  
   - Help  
   - Legal Notices  
   - Logout  
3. Monitor the configuration to completion:  
   ![Main Menu: Task Monitoring](image)  

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

```
[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  
4. Restart the fdconfig after a failure has occurred and has been resolved:  

```bash
$ sudo fdconfig restart --file=deploy_melbourne_20170329T202458_701b.fdcdb
```
## Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC:</th>
<th>Execution Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>21.</td>
<td>Repeat for each rack mount server configuration file</td>
<td>Repeat steps 13. -20. for each rack mount server/configuration file, if required.</td>
</tr>
</tbody>
</table>
| 22.  | Back up FDC file | 1. Copy the updated fdc file to the fdc backup directory:  
$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> 
/usr/TKLC/smac/etc/fdc/  
2. Change permissions:  
$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/<fdc_file> |
| 23.  | Perform CPU pinning | Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only) procedure from reference [8]. |
| 24.  | Obtain latest database backup and network configuration data | 1. Obtain the most recent database backup file from external backup sources (for example, file servers) or tape backup sources.  
2. Obtain most recent RADIUS shared secret encryption key from the DpiKf.bin.encr file on external backup sources (only when the RADIUS key revocation MOP has been executed on the system).  
3. From required materials list in the Required Materials section, use the site survey documents and Network Element report (if available) to determine network configuration data. |
| 25.  | Execute DSR installation procedure for the first NOAM | Verify the networking data for network elements.  
**Notes**  
- Use the backup copy of network configuration data and site surveys from step 2.  
- SDS disaster recovery actions can and should be worked simultaneously to allow faster recovery of the complete solution (that is, stale DB on DP servers do not receive updates until SDS-SOAM servers are recovered). The following steps accommodate both DSR and SDS disaster recovery steps.  
**Important**: While creating the first NOAMs in this step, it is important that the server hostname is the same as one of the NOAM hostnames used prior to the disaster.  
**DSR**:  
1. Configure the first NOAM server by executing the **Configure First NOAM NE and Server** procedure from reference [8].  
2. Configure the NOAM server group by executing the **Configure the NOAM Server Group** procedure from reference [8].  
**SDS**:  
1. Configure the first SDS NOAM server by executing **Configure First SDS NOAM NE and Server** procedure from reference [8].  
2. Configure the SDS NOAM server group by executing the **Configure the SDS NOAM Server Group** procedure from reference [8].  
## Procedure 1. Recovery Scenario 1

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

![Oracle System Login](image)

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 1. Recovery Scenario 1

27. NOAM GUI:
   Upload the backup database file.
   DSR only. If SDS, skip to step 31.

1. Navigate to Status & Manage > Files.

2. Select the active NOAM server.

3. Click Upload and select the NO Provisioning and Configuration file backed up after initial installation and provisioning.

4. Click Browse and locate the backup file.
   Note: If there is no backup file, refer to Appendix L Backup Directory to create the backup directory.

5. Click Open.

6. Mark the This is a backup file checkbox.

7. Click Upload.

The file takes a few seconds to upload depending on the size of the backup data. The file is visible on the list of entries after the upload is complete.
Procedure 1. Recovery Scenario 1

28. NOAM GUI:
    Disable provisioning. DSR only. If SDS, skip to step 31.

1. Navigate to Status & Manage > Database.

2. Click Disable Provisioning.

3. Click OK to disable Provisioning.
Procedure 1. Recovery Scenario 1

29. NOAM GUI: Verify the archive contents and database compatibility. DSR only. If SDS, skip to step 31.

1. Select the Active NOAM server and click Compare.

2. Click the button for the restored database file uploaded as a part of step 27 of this procedure.

3. Verify the output window matches the screen below.

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

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

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

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

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

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

4. If the verification is successful, click **Back** and continue to **next step** in this procedure.
## Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.</td>
<td><strong>Active NOAM:</strong> Restore the database. DSR only. If SDS, skip to step 31.</td>
</tr>
<tr>
<td>1.</td>
<td>From <strong>Status &amp; Manage &gt; Database.</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Select the active NOAM server and click Restore.</td>
</tr>
<tr>
<td>3.</td>
<td>Select the proper backup provisioning and configuration file.</td>
</tr>
<tr>
<td>4.</td>
<td>Click OK.</td>
</tr>
<tr>
<td>5.</td>
<td>If you get errors related to the warnings highlighted in the previous step, then it is expected. If no other errors display, then mark the <strong>Force</strong> checkbox and click <strong>OK</strong> to proceed with the DB restore.</td>
</tr>
<tr>
<td>6.</td>
<td>Go to step 37.</td>
</tr>
</tbody>
</table>

### Database Restore Confirm

**Incompatible archive selected**

---

- The selected database came from ZombieNOA
- Archive Contents
- Configuration data

**Database Compatibility**

The databases are compatible.

---

**Confirm archive**

For data restore?

- **Force**
- Force restore

**Ok** **Cancel**

**Note:** After the restore has started, the user is logged out of the XMI NO GUI since the restored topology is old data.
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>SDS NOAM:</th>
<th>Description</th>
</tr>
</thead>
</table>
| 31. | Transfer SDS configuration and provisioning backup database files. SDS only. If DSR, skip to step 37. | Using the IP of the recovered SDS NOAM, transfer the uncompressed backup database files to the `/var/TKLCD/db/filemgmt` directory. 
**Linux:**
1. From the command line of a Linux machine, copy the configuration backup file to the SDS NOAM guest:

   ```bash
   # scp <path_to_configuration_db_file>
   admusr@<SDS_NOAM_IP>:/var/TKLCD/db/filemgmt
   ```
2. From the command line of a Linux machine, copy the provisioning backup file to the SDS NOAM guest:

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

   where `<path_to_db_file>` is the path to the backup database file on the local system and `<SDS_NOAM_IP>` is the recovered SDS NOAM IP address. 
**Windows:**
Use WinSCP to copy the backup database files into the `/var/TKLCD/db/filemgmt` directory. Refer to the Using WinSCP procedure in reference [9] to copy the backup image to the customer system. |
| 32. | Login. SDS only. If DSR, skip to step 37. | Establish an SSH session to the SDS active NOAM XMI IP address and login as `admusr`. |
| 33. | Stop running applications. SDS only. If DSR, skip to step 37. | Issue the following command to stop running applications. Leave database running:

   ```bash
   $ sudo prod.stop --ignore-cap
   ```

   **Note:** This step may take several minutes to complete. |
| 34. | Restore configuration database. SDS only. If DSR, skip to step 37. | Restore the configuration DB by executing the following command:

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

   Refer to Appendix I Restore Provisioning Database to restore the provisioning database. |
| 35. | Restore provisioning database. SDS only. If DSR, skip to step 37. | Start the SDS application by executing the following command:

   ```bash
   $ sudo prod.start
   ```

   Refer to Appendix I Restore Provisioning Database to restore the provisioning database. |
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Login</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>37.</td>
<td></td>
<td>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:</td>
</tr>
<tr>
<td></td>
<td>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Login as the guiadmin user:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Oracle System Login" /></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>39.</td>
<td>Active NOAM: Set failed servers to OOS</td>
</tr>
<tr>
<td></td>
<td>- Navigate to <strong>Status &amp; Manage &gt; HA</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Status &amp; Manage</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Network Elements</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Server</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>HA</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Database</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>KPIs</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Processes</strong></td>
</tr>
<tr>
<td></td>
<td>- Click <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td>- Set the Max Allowed HA Role option to <strong>OOS</strong> for the failed servers.</td>
</tr>
<tr>
<td></td>
<td>- Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>40.</td>
<td>NOAM VIP GUI: Recover standby NOAM</td>
</tr>
<tr>
<td></td>
<td>- Install the second NOAM server:</td>
</tr>
<tr>
<td></td>
<td>- <strong>DSR:</strong> Execute the <strong>Configure the Second NOAM Server</strong> procedure, steps 1 and 3-6, from reference [8].</td>
</tr>
<tr>
<td></td>
<td>- <strong>SDS:</strong> Execute the <strong>Configure the Second SDS NOAM Server</strong> procedure, steps 1 and 3-6, from reference [8].</td>
</tr>
<tr>
<td>41.</td>
<td>Install NetBackup client (optional)</td>
</tr>
<tr>
<td></td>
<td>- If NetBackup is used, execute the <strong>Install NetBackup Client (Optional)</strong> procedure from reference [8].</td>
</tr>
</tbody>
</table>
## Procedure 1. Recovery Scenario 1

### 42. NOAM VIP GUI: Set HA on standby NOAM

1. Navigate to **Status & Manage > HA**.
2. Click **Edit**.
3. Select the standby NOAM server and set it to **Active**.
4. Click **OK**.

### 43. NOAM VIP GUI: Restart DSR application

1. Navigate to **Status & Manage > Server**.
2. Select the recovered standby NOAM server and click **Restart**.

### 44. Active NOAM: Correct the recognized authority table

1. Establish an SSH session to the active NOAM and login as **admusr**.
2. Execute this command:

   ```bash
   $ sudo top.setPrimary
   - Using my cluster: A1789
   - Updating A1789.022: <DSR_NOAM_B_hostname>
   - Updating A1789.144: <DSR_NOAM_A_hostname>
   ```
Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>45.</td>
<td><strong>NOAM VIP GUI:</strong> Perform Keyexchange with remote import server. SDS only. If DSR, skip to step 47.</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to SDS &gt; Configuration &gt; Options.</td>
</tr>
<tr>
<td>2.</td>
<td>Unmark the <strong>Remote Import Enabled</strong> checkbox.</td>
</tr>
</tbody>
</table>
| 3.   | Click **Apply**.  
  
  *Note:* Navigate to SDS > Configuration > Options again to clear the banner. |
| 4.   | Enter the **Remote Import Password**. |
| 5.   | Click **Apply**.  
  
  *Note:* Navigate to SDS > Configuration > Options again to clear the banner. |
| 6.   | Mark the **Remote Import Enabled** checkbox. |
| 46.  | **NOAM VIP GUI:** Repeat for remote export server. SDS only. If DSR, skip to step 47. |
|      | Repeat step 45. for the remote export server. |
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>No.</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>47.</td>
<td><strong>NOAM VIP GUI:</strong> Perform Keyexchange with export server.</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Administration &gt; Remote Servers &gt; Data Export.</strong></td>
</tr>
<tr>
<td></td>
<td>1. <strong>SSH Key Exchange</strong></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>SSH Key Exchange</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Type the <strong>Password</strong> and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>48.</td>
<td><strong>NOAM VIP GUI:</strong> Recover query servers.</td>
</tr>
<tr>
<td></td>
<td>SDS only. If DSR, skip to step 51.</td>
</tr>
<tr>
<td></td>
<td>Execute the <strong>Configuring SDS Query Servers</strong> procedure, steps 1 and 4-7, 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>49.</td>
<td><strong>SDS NOAM VIP GUI</strong>: Set HA on query server. SDS only. If DSR, skip to step 51.</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to Status &amp; Manage &gt; HA.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Status &amp; Manage</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Network Elements</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Server</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>HA</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Database</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>KPIs</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Processes</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Tasks</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Files</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Select the query server and select <strong>Observer</strong>.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>50.</td>
<td><strong>SDS NOAM VIP GUI</strong>: Restart SDS application. SDS only. If DSR, skip to step 51.</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to Status &amp; Manage &gt; Server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Status &amp; Manage</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Network Elements</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Server</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>HA</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Database</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>KPIs</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Processes</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Select the recovered query server and click <strong>Restart</strong>.</td>
</tr>
<tr>
<td>51.</td>
<td><strong>NOAM VIP GUI</strong>: Stop replication to the C-level servers of this site. DSR only. If SDS, skip to step next step.</td>
</tr>
</tbody>
</table>

### Warning

Before continuing this procedure, replication to C-level servers **MUST** be inhibited at the SOAM site being recovered. Failure to inhibit replication to the working C-level servers results in the database being destroyed!

**If the spare SOAM is also present in the site and lost**, execute Appendix E Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost) to inhibit replication to working C-level servers before continuing.

**If the spare SOAM is NOT deployed in the site**, execute Appendix C Inhibit A and B Level Replication on C-level Servers to inhibit replication to working C-level servers before continuing.
### Procedure 1. Recovery Scenario 1

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

55. NOAM VIP GUI:
Upload the backup SOAM database file.
DSR only. If SDS, skip to step 60.

1. Navigate to Status & Manage > Files.
2. Select the active SOAM server tab. Click Upload and select the file SO Provisioning and Configuration file backed up after initial installation and provisioning.
3. Click Browse and locate the backup file.
4. Mark the This is a backup file checkbox.
5. Click Open.
6. Click Upload.

The file takes a few seconds to upload depending on the size of the backup data and displays on the list of entries when it has completed the upload.
Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th></th>
<th>Recovered SOAM GUI: Login. DSR only. If SDS, skip to step 60.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Establish a GUI session on the recovered SOAM server.</td>
</tr>
<tr>
<td>2.</td>
<td>Open the web browser and enter a URL of:</td>
</tr>
<tr>
<td></td>
<td>http://&lt;Recovered_SOAM_IP_Address&gt;</td>
</tr>
<tr>
<td>3.</td>
<td>Login as the guiadmin user:</td>
</tr>
</tbody>
</table>

![Oracle System Login](image)
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>57.</th>
<th><strong>Recovered SOAM GUI:</strong> Verify the archive contents and database compatibility. DSR only. If SDS, skip to step 60.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Database.</strong></td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Active SOAM</strong> server and click <strong>Compare.</strong></td>
</tr>
<tr>
<td></td>
<td>3. Click the button for the restored database file uploaded as a part of step 27. of this procedure.</td>
</tr>
<tr>
<td></td>
<td>Database Compare</td>
</tr>
<tr>
<td></td>
<td>Select archive to compare on server: 1</td>
</tr>
<tr>
<td></td>
<td>Archive: backup:Backup.DSR.20m</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Database Compare" /></td>
</tr>
<tr>
<td></td>
<td>4. Verify the output window matches the screen below.</td>
</tr>
<tr>
<td></td>
<td><strong>Database Archive Compare</strong></td>
</tr>
<tr>
<td></td>
<td>The selected database came from ZombieSOAM1 on 1</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:** 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.

5. If the verification is successful, click **Back** and continue to **next step** in this procedure.
### Procedure 1. Recovery Scenario 1

| 58. | Recovered SOAM GUI: Restore the database.  
     | DSR only. If SDS, skip to step 60. |
|-----|----------------------------------------|
|     | 1. Select the **Active SOAM** server and click **Restore**.  
     | 2. Select the backup provisioning and configuration file. |
|     | ![Database Compare](image)  
     | ![Database Restore Confirm](image)  
     | 3. Click **OK**. |
|     | 4. If the Node Type Compatibility error displays, it is expected. If no other errors display, mark the **Force** checkbox and click **OK** to proceed with the DB restore. |

**Notes:**
- After the restore has started, the user is logged out of XMI SOAM GUI since the restored topology is old data.
- If the spare SOAM is in another network and is unreachable, the database restore cannot be done.  

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

| 59. | Recovered SOAM GUI: Monitor and confirm database restoration.  
     | DSR only. If SDS, skip to step 60. |
|-----|---------------------------------------------------------------|
|     | Wait for **5-10 minutes** for the system to stabilize with the new topology:  
     | Monitor the Info tab for **Success**. This indicates the restore is complete and the system is stabilized. |

**Notes:**
- Do not pay attention to alarms until all the servers in the system are completely restored.  
- The Configuration and Maintenance information is in the same state it was when backed up during initial backup.
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI:</th>
</tr>
</thead>
<tbody>
<tr>
<td>60.</td>
<td>Login</td>
</tr>
<tr>
<td>61.</td>
<td>Recover the remaining SOAM servers (standby, spare)</td>
</tr>
</tbody>
</table>

1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:

   \[
   \text{http://<Primary_NOAM_VIP_IP_Address>}
   \]

2. Login as the `guiadmin` user:

   ![Oracle System Login](image)

   **Note:** If you are using NetBackup, also execute step 12.

**DSR:**

Execute the **Configure the SOAM Servers** procedure, steps 1-3 and 5-9, from reference [8].

**SDS:**

Execute the **Configure the SDS DP SOAM Servers** procedure, steps 1-3 and 5-8, from reference [8].
## Procedure 1. Recovery Scenario 1

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>62.</td>
<td><strong>NOAM VIP GUI:</strong> Set HA on SOAM server</td>
<td></td>
</tr>
</tbody>
</table>

1. Navigate to **Status & Manage > HA.**
   - Status & Manage
     - Network Elements
     - Server
     - HA
     - Database
     - KPIs
     - Processes
     - Tasks
     - Files
   - Click **Edit.**
   - Select the SOAM server and set it to **Active.**

   ![](image)

2. Click **Edit.**

3. Select the SOAM server and set it to **Active.**

4. Click **OK.**
NOAM VIP GUI: Start replication on working C-level servers.
DSR only. If SDS, skip to next step.

Un-Inhibit (start) replication to the **working** C-level Servers which belongs to the same site as of the failed SOAM servers.

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

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

1. Navigate to **Status & Manage > Database**.

2. If the **Repl Status** is set to **Inhibited**, click **Allow Replication** using this order; otherwise, if none of the servers are inhibited, skip this step and continue with the next step:
   - Active NOAM Server
   - Standby NOAM Server
   - Active SOAM Server
   - Standby SOAM Server
   - Spare SOAM Server (if applicable) — Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only
   - Active DR NOAM Server
   - Standby DR NOAM Server
   - MP/IPFE Servers (if MPs are configured as active/standby, start with the active MP; otherwise, the order of the MPs does not matter)
   - SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only

3. Verify the replication on all the working servers is allowed. This can be done by examining the Repl Status table.

<table>
<thead>
<tr>
<th>OAM Repl Status</th>
<th>SIG Repl Status</th>
<th><strong>Repl Status</strong></th>
<th>Repl Audit Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>No/Applicable</td>
<td>No/Applicable</td>
<td>Allowed</td>
<td>No/Applicable</td>
</tr>
<tr>
<td>Normal</td>
<td>No/Applicable</td>
<td>Allowed</td>
<td>No/Applicable</td>
</tr>
<tr>
<td><strong>Normal</strong></td>
<td>No/Applicable</td>
<td><strong>Allowed</strong></td>
<td><strong>NotApplicable</strong></td>
</tr>
<tr>
<td>Normal</td>
<td>No/Applicable</td>
<td>Allowed</td>
<td>No/Applicable</td>
</tr>
</tbody>
</table>
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| 64.  | NOAM VIP GUI: Restart DSR application | 1. Navigate to **Status & Manage > Server**.  
   |                  | 2. Select the recovered standby NOAM server and click **Restart**. |
| 65.  | NOAM VIP GUI: Perform Keyexchange with export server | 1. Navigate to **Administration > Remote Servers > Data Export**.  
   |                  | 2. Click the **Task Name** and click **Key Exchange**.  
   |                  | 3. Type the **Password** and click **OK**. |
### Procedure 1. Recovery Scenario 1

#### 66. Activate PCA feature. DSR only

| If you have PCA installed in the system being recovered, re-activate PCA by executing the **PCA Activation on Entire Network** procedure on the recovered NOAM server from [7]. |

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

#### 67. NOAM VIP GUI: Recover the C-level server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs)

| DSR: Execute the **Configure the MP Servers** procedure, steps 1 and 9-13, from reference [8]. |

**Note:** Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.

**SDS** (Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only):

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

#### 68. NOAM VIP GUI: Set HA on all C-level servers

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

2. Click **Edit**.

3. For each recovered C-Level with a Max Allowed HA Role set to OOS, set it to **Active**.

4. Click **OK**.
## Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>69.</th>
<th><strong>NOAM VIP GUI:</strong> Restart DSR application on the recovered C-level servers</th>
</tr>
</thead>
</table>

1. Navigate to **Status & Manage > Server.**
   - **Status & Manage**
     - **Network Elements**
     - **Server**
     - **HA**
     - **Database**
     - **KPIs**
     - **Processes**

2. Select the recovered C-level servers and click **Restart.**
Procedure 1. Recovery Scenario 1

70. NOAM VIP GUI: Start replication on all C-Level servers. DSR only. If SDS, then skip to next step.

Un-Inhibit (start) replication to the ALL C-level servers.

1. Navigate to Status & Manage > Database.

   - Network Elements
   - Server
   - HA
   - Database
   - KPIs
   - Processes

2. If the Repl Status is set to Inhibited, click Allow Replication using this order:
   - Active NOAMP Server
   - Standby NOAMP Server
   - Active SOAM Server
   - Standby SOAM Server
   - Spare SOAM Server (if applicable) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only
   - Active DR NOAM Server
   - Standby DR NOAM Server
   - MP/IPFE Servers
   - SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only

3. Verify the replication on all servers is allowed. This can be done by checking the Repl Status.

<table>
<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>

71. Active NOAM: Perform keyexchange between the active NOAM and recovered servers

1. Establish an SSH session to the active NOAM and login as admusr.

2. Perform a keyexchange from the active NOAM to each recovered server:

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

   Note: If an export server is configured, perform this step.
### Procedure 1. Recovery Scenario 1

**72. Active NOAM:**
Activate optional features.
DSR only. If SDS, then skip to next step.

Establish an SSH session to the active NOAM and login as `admusr`.

**Note for PCA Feature Activation:**
If you have PCA installed in the system being recovered, re-activate the PCA by executing the **PCA Activation on Entire Server** procedure on the recovered NOAM server from [6].

**Notes:**
- If not all SOAM sites are recovered at this point, then repeat the activation for each “new” SOAM site that comes online.
- If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature.

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

**73. NOAM VIP GUI:**
Fetch and store the database report for the newly restored data and save it

1. Navigate to **Status & Manage > Database**.

   ![Status & Manage](image)

   - **Network Elements**
   - **Server**
   - **HA**
   - **Database**
   - **KPIs**
   - **Processes**

   The following screen displays:

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

   ![Database Status Report](image)

   - **Hostname**: `ZombieNOAM1`
   - **Database Birthday**: `2016-07-11 11:21:50 EDT`
   - **Appworks Database Version**: `6.0`
   - **Application Database Version**: 

   **Capacities and Utilization**
   - **Disk Utilization**: 8.4%, 588M used of 7.0G total, 6.0G available
   - **Memory Utilization**: 0.0%, used of total, 0K available

2. Select the active NOAM server and click **Report**.

3. Click **Save** and save the report to your local machine.
Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>No.</th>
<th>Active NOAM: Verify replication between servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>74.</td>
<td>Log into the active NOAM as admusr using SSH terminal.</td>
</tr>
<tr>
<td>2.</td>
<td>Execute this command:</td>
</tr>
</tbody>
</table>

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

Example output:

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

1. Navigate to **Status & Manager > Database**.

   ![Image of Status & Manager menu]

2. Verify the OAM Max HA Role is either **Active** or **Standby** for NOAM and SOAM; Application Max HA Role for MPs is **Active**; and status is **Normal**.

<table>
<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>ZombieDRNOAM</td>
<td>ZombieDRNOAM1</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>ZombieMP2</td>
<td>MP</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieMP1</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 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>76.</th>
<th><strong>NOAM VIP GUI:</strong> Upload the backed up RADIUS key file (RADIUS only). DSR only. If SDS, skip to the next step.</th>
</tr>
</thead>
<tbody>
<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>1. Navigate to <strong>Status &amp; Manage &gt; Files</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Select the active NOAM server tab. Click <strong>Upload</strong> and select the <strong>RADIUS shared secret encryption key</strong> file backed up after initial installation and provisioning or after key revocation execution.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Browse</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Locate the <strong>DpiKf.bin.encr</strong> file.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Upload</strong>.</td>
</tr>
</tbody>
</table>

![Upload File](image)

The file takes a few seconds to upload depending on the size of the file. The file is visible on the list of entries after the upload is complete.

**Note:** This file should be deleted from the operator’s local servers as soon as key file is uploaded to the active NOAM server.
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>NOAM VIP: Copy and distribute RADIUS key file on active NOAM (RADIUS only) — Part 1</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.

1. Log into the active NOAM VIP as `admusr` user using SSH terminal.

2. Copy the key file:

```bash
$ cd /usr/TKLC/dpi/bin
$ ./sharedKrevo -decr
$ sudo rm /var/TKLC/db/filemgmt/<backed up key file name>
```

3. Make sure all servers in the topology are accessible.

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

```bash
[admusr@NOAM-2 bin]$ ./sharedKrevo -checkAccess
RADIUS 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] 'IFPE' is accessible.
FIPS integrity verification test failed.
1450723085: [INFO] 'MP-2' is accessible.
```

**Note:** If all the servers are not accessible, then contact My Oracle Support (MOS).
Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>78.</td>
<td><strong>NOAM VIP:</strong> Copy and distribute the RADIUS key file on active NOAM (RADIUS only) — Part 2</td>
<td>Distribute key file to all the servers in the topology:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ ./sharedKrevo -synchronize</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ ./sharedKrevo -updateData</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example output:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Example output" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> For any errors refer My Oracle Support (MOS).</td>
</tr>
<tr>
<td>79.</td>
<td><strong>NOAM VIP GUI:</strong> Verify the HA status</td>
<td>1. Navigate to <strong>Status and Manage &gt; HA.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Status and Manage" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the row for all of the servers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Verify the HA Role is either <strong>Active</strong> or <strong>Standby.</strong></td>
</tr>
</tbody>
</table>

<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>
## Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **80.** | **NOAM GUI:** Enable provisioning  
Enable provisioning.  
DSR only. If SDS, then skip to step 91. |
| 1. | Navigate to **Status & Manage > Database**.  
- Status & Manage  
  - Network Elements  
  - Server  
  - HA  
  - Database  
  - KPIs  
  - Processes  
  - Tasks  
  - Files  
2. | Click **Enable Provisioning**.  
3. | Click **OK**. |
| **81.** | **SOAM GU**I: Enable site provisioning.  
Enable site provisioning.  
DSR only. If SDS, then skip to step 91. |
| 1. | Navigate to **Status & Manage > Database**.  
- Status & Manage  
  - Network Elements  
  - Server  
  - HA  
  - Database  
  - KPIs  
  - Processes  
  - Tasks  
  - Files  
2. | Click **Enable Site Provisioning**.  
3. | Click **OK**. |
| **82.** | **SOAM VIP GUI:** Verify the local node information.  
Verify the local node information.  
DSR only. If SDS, then skip to step 91. |
| 1. | Navigate to **Diameter > Configuration > Local Node**.  
- Diameter  
  - Configuration  
  - Capacity Summary  
  - Connection Capacity Da  
  - Application Dids  
  - CEX Parameters  
  - Command Codes  
  - Configuration Sets  
  - Local Nodes  
2. | Verify all the local nodes are shown. |
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>83.</td>
<td><strong>SOAM VIP GUI:</strong> Verify the peer node information. DSR only. If SDS, then skip to step 91.</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Diameter &gt; Configuration &gt; Peer Node</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Verify all the peer nodes are shown.</td>
</tr>
<tr>
<td>84.</td>
<td><strong>SOAM VIP GUI:</strong> Verify the connections information. DSR only. If SDS, then skip to step 91.</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Diameter &gt; Configuration &gt; Connections</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Verify all the connections are shown.</td>
</tr>
<tr>
<td>85.</td>
<td><strong>MP Servers:</strong> Disable SCTP Auth Flag. DSR only. If SDS, then skip to step 91.</td>
</tr>
<tr>
<td></td>
<td>For SCTP connections without DTLS enabled, refer to the <strong>Enable/Disable DTLS (SCTP Diameter Connections Only)</strong> section in reference [8]. Execute this procedure on all failed MP servers.</td>
</tr>
</tbody>
</table>
## Procedure 1. Recovery Scenario 1

### 86. SOAM VIP GUI: Enable connections, if needed.

- **DSR only. If SDS, then skip to step 91.**

1. Navigate to **Diameter > Maintenance > Connections**.
   - Select each connection and click **Enable**. Alternatively, enable all the connections by clicking **EnableAll**.
   - Verify the Operational State is **Available**.

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

### 87. SOAM VIP GUI: Enable optional features.

- **DSR only. If SDS, then skip to step 91.**

1. Navigate to **Diameter > Maintenance > Applications**.
2. Select the optional feature application configured in step 72.
3. Click **Enable**.

### 88. SOAM VIP GUI: Re-enable transports, if needed.

- **DSR only. If SDS, then skip to step 91.**

1. Navigate to **Transport Manager > Maintenance > Transport**.
2. Select each transport and click **Enable**.
3. Verify the Operational Status for each transport is **Up**.
### Procedure 1. Recovery Scenario 1

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>92.</td>
<td>NOAM VIP GUI: Examine all alarms</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to Alarms &amp; Events &gt; View Active.</td>
</tr>
<tr>
<td></td>
<td><img src="Image" alt="Alarms &amp; Events" /></td>
</tr>
<tr>
<td></td>
<td><img src="Image" alt="View Active" /></td>
</tr>
<tr>
<td></td>
<td><img src="Image" alt="View History" /></td>
</tr>
<tr>
<td></td>
<td><img src="Image" alt="View Trap Log" /></td>
</tr>
<tr>
<td></td>
<td>2. Examine all active alarms and refer to the on-line help on how to address them.</td>
</tr>
<tr>
<td></td>
<td>If needed, contact My Oracle Support (MOS).</td>
</tr>
<tr>
<td>93.</td>
<td>Restore GUI usernames and passwords</td>
</tr>
<tr>
<td></td>
<td>If applicable, execute the section 5 Resolve User Credential Issues after Database Restore procedure to recover the user and group information restored.</td>
</tr>
<tr>
<td>94.</td>
<td>Back up and archive all the databases from the recovered system</td>
</tr>
<tr>
<td></td>
<td>Execute the DSR Database Backup procedure to back up the configuration databases.</td>
</tr>
<tr>
<td>95.</td>
<td>Recover IDIH, if configured</td>
</tr>
<tr>
<td></td>
<td>If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.</td>
</tr>
<tr>
<td>96.</td>
<td>SNMP workaround</td>
</tr>
<tr>
<td></td>
<td>Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases:</td>
</tr>
<tr>
<td></td>
<td>1. If SNMP is not configured in DSR/SDS.</td>
</tr>
<tr>
<td></td>
<td>2. If SNMP is already configured and SNMPv3 is selected as enabled version.</td>
</tr>
</tbody>
</table>

4.2 Recovery Scenario 2 (Partial Server Outage with One NOAM Server Intact and ALL SOAMs Failed)

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

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

**Procedure 2. Recovery Scenario 2**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Workarounds</th>
<th>Gather required materials</th>
</tr>
</thead>
</table>
| 1.     | Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist. Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases:
  1. If SNMP is not configured in DSR.
  2. If SNMP is already configured and SNMPv3 is selected as enabled version. | Gather the documents and required materials listed in Required Materials. |
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>3.</th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
</table>

1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:

   ```
   http://<Primary_NOAM_VIP_IP_Address>
   ```

2. Login as the `guiadmin` user:

![Oracle System Login](image)

   Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.

---

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 2. Recovery Scenario 2

1. Navigate to **Status & Manage > HA**.

2. Click **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>ZombieDRNOAM1</td>
<td>Standby</td>
<td>Spare Observer</td>
</tr>
</tbody>
</table>

3. Set the Max Allowed HA Role option to **OOS** for the failed servers.

4. Click **OK**.

5. **Replace failed equipment**

   Work with the hardware 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/X7-2**: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings
      - **HP DL380 Gen9**: Configure HP Gen9 Server BIOS Settings

   2. Verify and/or upgrade server firmware by executing the **Upgrade Rack Mount Server Firmware** procedure from reference [8].
### Procedure 2. Recovery Scenario 2

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

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

- sdsIso (if SDS VMs are being configured)
- NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured)
- XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured)
- XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured)
- 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)

Notes:
- Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].
- Comment out SDS and DSR profile items if corresponding products are not used.
- For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9, refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].
- VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName.
- VM locations should not be changed from their RMSx format. Each RMS should correspond to a separate rack mount server.

**WARNING**

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

<table>
<thead>
<tr>
<th>18. PMAC:</th>
<th>Copy the backed up fdc file to the RMS directory</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Copy the fdconfig backup file to the RMS directory.</td>
</tr>
<tr>
<td></td>
<td>$ sudo cp /usr/TKLC/smac/etc/fdc/&lt;backup_fdc_file&gt;</td>
</tr>
<tr>
<td></td>
<td>/usr/TKLC/smac/etc/RMS/</td>
</tr>
</tbody>
</table>
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.</td>
<td><strong>PMAC:</strong> Execute the <code>config.sh</code> script</td>
</tr>
</tbody>
</table>

Execute `config.sh` against the modified backup config file.

**Note:** If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again.

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

**Example output:**

```
[sdmasc@t210541PMAC RMS]$ sudo ./config.sh rms.cfg
Validating cfg file...
Successful validation of cfg file.
Added Cabinet 101 to Fast Deployment File.
Added Zombie_TVOE1 to Fast Deployment File.
Added Zombie_TVZQ2 to Fast Deployment File.
Added xml(bond0.4) to Fast Deployment File.
Added imi(bond0.3) to Fast Deployment File.
Added rep(bond1.10) to Fast Deployment File.
Added xs11(bond1.6) to Fast Deployment File.
Added xs12(bond1.7) to Fast Deployment File.
Added xs13(bond1.8) to Fast Deployment File.
Added xs14(bond1.9) to Fast Deployment File.
Added xs15(bond1.10) to Fast Deployment File.
Added xs16(bond1.12) to Fast Deployment File.
Added xs17(bond1.13) to Fast Deployment File.
Added xs18(bond1.14) to Fast Deployment File.
Added xs19(bond1.15) to Fast Deployment File.
Added xs10(bond1.16) to Fast Deployment File.
Added xs11(bond1.17) to Fast Deployment File.
Added xs12(bond1.18) to Fast Deployment File.
Added xs13(bond1.19) to Fast Deployment File.
Added xs14(bond1.20) to Fast Deployment File.
Added xs15(bond1.21) to Fast Deployment File.
Added xs16(bond1.22) to Fast Deployment File.
Added Zombie_DSRK00M1 to Fast Deployment File.
Added Zombie_DSRK00M2 to Fast Deployment File.
Added Zombie_DSRKUNAH1 to Fast Deployment File.
Added Zombie_DSRKUNAH2 to Fast Deployment File.
Added Zombie_DS00A0M1 to Fast Deployment File.
Added Zombie_DS00A0M2 to Fast Deployment File.
Added Zombie_DS00A1M1 to Fast Deployment File.
Added Zombie_DS00A1M2 to Fast Deployment File.
Added Zombie_DS00A2M1 to Fast Deployment File.
Added Zombie_DS00A2M2 to Fast Deployment File.
Added Zombie_DS00A3M1 to Fast Deployment File.
Added Zombie_DS00A3M2 to Fast Deployment File.
```

Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml"
Configuration file validation successful.
Validation complete

Success! Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml
SUCCESS: OPERATION SUCCESS!!
```
## Procedure 2. Recovery Scenario 2

### 20. PMAC: 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 before executing the fdconfig, perform a `screen -dr` to resume the screen session in the event of a terminal timeout, etc.

### 21. PMAC GUI: Monitor the configuration

1. If not already done, establish a GUI session on the PMAC server.
2. Navigate to **Task Monitoring**.

   ![Status and Manage](image)

   ![Task Monitoring](image)

   ![Help](image)

   ![Legal Notices](image)

   ![Logout](image)

   3. Monitor the configuration to completion:

   ![Main Menu: Task Monitoring](image)

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

   ```bash
   [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
   ------------------- end -------------------
   ```

4. Restart the fdconfig after a failure has occurred and has been resolved:

```bash
$ sudo fdconfig restart --file=deploy_melbourne_20170329T202458_701b.fdcdb
```
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td><strong>PMAC:</strong> Repeat for each rack mount server configuration file</td>
</tr>
</tbody>
</table>
| 23. | **PMAC:** Back up FDC file | 1. Copy the updated fdc file to the fdc backup directory:  
\[ $ sudo \ cp \ /usr/TKLC/smac/etc/RMS/<fdc\_file> \ /usr/TKLC/smac/etc/fdc/ \]  
2. Change permissions:  
\[ $ sudo \ chmod \ 777 \ /usr/TKLC/smac/etc/fdc/<fdc\_file> \] |
| 24. | Perform CPU pinning | Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only) procedure from reference [8]. |
| 25. | **NOAM GUI:** Login  
If the failed server is not OAM, then skip to step 47. | 1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  
\[ http://<Primary\_NOAM\_VIP\_IP\_Address> \]  
2. Login as the guiadmin user: |

![Oracle System Login](image-url)
**Procedure 2. Recovery Scenario 2**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **26.** | NOAM VIP GUI: Recover standby NOAM, if needed | Install the second NOAM server:  
DSR: Execute the **Configure the Second NOAM Server** procedure, steps 1 and 3-6, from reference [8].  
SDS: Execute the **Configure the Second SDS NOAM Server** procedure, steps 1 and 3-6, from reference [8]. |
| **27.** | Install NetBackup client (optional) | If NetBackup is used, execute the **Install NetBackup Client (Optional)** procedure from reference [8]. |
| **28.** | NOAM VIP GUI: Set HA on standby NOAM | 1. Navigate to **Status & Manage > HA**.  
   ![Modifying HA attributes](image)  
   2. Click **Edit**.  
   3. Select the standby NOAM server and set it to **Active**.  
   4. Click **OK**. |
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29.</td>
<td><strong>NOAM VIP GUI:</strong> Restart DSR application</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Server.</strong></td>
</tr>
<tr>
<td></td>
<td>2. Select the recovered standby NOAM server and click <strong>Restart.</strong></td>
</tr>
</tbody>
</table>
| 30.  | **NOAM VIP GUI:** Recover query servers.  
      | SDS only. If DSR, skip to step 33.  
      | Execute the **Configuring SDS Query Servers** procedure, steps 1 and 4-7, from reference [8]. |
| 31.  | **SDS NOAM VIP GUI:** Set HA on query server.  
      | SDS only. If DSR, skip to step 33.  
      | 1. Navigate to **Status & Manage > HA.**  
      | 2. Click **Edit.**  
      | 3. Select the query server and select **Observer.**  
      | 4. Click **OK.** |
Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>32.</td>
<td>SDS NOAM VIP GUI: Restart SDS application. SDS only. If DSR, skip to step 33.</td>
</tr>
</tbody>
</table>
|     | Navigate to **Status & Manage > Server**.  
|     | 1. **Status & Manage**  
|     |   - **Network Elements**  
|     |   - **Server**  
|     |   - **HA**  
|     |   - **Database**  
|     |   - **KPIs**  
|     |   - **Processes**  
|     | 2. Select the recovered query server and click **Restart**. |
| 33. | NOAM VIP GUI: Stop replication to the C-level servers of this site. |
|     | For DSR:  
|     | Before continuing this procedure, replication to C-level servers **MUST** be inhibited at the SOAM site being recovered. Failure to inhibit replication to the working C-level servers results in the database being destroyed!  
|     | **If the spare SOAM is also present in the site and lost**, execute Appendix E Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost) to inhibit replication to working C-level servers before continuing.  
|     | **If the spare SOAM is NOT deployed in the site**, execute Appendix C Inhibit A and B Level Replication on C-level Servers to inhibit replication to working C-level servers before continuing.  
|     | For SDS,  
|     | Inhibit database replication for defective SOAM servers and DP servers associated with this SOAM network element.  
|     | NOTE: It is expected that each SOAM and subtending DP will have a DB Level of "UNKNOWN" until the SOAMs are restored.  
|     | 1. Go to the NOAMP GUI.  
|     | 2. Select **Main Menu: Status & Manage → Database** screen  
|     | 3. Filter on the SOAM Network Element name.  
|     | 4. Record the DP server hostnames (Role: MP).  
|     | 5. Click "Inhibit Replication" button for each DP server until all DP servers associated with this SOAM Network Element have been inhibited "Inhibiting" SOAM server: Click "Inhibit Replication" button for each defective SOAM servers.
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM VIP GUI: Recover active SOAM server</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>34.</td>
<td>Install the SOAM servers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>DSR:</strong> Execute the <strong>Configure the SOAM Servers</strong> procedure, steps 1-3 and 5-9, from reference [8].</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you are using NetBackup, also execute step 12.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SDS:</strong> Execute the <strong>Configure the SDS DP SOAM Servers</strong> procedure, steps 1-3 and 5-8, from reference [8].</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM VIP GUI: Set HA on the SOAM server</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>35.</td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; HA</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Edit</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Select the SOAM server and set it to <strong>Active</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM VIP GUI: Restart DSR application</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>36.</td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Server</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Select the recovered SOAM server and click <strong>Restart</strong>.</td>
<td></td>
</tr>
</tbody>
</table>
Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI:</th>
</tr>
</thead>
<tbody>
<tr>
<td>37.</td>
<td>Upload the backup SOAM database file.</td>
</tr>
<tr>
<td></td>
<td>DSR only. If SDS, skip to step 42.</td>
</tr>
</tbody>
</table>

1. Navigate to **Status & Manage > Files**.

2. Select the active SOAM server tab. Click **Upload** and select the file **SO Provisioning and Configuration** file backed up after initial installation and provisioning.

3. Click **Browse** and locate the backup file.
4. Mark the **This is a backup file** checkbox.
5. Click **Open**.
6. Click **Upload**.

The file takes a few seconds to upload depending on the size of the backup data and displays on the list of entries when it has completed the upload.
**Procedure 2. Recovery Scenario 2**

<table>
<thead>
<tr>
<th></th>
<th>Recovered SOAM GUI: Login. DSR only. If SDS, skip to step 42.</th>
</tr>
</thead>
<tbody>
<tr>
<td>38.</td>
<td>1. Establish a GUI session on the recovered SOAM server.</td>
</tr>
<tr>
<td></td>
<td>2. Open the web browser and enter a URL of:</td>
</tr>
<tr>
<td></td>
<td>http://&lt;Recovered_SOAM_IP_Address&gt;</td>
</tr>
<tr>
<td></td>
<td>3. Login as the guiadmin user:</td>
</tr>
</tbody>
</table>

![Oracle System Login Image]

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.

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 2. Recovery Scenario 2

| 39. | **Recovered SOAM GUI:** Verify the archive contents and database compatibility. DSR only. If SDS, skip to step 42. |

1. Navigate to **Status & Manage > Database**.
2. Select the **Active SOAM** server and click **Compare**.
3. Click the button for the restored database file uploaded as a part of step 27. of this procedure.

### Database Compare

![Database Compare Screenshot]

4. Verify the output window matches the screen below.

### Database Archive Compare

![Database Archive Compare Screenshot]

- **Note:** Archive Contents and Database Compatibilities must be the following:
  - **Archive Contents:** Configuration data.
  - **Database Compatibility:** The databases are compatible.

- **Note:** The following is expected output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM:
  - **Topology Compatibility**
    - The topology should be compatible minus the NODEID.

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

5. If the verification is successful, click **Back** and continue to **next step** in this procedure.
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 40. | **Recovered SOAM GUI:** Restore the database. DSR only. If SDS, skip to step 42.  

1. Select the **Active SOAM** server and click **Restore**.  
2. Select the backup provisioning and configuration file.  
   
   **Database Compare**  
   
   Select archive to compare on server:  
   Archive: backup/Backup.dsr2  
   
   ![Database Compare](image)  
   
   3. Click **OK**.  
   
   **Database Restore Confirm**  
   
   Compatible archive.  
   
   ![Database Restore Confirm](image)  
   
   4. If the Node Type Compatibility error displays, it is expected. If no other errors display, mark the **Force** checkbox and click **OK** to proceed with the DB restore.  

**Notes:**  
- After the restore has started, the user is logged out of XMI SOAM GUI since the restored topology is old data.  
- If the spare SOAM is in another network and is unreachable, the database restore cannot be done.  

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 41. | **Recovered SOAM GUI:** Monitor and confirm database restoral. DSR only. If SDS, skip to step 42.  

Wait for **5-10 minutes** for the system to stabilize with the new topology:  
Monitor the Info tab for **Success**. This indicates the restore is complete and the system is stabilized.  

**Notes:**  
- Do not pay attention to alarms until all the servers in the system are completely restored.  
- The Configuration and Maintenance information is in the same state it was when backed up during initial backup.
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Login</th>
<th></th>
</tr>
</thead>
</table>
| 42. | 1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  
   | http://<Primary_NOAM_VIP_IP_Address> |   |
|   | 2. Login as the **guiadmin** user: |   |

**Oracle System Login**

![Oracle System Login](image)

*Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.*

*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.*

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Recover the remaining SOAM servers (standby, spare)</th>
<th>DSR:</th>
</tr>
</thead>
<tbody>
<tr>
<td>43.</td>
<td>Execute the <strong>Configure the SOAM Servers</strong> procedure, steps 1-3 and 5-9, from reference [8].</td>
<td><strong>Note:</strong> If you are using NetBackup, also execute step 12.</td>
</tr>
<tr>
<td></td>
<td><strong>SDS:</strong> Execute the <strong>Configure the SDS DP SOAM Servers</strong> procedure, steps 1-3 and 5-8, from reference [8].</td>
<td></td>
</tr>
</tbody>
</table>
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.</td>
<td><strong>NOAM VIP GUI:</strong> Start replication on the recovered SOAMs, if replication is inhibited.</td>
</tr>
<tr>
<td></td>
<td>Un-Inhibit (start) replication to the recovered SOAM servers.</td>
</tr>
<tr>
<td>5.</td>
<td>Navigate to <strong>Status &amp; Manage &gt; Database</strong>.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /> <strong>Status &amp; Manage</strong> &gt; <strong>Database</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /> <strong>Status &amp; Manage</strong> &gt; <strong>Database</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /> <strong>Status &amp; Manage</strong> &gt; <strong>HA</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /> <strong>Status &amp; Manage</strong> &gt; <strong>KPIs</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /> <strong>Status &amp; Manage</strong> &gt; <strong>Processes</strong></td>
</tr>
<tr>
<td>6.</td>
<td>Click <strong>Allow Replication</strong> on the recovered SOAM servers.</td>
</tr>
<tr>
<td>7.</td>
<td>Verify the replication on all SOAMs servers is allowed. This can be done by checking <strong>Repl status</strong> column of respective server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>45.</td>
<td><strong>NOAM VIP GUI:</strong> Set HA on the recovered standby SOAM server.</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Status &amp; Manage &gt; HA</strong>.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /> <strong>Status &amp; Manage</strong> &gt; <strong>HA</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /> <strong>Status &amp; Manage</strong> &gt; <strong>KPIs</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /> <strong>Status &amp; Manage</strong> &gt; <strong>Processes</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /> <strong>Status &amp; Manage</strong> &gt; <strong>Files</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Edit</strong> at the bottom of the screen.</td>
</tr>
<tr>
<td>3.</td>
<td>Select the recovered standby SOAM server and set it to <strong>Active</strong>.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Procedure</th>
<th>NOAM VIP GUI: Restart DSR application</th>
<th>NOAM VIP GUI: Start replication on working C-level servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>46.</td>
<td>1. Navigate to Status &amp; Manage &gt; Server.</td>
<td>Un-Inhibit (start) replication to the working C-level Servers which belongs to the same site as of the failed SOAM servers.</td>
</tr>
<tr>
<td></td>
<td>2. Select the recovered NOAM server and click Restart.</td>
<td><strong>If the spare SOAM is also present in the site and lost</strong>, execute Appendix F Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost).</td>
</tr>
<tr>
<td></td>
<td><strong>If the spare SOAM is NOT deployed in the site</strong>, execute Appendix D Un-Inhibit A and B Level Replication on C-level Servers.</td>
<td><strong>If the Repl Status is set to Inhibited</strong>, click Allow Replication using this order; otherwise, if none of the servers are inhibited, skip this step and continue with the next step:</td>
</tr>
<tr>
<td>47.</td>
<td>1. Navigate to Status &amp; Manage &gt; Database.</td>
<td>- Active NOAM Server</td>
</tr>
<tr>
<td></td>
<td>2. If the Repl Status is set to Inhibited, click Allow Replication using this order; otherwise, if none of the servers are inhibited, skip this step and continue with the next step:</td>
<td>- Standby NOAM Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Active SOAM Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Standby SOAM Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Spare SOAM Server <em>(if applicable)</em> — Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Active DR NOAM Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Standby DR NOAM Server</td>
</tr>
</tbody>
</table>
|             |                                           | - MP/IPFE Servers *(if MPs are configured as active/standby, start with*
Procedure 2. Recovery Scenario 2

the active MP; otherwise, the order of the MPs does not matter

- SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only

3. Verify the replication on all the working servers is allowed. This can be done by examining the Repl Status table.

<table>
<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>

For SDS:
Allow database replication for SOAM-A and SOAM-B servers and DP servers associated with this SOAM network element.
1. Go to the NOAMP GUI.
2. Select [Main Menu: Status & Manage → Database] screen
3. Filter on the SOAM Network Element name.
4. Record the DP server hostnames (Role: MP).
5. Wait until audit becomes active on SOAM's. Allowing Replication: Click “Allow Replication” button for each newly replaced SOAM-A and SOAM-B servers
   Allowing Replication: Click "Allow Replication" button for each DP server until all DP servers associated with this SOAM Network Element have been inhibited

48. ☐ Activate PCA feature. DSR only
If you have PCA installed in the system being recovered, re-activate PCA by executing the **PCA Activation on Entire Network** procedure on the recovered standby NOAM server from [7].

49. ☐ NOAM VIP GUI: Recover the C-level server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs
   DSR:
   Execute the **Configure the MP Servers** procedure, steps 1 and 9-13, from reference [8].
   **Note:** Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.

   SDS (Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only):
   Execute the **Configure the SDS DP Servers** procedure, steps 1 and 5-8, from reference [8].
   Repeat this step for any remaining failed MP servers.
Procedure 2. Recovery Scenario 2

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 50. | **NOAM VIP GUI:** Set HA on all C-level servers | 1. Navigate to **Status & Manage -> HA.**

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

   2. Click **Edit.**

   3. For each recovered C-Level with a Max Allowed HA Role set to **OOS**, set it to **Active.**

<table>
<thead>
<tr>
<th>ZombieDAMP1</th>
<th>Active</th>
<th>The maximum desired HA Role for ZombieDAMP1</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieDAMP2</td>
<td>Spare</td>
<td>The maximum desired HA Role for ZombieDAMP2</td>
</tr>
</tbody>
</table>

   4. Click **OK.**

| 51. | **NOAM VIP GUI:** Restart DSR application on the recovered C-level servers | 1. Navigate to **Status & Manage > Server.**

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

   2. Select the recovered C-level servers and click **Restart.**
Procedure 2. Recovery Scenario 2

52. **NOAM VIP GUI:**

Start replication on all C-Level servers.

DSR only. If SDS, then skip to next step.

1. Navigate to **Status & Manage > Database.**

![Status & Manage > Database]

2. If the Repl Status is set to **Inhibited,** click **Allow Replication** using this order:
   - Active NOAMP Server
   - Standby NOAMP Server
   - Active SOAM Server
   - Standby SOAM Server
   - Spare SOAM Server **(if applicable)** — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only
   - Active DR NOAM Server
   - Standby DR NOAM Server
   - MP/IPFE Servers
   - SBRS **(if SBR servers are configured, start with the active SBR, then standby, then spare)** — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only

3. Verify the replication on all servers is allowed. This can be done by checking the **Repl Status.**

<table>
<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 (if applicable) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
</tbody>
</table>

53. **Active NOAM:**

Perform keyexchange between the active-NOAM and recovered servers

1. Establish an SSH session to the active NOAM and login as **admusr.**

2. Perform a keyexchange from the active NOAM to each recovered server:

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

**Note:** If an export server is configured, perform this step.
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>54.</th>
<th><strong>Active NOAM:</strong> Activate optional features. DSR only. If SDS, then skip to next step.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Establish an SSH session to the active NOAM and login as <em>admusr</em>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note for PCA Feature Activation:</strong></td>
</tr>
<tr>
<td></td>
<td>If you have PCA installed in the system being recovered, re-activate the PCA by executing the <strong>PCA Activation on Stand By NOAM Server</strong> procedure on the recovered standby NOAM server; and the <strong>PCA Activation on Active SOAM Server</strong> procedure on the recovered active SOAM server from [6].</td>
</tr>
</tbody>
</table>

**Notes:**
- If not all SOAM sites are recovered at this point, then repeat the activation for each “new” SOAM site that comes online.
- If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature.

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

**Note:** While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored:

```
iload#31000{S/W Fault}
```
Procedure 2. Recovery Scenario 2

| 55. | NOAM VIP GUI: Fetch and store the database report for the newly restored data and save it |

1. Navigate to Status & Manage > Database.

2. Select the active NOAM server and click Report.

The following screen displays:

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

```
Database Status Report

From: Active Network OAM&P on host ZombieNOAM1
Report Version: 8.0.0.0.0-90.9.0
User: guiadmin

General
Hostname : ZombieNOAM1
Database Birthday : 2016-07-11 11:21:50 EDT
AppWorks Database Version : 6.0
Application Database Version :

Capacities and Utilization
Disk Utilization 8.4%: 588M used of 7.0G total, 6.0G available
Memory Utilization 0.0%: used of total, 0M available
```

3. Click **Save** and save the report to your local machine.
Procedure 2. Recovery Scenario 2

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

57. NOAM VIP GUI: Verify the database states

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

<table>
<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>ZombieNOAM1</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>ZombieNOAM2</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>ZombieSOAM3</td>
<td>MP</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSS7MP2</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSS7MP1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieIPFE1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieIPFE2</td>
<td>MP</td>
<td>Active</td>
</tr>
</tbody>
</table>

2. Verify the NOAM VIP GUI:
   - Navigate to Status and Manage > HA.
   - Select the row for all of the servers.
   - Verify the HA Role is either Active or Standby:

58. NOAM VIP GUI: Verify the HA status

1. Navigate to Status and Manage > HA.
   - Select the row for all of the servers.
   - Verify 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>
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>SOAM GUI: Enable site provisioning. DSR only. If SDS, skip to step 69.</th>
<th>SOAM VIP GUI: Verify local node information. DSR only. If SDS, skip to step 69.</th>
<th>SOAM VIP GUI: Verify the peer node information. DSR only. If SDS, then skip to step 69.</th>
</tr>
</thead>
<tbody>
<tr>
<td>59.</td>
<td>- Navigate to <strong>Status &amp; Manage &gt; Database</strong>.</td>
<td>- Navigate to <strong>Diameter &gt; Configuration &gt; Local Node</strong>.</td>
<td>- Navigate to <strong>Diameter &gt; Configuration &gt; Peer Node</strong>.</td>
</tr>
<tr>
<td></td>
<td>1. Click <strong>Enable Site Provisioning</strong>.</td>
<td>1. Verify all the local nodes are shown.</td>
<td>1. Verify all the peer nodes are shown.</td>
</tr>
<tr>
<td></td>
<td>2. A confirmation window displays. Click <strong>OK</strong> to enable provisioning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>60.</td>
<td>1. Click <strong>Enable Site Provisioning</strong>.</td>
<td>2. Verify all the local nodes are shown.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. A confirmation window displays. Click <strong>OK</strong> to enable provisioning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>61.</td>
<td>1. Navigate to <strong>Diameter &gt; Configuration &gt; Local Node</strong>.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Procedure 2. Recovery Scenario 2

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

| 65. | **SOAM VIP GUI:** Enable optional features.  
DSR only. If SDS, then skip to step 69. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to <strong>Diameter &gt; Maintenance &gt; Applications.</strong></td>
</tr>
</tbody>
</table>
| | - Maintenance  
- Route Lists  
- Route Groups  
- Peer Nodes  
- Connections  
- Egress Throttle Groups  
- Applications |
| 2. | Select the optional feature application configured in step 72. |
| 3. | Click **Enable.** |
| | ![Enable, Disable, Pause updates buttons] |

| 66. | **SOAM VIP GUI:** Re-enable transports, if needed.  
DSR only. If SDS, then skip to step 69. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to <strong>Transport Manager &gt; Maintenance &gt; Transport.</strong></td>
</tr>
</tbody>
</table>
| | - Transport Manager  
- Configuration  
- Maintenance  
- Transport |
| 2. | Select each transport and click **Enable.** |
| | ![Enable, Disable, Block buttons] |
| 3. | Verify the Operational Status for each transport is **Up.** |

| 67. | **SOAM VIP GUI:** Re-enable MAPIWF application, if needed.  
DSR only. If SDS, then skip to step 69. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to <strong>SS7/Sigtran &gt; Maintenance &gt; Local SCCP Users.</strong></td>
</tr>
</tbody>
</table>
| | - SS7/Sigtran  
- Configuration  
- Maintenance  
- Local SCCP Users  
- Remote Signaling Points  
- Remote MTP3 Users  
- Linksets  
- Links |
| 2. | Click the **Enable** button corresponding to MAPIWF Application Name. |
| | ![Enable, Disable buttons] |
| 3. | Verify the SSN Status is **Enabled.** |
Procedure 2. Recovery Scenario 2

68. SOAM VIP GUI: Re-enable links, if needed. DSR only. If SDS, then skip to step 69.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to SS7/Sigtran &gt; Maintenance &gt; Links.</td>
</tr>
<tr>
<td>2.</td>
<td>Click Enable for each link.</td>
</tr>
<tr>
<td>3.</td>
<td>Verify the Operational Status for each link is Up.</td>
</tr>
</tbody>
</table>

69. SOAM VIP GUI: Examine all alarms

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to Alarms &amp; Events &gt; View Active.</td>
</tr>
<tr>
<td>2.</td>
<td>Examine all active alarms and refer to the on-line help on how to address them.</td>
</tr>
<tr>
<td></td>
<td>If needed, contact My Oracle Support (MOS).</td>
</tr>
</tbody>
</table>

70. NOAM VIP GUI: Examine all alarms

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to Alarms &amp; Events &gt; View Active.</td>
</tr>
<tr>
<td>2.</td>
<td>Examine all active alarms and refer to the on-line help on how to address them.</td>
</tr>
<tr>
<td></td>
<td>If needed, contact My Oracle Support (MOS).</td>
</tr>
</tbody>
</table>
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Details</th>
</tr>
</thead>
</table>
| 71. | NOAM VIP: Verify all servers in topology are accessible (RADIUS only) | If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.  
1. Establish an SSH session to the NOAM VIP and login as **admusr**.  
2. Check if all the servers in the topology are accessible:  
   ```bash  
   $ /usr/TKLC/dpi/bin/  
   $ ./sharedKrevo -checkAccess  
   ```  
   Example output:  
   ```bash  
   [admusr@NOAM-2 bin]$ ./sharedKrevo -checkAccess  
   FIPS integrity verification test failed.  
   1450723403: [INFO] 'NOAM-1' is accessible.  
   FIPS integrity verification test failed.  
   1450723403: [INFO] 'SOAM-1' is accessible.  
   FIPS integrity verification test failed.  
   1450723403: [INFO] 'SOAM-2' is accessible.  
   FIPS integrity verification test failed.  
   1450723404: [INFO] 'IPFE' is accessible.  
   FIPS integrity verification test failed.  
   1450723404: [INFO] 'MP-2' is accessible.  
   FIPS integrity verification test failed.  
   1450723404: [INFO] 'MP-1' is accessible.  
   [admusr@NOAM-2 bin]$  
   ```  
   **Note:** If any server is not accessible, stop and contact My Oracle Support (MOS). |
| 72. | NOAM VIP: Copy key file to all the servers in topology (RADIUS only) | If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.  
1. Check if existing key file on active NOAM (the NOAM, which is intact and was not recovered) server is valid:  
   ```bash  
   $ cd /usr/TKLC/dpi/bin/  
   $ ./sharedKrevo -validate  
   ```  
   Example output: |
Procedure 2. Recovery Scenario 2

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

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

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

Example output:

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

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

Example output:
Procedure 2. Recovery Scenario 2

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>73.</td>
<td>Back up and archive all the databases from the recovered system</td>
<td>Execute Appendix A DSR Database Backup to back up the Configuration databases.</td>
</tr>
<tr>
<td>74.</td>
<td>Recover IDIH</td>
<td>If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.</td>
</tr>
</tbody>
</table>

4.3 Recovery Scenario 3 (Partial Server Outage with All NOAM Servers Failed and One SOAM Server Intact)

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

- Recover **Active NOAM** server by recovering base hardware, software, and the database
  - Recover the base hardware
  - Recover the software
  - Recover the database
- Recover **NOAM servers** by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover **Query Server** (if needed) by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover any failed **SOAM and MP/DP servers** by recovering base hardware and software
  - Recover the base hardware
  - Recover the software

Note: If any errors display, stop and contact My Oracle Support (MOS).
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>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Gather required materials</td>
</tr>
<tr>
<td>2.</td>
<td>Create a backup directory, if needed</td>
</tr>
<tr>
<td>3.</td>
<td>Replace failed equipment</td>
</tr>
<tr>
<td>4.</td>
<td>Recover PMAC and PMAC TVOE Host: Configure BIOS settings and update firmware</td>
</tr>
<tr>
<td>5.</td>
<td>PMAC, TVOE Hosts, and Switch Recovery: Backups available</td>
</tr>
<tr>
<td>6.</td>
<td>PMAC, TVOE Hosts, and Switch Recovery: Backups NOT available</td>
</tr>
</tbody>
</table>

#### Procedure 3.1: Gather required materials
Gather the documents and required materials listed in the Required Materials section.

#### Procedure 3.2: Create a backup directory, if needed
Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.

#### Procedure 3.3: Replace failed equipment
HW vendor to replace the failed equipment.

#### Procedure 3.4: Recover PMAC and PMAC TVOE Host: Configure BIOS settings and update firmware

1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:
   - HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings
   - HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings

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

#### Procedure 3.5: PMAC, TVOE Hosts, and Switch Recovery: Backups available
This step assumes TVOE and PMAC backups are available. If backups are NOT available, skip this step.

1. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.
2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup.
3. Proceed to step 7.

#### Procedure 3.6: PMAC, TVOE Hosts, and Switch Recovery: Backups NOT available
This step assumes TVOE and PMAC backups are NOT available. If the TVOE and PMAC have already been restored, skip this step.

1. Execute the Install and Configure TVOE on First RMS (PMAC Host) procedure from reference [8].
2. Execute the Install PMAC procedure from reference [8].
3. Execute the Initialize the PMAC Application section from reference [8].
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 7.   | Recovery failed Cisco 4948 aggregation switches (HP DL380 only)  
Recover failed Cisco 4948 aggregation switches, if needed:  
1. Back up available configuration files. Refer to Appendix C  
Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only) to recover failed Cisco 4948 aggregation switches.  
2. Back up configuration files NOT available. Execute **Configure Cisco 4948E-F Aggregation Switches (HP DL 380 Gen 8 Only)** section from reference [8]. |
| 8.   | Configure PMAC (no backup)  
If PMAC backup was NOT restored in step 5, execute this step; otherwise skip this step.  
Execute the **Configure PMAC Server (NetBackup Only)** and **Add RMS to the PMAC Inventory** sections from reference [8]. |
| 9.   | Install/Configure additional rack mount servers  
1. Execute the **Install TVOE on Additional Rack Mount Servers** procedure from reference [8].  
2. **If backups are available**, restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers. **If backups are NOT available**, execute the **Configure TVOE on Additional Rack Mount Servers** procedure from reference [8]. |
| 10.  | Configure BIOS settings and update firmware on additional rack mount servers  
1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:  
   - HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings  
   - HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings  
2. Verify and/or upgrade server firmware by executing the **Upgrade Rack Mount Server Firmware** procedure from reference [8]. |
| 11.  | Determine VM Placement and Socket Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 only)  
HP DL380 GEN 8, skip this step.  
Determine VM placement and pinning by following:  
1. From this document, section 3.1, item 14, to determine the VM placement; and  
2. In reference [8], Appendix S VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1 Gbps NICs) and CPU Pinning in HP DL380 Gen 9 (Onboard 1 Gbps NICs) for Pinning Information on HP DL380 Gen 9. |
| 12.  | Deploy redundant PMAC, if required  
Refer to the **Deploy Redundant PMAC (Optional)** procedure to re-deploy and configure any redundant PMACs previously configured. |
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th></th>
<th>PMAC:</th>
<th></th>
</tr>
</thead>
</table>
| 13 | Determine if the fdconfig file exists from the initial deployment | 1. Type: 

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

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

*Note:* There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS.

<table>
<thead>
<tr>
<th></th>
<th>PMAC:</th>
<th></th>
</tr>
</thead>
</table>
| 14 | Create fdconfig backup file, if it does not already exist | Execute this step ONLY if the fdconfig backup file does NOT exist.

1. Create the needed file(s) by executing the Virtual Machine/Network Fast Deployment section from reference [8].

**WARNING**

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

2. Skip to step 23. if this step was executed.

<table>
<thead>
<tr>
<th></th>
<th>PMAC:</th>
<th></th>
</tr>
</thead>
</table>
| 15 | Load ISOs into PMAC, if not done already | If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the Virtual Machine/Network Fast Deployment section from reference [8].

<table>
<thead>
<tr>
<th></th>
<th>PMAC:</th>
<th></th>
</tr>
</thead>
</table>
| 16 | Edit/Update configuration file | Edit the fdconfig file to include only the required/failed servers.

*Notes:*
- Comment out configuration items that are not needed.
- Create a separate configuration file for EACH rack mount server being deployed.
- The Cabinet ID in the config file needs to match the cabinet already defined in PMAC.

The following items are mandatory:
- `siteName`
- `tpdIso`
- `dsrIso` (if DSR VMs are being configured)
- `sdsIso` (if SDS VMs are being configured)
- NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured)
- XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured)
- XMISSUBNETMASK (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)
Procedure 3. Recovery Scenario 3

- SDSNOAM1XMIIIPADDRESS (if SDSNOAM1 is being configured)
- SDSNOAM2XMIIIPADDRESS (if SDSNOAM2 is being configured)
- SDSDRNOAM1XMIIIPADDRESS (if SDSDRNOAM1 is being configured)
- SDSDRNOAM2XMIIIPADDRESS (if SDSDRNOAM2 is being configured)

**Notes:**
- Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].
- Comment out SDS and DSR profile items if corresponding products are not used.
- For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9: Refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].
- VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName.
- VM locations should not be changed from their RMSx format. Each RMS should correspond to a separate rack mount server.

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

17. **PMAC:** Copy the backed up fdc file to the RMS directory

   Copy the fdconfig backup file to the RMS directory.

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

18. PMAC: Execute the config.sh script

Execute `config.sh` against the modified backup config file.

**Note:** If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again.

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

Example output:

```
Validating cfg files...
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 xml(bond0.4) to Fast Deployment File.
Added imi(bond0.5) to Fast Deployment File.
Added rep(bond1.10) to Fast Deployment File.
Added xsi1(bond1.6) to Fast Deployment File.
Added xsi2(bond1.7) to Fast Deployment File.
Added xsi3(bond1.8) to Fast Deployment File.
Added xsi4(bond1.9) to Fast Deployment File.
Added xsi6(bond1.10) to Fast Deployment File.
Added xsi16(bond1.12) to Fast Deployment File.
Added xsi17(bond1.13) to Fast Deployment File.
Added xsi18(bond1.14) to Fast Deployment File.
Added xsi19(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_DSRK0AM1 to Fast Deployment File.
Added Zombie_DSRK0AM2 to Fast Deployment File.
Added Zombie_DSRK0UNAM1 to Fast Deployment File.
Added Zombie_DSRK0UNAM2 to Fast Deployment File.
Added Zombie_DSRK0UNAM1 to Fast Deployment File.
Added Zombie_DSRK0UNAM2 to Fast Deployment File.
Added Zombie_DSRK0UNAM1 to Fast Deployment File.
Added Zombie_DSRK0UNAM2 to Fast Deployment File.
Added Zombie_DSRK0UNAM1 to Fast Deployment File.
Added Zombie_DSRK0UNAM2 to Fast Deployment File.
Added Zombie_DSRK0UNAM1 to Fast Deployment File.
Added Zombie_DSRK0UNAM2 to Fast Deployment File.
Added Zombie_DSRK0UNAM1 to Fast Deployment File.
Added Zombie_DSRK0UNAM2 to Fast Deployment File.
Added Zombie_DSRK0UNAM1 to Fast Deployment File.
Added Zombie_DSRK0UNAM2 to Fast Deployment File.
Added Zombie_DSRK0UNAM1 to Fast Deployment File.
Added Zombie_DSRK0UNAM2 to Fast Deployment File.
Added Zombie_DSRK0UNAM1 to Fast Deployment File.
Added Zombie_DSRK0UNAM2 to Fast Deployment File.
Added Zombie_DSRK0UNAM1 to Fast Deployment File.
Added Zombie_DSRK0UNAM2 to Fast Deployment File.
Added Zombie_DSRK0UNAM1 to Fast Deployment File.
Added Zombie_DSRK0UNAM2 to Fast Deployment File.
Added Zombie_DSRK0UNAM1 to Fast Deployment File.
Added Zombie_DSRK0UNAM2 to Fast Deployment File.
Added Zombie_DSRK0UNAM1 to Fast Deployment File.
Added Zombie_DSRK0UNAM2 to Fast Deployment File.
Added Zombie_DSRK0UNAM1 to Fast Deployment File.
Added Zombie_DSRK0UNAM2 to Fast Deployment File.
```

Example output:

```
Validating Fast Deployment File......
Validation configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml"
Configuration file validation successful.
Validation complete.
SUCCESS: OPERATION SUCCESS!!
```

[admnc@Z010441PMAC ~]$
Procedure 3. Recovery Scenario 3

19. **PMAC**: Execute fast deployment

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

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

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

20. **PMAC GUI**: Monitor the configuration

   1. If not already done, establish a GUI session on the PMAC server.
   2. Navigate to **Task Monitoring**.
   3. Monitor the configuration to completion:

   ![Main Menu: Task Monitoring](image)

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

   ```
   [admusr@melbourne-pmac-1 fdconfig]$ sudo fdconfig dumpsteps --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 11 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

   4. Restart the fdconfig after a failure has occurred and has been resolved:

   ```
   [admusr@melbourne-pmac-1 fdconfig]$ sudo fdconfig restart --file=deploy_melbourne_20170329T202458_701b.fdcdb
   ```
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>21. PMAC: Repeat for each rack mount server configuration file</td>
<td>Repeat steps 13.-20. for each rack mount server/configuration file, if required.</td>
<td></td>
</tr>
</tbody>
</table>
| 22. PMAC: Back up FDC file | 1. 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/
   ```  
   2. Change permissions:  
   
   ```bash
   $ sudo chmod 777 /usr/TKLC/smac/etc/fdc/<fdc_file>
   ``` |
| 23. Perform CPU pinning | Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only) procedure from reference [8]. |
| 24. Obtain latest database backup and network configuration data | 1. Obtain the most recent database backup file from external backup sources (for example, file servers) or tape backup sources.  
   2. Obtain most recent RADIUS shared secret encryption key from the DpiKf.bin.encr file on external backup sources (only when the RADIUS key revocation MOP has been executed on the system).  
   3. From required materials list in the Required Materials section, use the site survey documents and Network Element report (if available) to determine network configuration data. |
| 25. Execute DSR installation procedure for the first NOAM | Verify the networking data for network elements.  

**Notes**  
- Use the backup copy of network configuration data and site surveys from step 2.  
- SDS disaster recovery actions can and should be worked simultaneously to allow faster recovery of the complete solution (that is, stale DB on DP servers do not receive updates until SDS-SOAM servers are recovered). The following steps accommodate both DSR and SDS disaster recovery steps.  

**Important:** While creating the first NOAMs in this step, it is important that the server hostname is the same as one of the NOAM hostnames used prior to the disaster.  

**DSR:**  
1. Configure the first NOAM server by executing the **Configure First NOAM NE and Server** procedure from reference [8].  
2. Configure the NOAM server group by executing the **Configure the NOAM Server Group** procedure from reference [8].  

**SDS:**  
3. Configure the first SDS NOAM server by executing **Configure First SDS NOAM NE and Server** procedure from reference [8].  
4. Configure the SDS NOAM server group by executing the **Configure the SDS NOAM Server Group** procedure from reference [8].  
5. Skip to step 31.
Procedure 3. Recovery Scenario 3

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

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

2. Login as the **guiadmin** user:

   ![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 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>27.</td>
<td>NOAM GUI: Upload the backup database file. DSR only. If SDS, skip to step 31.</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to Status &amp; Manage &gt; Files.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the active NOAM server.</td>
</tr>
<tr>
<td>3.</td>
<td>Click Upload and select the <strong>NO Provisioning and Configuration</strong> file backed up after initial installation and provisioning.</td>
</tr>
</tbody>
</table>
| 4. | Click **Browse** and locate the backup file.  
**Note:** If there is no backup file, refer to Appendix L Backup Directory to create the backup directory. |
| 5. | Click **Open**. |
| 6. | Mark the **This is a backup file** checkbox. |
| 7. | Click **Upload**. |

The file takes a few seconds to upload depending on the size of the backup data. The file is visible on the list of entries after the upload is complete.
### Procedure 3. Recovery Scenario 3

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 28 | **NOAM GUI:**  
**Disable provisioning.**  
DSR only. If SDS, skip to step 31. |
|   | **1.** Navigate to **Status & Manage > Database.** |
|   | - **Status & Manage**  
- **Network Elements**  
- **Server**  
- **HA**  
- **Database**  
- **KFs**  
- **Processes**  
- **Tasks**  
- **Files** |
|   | **2.** Click **Disable Provisioning.** |
|   | ![Disable Provisioning Button](image)  
**Disable Provisioning**  
**Report**  
**Inhibit/Allow** |
|   | **3.** Click **OK** to disable Provisioning.  
**Disable provisioning.**  
**Are you sure?** |
|   | ![OK Button](image)  
**OK**  
**Cancel** |
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>29.</th>
<th><strong>NOAM GUI:</strong> Verify the archive contents and database compatibility. DSR only. If SDS, skip to step 31.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select the active NOAM server and click <strong>Compare</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Click the button for the restored database file uploaded as a part of step 27. of this procedure.</td>
</tr>
<tr>
<td>3.</td>
<td><strong>Verify</strong> the output window matches the screen below.</td>
</tr>
</tbody>
</table>

### Note:
- A database mismatch regarding the Topology Compatibility and possibly User compatibility (due to authentication) display. These warnings are expected. If these are the only mismatches, proceed; otherwise, stop and contact My Oracle Support (MOS) to ask for assistance.

### Database Archive Compare

<table>
<thead>
<tr>
<th>Archive Contents</th>
<th>Configuration data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Compatibility</td>
<td>The databases are compatible.</td>
</tr>
<tr>
<td>Node Type Compatibility</td>
<td>The node types are compatible.</td>
</tr>
<tr>
<td><strong>Topology Compatibility</strong></td>
<td><strong>THE TOPOLOGY IS NOT COMPATIBLE. CONTACT ORACLE CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE.</strong></td>
</tr>
</tbody>
</table>
- Server A1580.952 on network XHI is in the current topology but not the selected backup file. |
- Server A1560.952 on network XHI is in the current topology but not the selected backup file. |
- Server A1560.258 on network XHI is in the selected backup file but not the current topology. |
- Server A1534.911 on network XHI is in the selected backup file but not the current topology. |
- Server C0421.239 on network XHI is in the selected backup file but not the current topology. |

### Note:
- Archive Contents and Database Compatibilities must be the following:
  - **Archive Contents:** Configuration data.
  - **Database Compatibility:** The databases are compatible.

### Note:
- The following is expected output for Topology Compatibility Check since we are restoring from an existing backed up database to a database with just one NOAM:
  - **Topology Compatibility**
    - The topology should be compatible minus the NODEID.

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

4. If the verification is successful, click **Back** and continue to **next step** in this procedure.
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.</td>
<td><strong>Active NOAM:</strong> Restore the database. DSR only. If SDS, skip to step 31.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> After the restore has started, the user is logged out of the XMI NO GUI since the restored topology is old data.</td>
</tr>
</tbody>
</table>
| 31.  | 1. From **Status & Manage > Database.**  
   | 2. Select the active NOAM server and click **Restore.**  
   | ![Restore](image)  
   | 3. Select the proper backup provisioning and configuration file.  
   | ![Select archive to Restore on server:](image)  
   | 4. Click **OK.**  
   | 5. If you get errors related to the warnings highlighted in the previous step, then it is expected. If no other errors display, then mark the **Force** checkbox and click **OK** to proceed with the DB restore.  
   | ![Database Restore Confirm](image)  
   | **Note:** After the restore has started, the user is logged out of the XMI NO GUI since the restored topology is old data.  
   | 6. Go to step 37. |
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>SDS NOAM:</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| 31.  | SDS NOAM: Transfer SDS configuration and provisioning backup database files. SDS only. If DSR, skip to step 37. | Using the IP of the recovered SDS NOAM, transfer the uncompressed backup database files to the `/var/TKLC/db/filemgmt` directory. **Linux:**  
  1. From the command line of a Linux machine, copy the configuration backup file to the SDS NOAM guest:  
     ```bash  
     # scp <path_to_configuration_db_file> admusr@<SDS_NOAM_IP>:/var/TKLC/db/filemgmt  
     ```  
  2. From the command line of a Linux machine, copy the provisioning backup file to the SDS NOAM guest:  
     ```bash  
     # scp <path_to_provisioning_db_file> admusr@<SDS_NOAM_IP>:/var/TKLC/db/filemgmt  
     ```  
  where `<path_to_db_file>` is the path to the backup database file on the local system and `<SDS_NOAM_IP>` is the recovered SDS NOAM IP address. **Windows:**  
  Use WinSCP to copy the backup database files into the `/var/TKLC/db/filemgmt` directory. Refer to the Using WinSCP procedure in reference [9] to copy the backup image to the customer system. |
| 32.  | SDS NOAM: Login. SDS only. If DSR, skip to step 37. | Establish an SSH session to the SDS active NOAM XMI IP address and login as admusr. |
| 33.  | SDS NOAM: Stop running applications. SDS only. If DSR, skip to step 37. | Issue the following command to stop running applications. Leave database running:  
  ```bash  
  $ sudo prod.stop --ignore-cap  
  ```  
  **Note:** This step may take several minutes to complete. |
| 34.  | SDS NOAM: Restore configuration database. SDS only. If DSR, skip to step 37. | Restore the configuration DB by executing the following command:  
  ```bash  
  $ sudo idb.restore -n -t /var/TKLC/db/filemgmt -v <full path to configuration archive file name>  
  ``` |
| 35.  | SDS NOAM: Restore provisioning database. SDS only. If DSR, skip to step 37. | Refer to Appendix I Restore Provisioning Database to restore the provisioning database. |
| 36.  | SDS NOAM: Start running applications. SDS only. If DSR, skip to step 37. | Start the SDS application by executing the following command:  
  ```bash  
  $ sudo prod.start  
  ``` |
Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Steps</th>
</tr>
</thead>
</table>
| 37. NOAM VIP GUI: Login | 1. **Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server.** Open the web browser and enter a URL of: 

   \[
   \text{http://<Primary_NOAM_VIP_IP_Address>}
   \]

   2. **Login as the guiadmin user:**

   ![Oracle System Login](image)

| 38. NOAM VIP GUI: Monitor and confirm database restore | 1. **Wait for 5-10 minutes** for the system to stabilize with the new topology:  

2. **Monitor the Info tab for Success.** This indicates the restore is complete and the system is stabilized.

   Ignore these alarms for NOAM and MP servers until all the servers are configured:

   - Alarms with Type Column as REPL, COLL, HA (with mate NOAM), DB (about Provisioning Manually Disabled).

   **Notes:**

   - Do not pay attention to alarms until all the servers in the system are completely restored.
   - The Configuration and Maintenance information is in the same state it was when backed up during initial backup. |
Procedure 3. Recovery Scenario 3

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>39.</td>
<td><strong>Active NOAM:</strong> Set failed servers to OOS</td>
</tr>
<tr>
<td>40.</td>
<td><strong>NOAM VIP GUI:</strong> Recover standby NOAM</td>
</tr>
<tr>
<td>41.</td>
<td>Install NetBackup client (optional)</td>
</tr>
</tbody>
</table>

1. Navigate to **Status & Manage > HA.**
   - Status & Manage
     - Network Elements
     - Server
     - HA
     - Database
     - KPIs
     - Processes
   - Click **Edit.**
   - Set the Max Allowed HA Role option to **OOS** for the failed servers.
   - Click **OK.**

2. Install the second NOAM server:
   - **DSR:** Execute the **Configure the Second NOAM Server** procedure, steps 1, 3-6, from reference [8].
   - **SDS:** Execute the **Configure the Second SDS NOAM Server** procedure, steps 1, 3-6, from reference [8].

3. If NetBackup is used, execute the **Install NetBackup Client (Optional)** procedure from reference [8].
## Procedure 3. Recovery Scenario 3

### 42. NOAM VIP GUI: Set HA on standby NOAM

1. Navigate to **Status & Manage > HA**.
   - ![Status & Manage](image1.png)
   - **Modifying HA attributes**
     - | Hostname     | Max Allowed HA Role | Description |
       |--------------|---------------------|-------------|
       | ZombieNOAM1  | Active              | The maximum |
       | ZombieNOAM2  | Active              | The maximum |
       | ZombieNOAM3  | Standby             | The maximum |

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

### 43. NOAM VIP GUI: Restart DSR application

1. Navigate to **Status & Manage > Server**.
   - ![Status & Manage](image2.png)

2. Select the recovered standby NOAM server and click **Restart**.
## Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th></th>
<th>Active NOAM: Correct the recognized authority table</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.</td>
<td>Establish an SSH session to the active NOAM and login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td>Execute this command:</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo top.setPrimary</code></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>

|   | NOAM VIP GUI: Perform Keyexchange with remote import server. SDS only. If DSR, skip to step 47. |
| 45. | Navigate to **SDS > Configuration > Options**.         |
|    | Unmark the **Remote Import Enabled** checkbox.         |
|    | Click **Apply**.                                        |
|    | **Note:** Navigate to **SDS > Configuration > Options** again to clear the banner. |
|    | Enter the **Remote Import Password**.                   |
|    | Click **Apply**.                                        |
|    | **Note:** Navigate to **SDS > Configuration > Options** again to clear the banner. |
|    | Mark the **Remote Import Enabled** checkbox.            |
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM VIP GUI:</th>
</tr>
</thead>
<tbody>
<tr>
<td>46.</td>
<td>Repeat for remote export server. SDS only. If DSR, skip to step 47.</td>
</tr>
<tr>
<td></td>
<td><strong>Repeat step 45. for the remote export server.</strong></td>
</tr>
<tr>
<td>47.</td>
<td>Perform Keyexchange with export server</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to Administration &gt; Remote Servers &gt; Data Export.</td>
</tr>
<tr>
<td></td>
<td><strong><a href="#">Diagram of NOAM VIP GUI interface</a></strong></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>SSH Key Exchange</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Type the <strong>Password</strong> and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>48.</td>
<td>Recover query servers. SDS only. If DSR, skip to step 51.</td>
</tr>
<tr>
<td></td>
<td><strong>Execute the Configuring SDS Query Servers procedure, steps 1, 4-7, from reference [8].</strong></td>
</tr>
</tbody>
</table>
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>49.</td>
<td><strong>SDS NOAM VIP GUI:</strong> Set HA on query server. SDS only. If DSR, skip to step 51.</td>
</tr>
</tbody>
</table>
| 1.   | Navigate to Status & Manage > HA.  
|      |   - Status & Manage  
|      |     - Network Elements  
|      |     - Server  
|      |     - HA  
|      |     - Database  
|      |     - KPIs  
|      |     - Processes  
|      |     - Tasks  
|      |     - Files  
| 2.   | Click **Edit**.  
| 3.   | Select the query server and select **Observer**.  
| 4.   | Click **OK**.  
| 50.  | **SDS NOAM VIP GUI:** Restart SDS application. SDS only. If DSR, skip to step 51. |
| 1.   | Navigate to Status & Manage > Server.  
|      |   - Status & Manage  
|      |     - Network Elements  
|      |     - Server  
|      |     - HA  
|      |     - Database  
|      |     - KPIs  
|      |     - Processes  
| 2.   | Select the recovered query server and click **Restart**.  
| 51.  | **NOAM VIP GUI:** Recover the remaining SOAM servers (standby, spare) |
| DSR: | Execute the **Configure the SOAM Servers** procedure, steps 1-3 and 5-9, from reference [8].  
| Note: | If you are using NetBackup, also execute step 12.  
| SDS: | Execute the **Configure the SDS DP SOAM Servers** procedure, steps 1-3 and 5-8, from reference [8].  

### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>52.</strong></td>
<td><strong>NOAM VIP GUI:</strong> Set HA on SOAM server</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Status &amp; Manage &gt; HA.</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Status &amp; Manage</strong> &gt; <strong>Network Elements</strong> &gt; <strong>Server</strong> &gt; <strong>HA</strong> &gt; <strong>Tasks</strong> &gt; <strong>Data</strong> &gt; <strong>Files</strong></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Edit.</strong></td>
</tr>
<tr>
<td></td>
<td>3. Select the SOAM server and set it to <strong>Active.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Diagram" /></td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>OK.</strong></td>
</tr>
<tr>
<td><strong>53.</strong></td>
<td><strong>NOAM VIP GUI:</strong> Set HA on the SOAM server</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Status &amp; Manage &gt; HA.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Diagram" /></td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Edit.</strong></td>
</tr>
<tr>
<td>3.</td>
<td>Select the SOAM server and set it to <strong>Active.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Diagram" /></td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>OK.</strong></td>
</tr>
</tbody>
</table>
Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 54. | **NOAM VIP GUI:** Restart DSR application  
   1. Navigate to **Status & Manage > Server.**  
   2. Select the recovered SOAM server and click **Restart.** |
| 55. | Activate PCA feature. DSR only. If SDS, skip this step.  
   If you have PCA installed in the system being recovered, re-activate PCA by executing the **PCA Activation on Active NOAM Network** procedure on the recovered active NOAM server and the **PCA Activation on Stand By SOAM Network** procedure on the recovered standby SOAM from reference [7]. |
| 56. | **NOAM VIP GUI:** Recover the C-level servers (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs  
   **DSR:** Execute the **Configure the MP Servers** procedure, steps 1 and 9-13, from reference [8].  
   **Note:** Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.  
   **SDS:** Execute the **Configure the SDS DP Servers** procedure, steps 1 and 5-8, from reference [8].  
   Repeat this step for any remaining failed MP servers. |
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>57.</td>
<td>NOAM VIP GUI: Set HA on all C-level servers</td>
</tr>
</tbody>
</table>
|      | 1. Navigate to **Status & Manage > HA**.  
|      | ![Status & Manage menu](image)  
|      | - **Network Elements**  
|      | - **Server**  
|      | - **HA**  
|      | - **Database**  
|      | - **KPIs**  
|      | - **Processes**  
|      | 2. Click **Edit**.  
|      | 3. For each server whose Max Allowed HA Role is set to OOS, set it to **Active**.  
|      | ![ZombieDAMP1 and ZombieDAMP2 settings](image)  
|      | 4. Click **OK**. |
| 58. | NOAM VIP GUI: Restart DSR application on recovered C-level servers |
|      | 1. Navigate to **Status & Manage > Server**.  
|      | ![Status & Manage menu](image)  
|      | 2. Select the recovered C-level servers and click **Restart**. |
| 59. | Active NOAM: Perform keyexchange between the active-NOAM and recovered servers |
|      | 1. Establish an SSH session to the active NOAM, login as **admusr**.  
|      | 2. Perform a keyexchange from the active NOAM to each recovered server:  
|      | `$ keyexchange admusr@<Recovered Server Hostname>`  
|      | **Note:** If an export server is configured, perform this step. |
## Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th></th>
<th><strong>Active NOAM:</strong> Activate optional features. DSR only. If SDS, then skip to next step.</th>
</tr>
</thead>
<tbody>
<tr>
<td>60.</td>
<td>Establish an SSH session to the active NOAM and login as <code>admusr</code>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note for PCA Feature Activation:</strong></td>
</tr>
<tr>
<td></td>
<td>If you have PCA installed in the system being recovered, re-activate the PCA by executing the <strong>PCA Activation on Active NOAM Server</strong> procedure on recovered active NOAM server and the <strong>PCA Activation on Standby SOAM Server</strong> procedure on the recovered standby SOAM server from [6].</td>
</tr>
<tr>
<td></td>
<td><strong>Notes:</strong></td>
</tr>
<tr>
<td></td>
<td>• If not all SOAM sites are recovered at this point, then repeat the activation for each “new” SOAM site that comes online.</td>
</tr>
<tr>
<td></td>
<td>• If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature.</td>
</tr>
<tr>
<td></td>
<td>Refer to section 1.5 Optional Features to activate any features that were previously activated.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored:</td>
</tr>
<tr>
<td></td>
<td><code>iload#31000{S/W Fault}</code></td>
</tr>
</tbody>
</table>
## Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>61.</td>
<td><strong>NOAM VIP GUI:</strong> Fetch and store the database report for the newly restored data and save it</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Status &amp; Manage &gt; Database.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Status &amp; Manage" /></td>
</tr>
<tr>
<td></td>
<td><strong>Network Elements</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Server</strong></td>
</tr>
<tr>
<td></td>
<td><strong>HA</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Database</strong></td>
</tr>
<tr>
<td></td>
<td><strong>KPIs</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Processes</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Select the active NOAM server and click <strong>Report.</strong></td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>Save</strong> and save the report to your local machine.</td>
</tr>
</tbody>
</table>
**Rack Mount Server Disaster Recovery Guide**

**Procedure 3. Recovery Scenario 3**

<table>
<thead>
<tr>
<th>62.</th>
<th>Active NOAM: Verify replication between servers</th>
</tr>
</thead>
</table>

1. Log into the active NOAM as *admusr* using SSH terminal.
2. Execute this command:

```
$ sudo irepstat -m
```

**Example output:**

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

63. NOAM VIP GUI: Verify the database states

1. Navigate to Status & Manager > Database.

   - Network Elements
   - Server
   - HA
   - Database
   - KPIs
   - Processes

2. Verify the OAM Max HA Role is either Active or Standby for NOAM and SOAM; Application Max HA Role for MPs is Active; and status is Normal:

<table>
<thead>
<tr>
<th>Network Element</th>
<th>Server</th>
<th>Role</th>
<th>OAM Max HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieDRNNOAM</td>
<td>ZMBNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZMBNOAM2</td>
<td>Network OAM&amp;P</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZMBSOAM2</td>
<td>System OAM</td>
<td>N/A</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZMBNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZMBSOAM1</td>
<td>System OAM</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM</td>
<td>ZMBDRNOAM2</td>
<td>Network OAM&amp;P</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZMBSOAM2</td>
<td>System OAM</td>
<td>N/A</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZMBSS7MP2</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZMBSS7MP1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZMBPFE1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZMBPFE2</td>
<td>MP</td>
<td>Active</td>
</tr>
</tbody>
</table>

64. NOAM VIP GUI: Verify the HA status

1. Navigate to Status and Manage > HA.

   - Network Elements
   - Server
   - HA
   - Database
   - KPIs
   - Processes
   - Tasks
   - Files

2. Select the row for all of the servers.

3. Verify 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>ZombieDRNNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNNOAM2</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>Active</td>
</tr>
</tbody>
</table>
## Procedure 3. Recovery Scenario 3

### 65. NOAM GUI: Enable provisioning

1. Navigate to **Status & Manage > Database**.
   - Status & Manage
     - Network Elements
     - Server
     - HA
     - Database
     - KPIs
     - Processes
     - Tasks
     - Files

2. Click **Enable Provisioning**.

3. Click **OK**.

### 66. SOAM GUI: Enable site provisioning. DSR only. If SDS, then skip to step 75.

1. Navigate to **Status & Manage > Database**.
   - Status & Manage
     - Network Elements
     - Server
     - HA
     - Database
     - KPIs
     - Processes
     - Tasks
     - Files

2. Click **Enable Site Provisioning**.

3. Click **OK**.

### 67. SOAM VIP GUI: Verify the peer node information. DSR only. If SDS, then skip to step 75.

1. Navigate to **Diameter > Configuration > Peer Node**.
   - Diameter
     - Configuration
       - Capacity Summary
       - Connection Capacity
       - Application Ids
       - CEX Parameters
       - Command Codes
       - Configuration Sets
       - Local Nodes
       - Peer Nodes

2. Verify all the peer nodes are shown.
### Procedure 3. Recovery Scenario 3

#### 68. SOAM VIP GUI:
- Verify the connections information.
  - DSR only. If SDS, then skip to step 75.

1. Navigate to Diameter > Configuration > Connections.
   - **Diameter**
     - **Configuration**
       - **Capacity Summary**
       - **Connection Capacity Dash**
       - **Application Ids**
       - **CEX Parameters**
       - **Command Codes**
     - **Configuration Sets**
       - **Local Nodes**
       - **Peer Nodes**
       - **Peer Node Groups**
       - **Connections**

2. Verify all the connections are shown.

#### 69. MP Servers:
- Disable SCTP Auth Flag (DSR only).
  - DSR only. If SDS, then skip to step 75.

   For SCTP connections without DTLS enabled, refer to the Enable/Disable DTLS (SCTP Diameter Connections Only) section in reference [8]. Execute this procedure on all failed MP servers.

#### 70. SOAM VIP GUI:
- Enable connections, if needed.
  - DSR only. If SDS, then skip to step 75.

1. Navigate to Diameter > Maintenance > Connections.
   - **Maintenance**
     - **Route Lists**
     - **Route Groups**
     - **Peer Nodes**
     - **Connections**

2. Select each connection and click **Enable**. Alternatively, enable all the connections by clicking **EnableAll**.

3. Verify the Operational State is **Available**.

**Note:** If a disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution.
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>SOAM VIP GUI:</th>
<th>Task Description</th>
</tr>
</thead>
</table>
| 71.  | Enable optional features.  
      | DSR only. If SDS, then skip to step 75. | Navigate to **Diameter > Maintenance > Applications**.  
Select the optional feature application configured in step 60.  
Click **Enable**.  
Enable | Disable | Pause updates |
| 72.  | Re-enable transports, if needed.  
      | DSR only. If SDS, then skip to step 75. | Navigate to **Transport Manager > Maintenance > Transport**.  
Select each transport and click **Enable**.  
Enable | Disable | Block |
| 73.  | Re-enable MAPIWF application, if needed.  
      | DSR only. If SDS, then skip to step 75. | Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.  
Click the **Enable** button corresponding to MAPIWF Application Name.  
Enable | Disable |

3. Verify the SSN Status is **Enabled**.
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>74.</td>
<td><strong>SOAM VIP GUI:</strong> Re-enable links, if needed. DSR only. If SDS, then skip to step 75.</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to SS7/Sigtran &gt; Maintenance &gt; Links.</td>
</tr>
<tr>
<td></td>
<td>- SS7/Sigtran</td>
</tr>
<tr>
<td></td>
<td>- Configuration</td>
</tr>
<tr>
<td></td>
<td>- Maintenance</td>
</tr>
<tr>
<td></td>
<td>- Local SCCP Users</td>
</tr>
<tr>
<td></td>
<td>- Remote Signaling Points</td>
</tr>
<tr>
<td></td>
<td>- Remote MTP3 Users</td>
</tr>
<tr>
<td></td>
<td>- Linksets</td>
</tr>
<tr>
<td></td>
<td>- Links</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Enable</strong> for each link.</td>
</tr>
<tr>
<td></td>
<td>3. Verify the Operational Status for each link is <strong>Up</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>NOAM VIP:</strong> Verify all servers in topology are accessible (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>1. Establish an SSH session to the NOAM VIP and login as admusr.</td>
</tr>
<tr>
<td></td>
<td>2. Check if all the servers in the topology are accessible:</td>
</tr>
<tr>
<td></td>
<td><code>$ /usr/TKLC/dpi/bin/</code></td>
</tr>
<tr>
<td></td>
<td><code>./sharedKrevo -checkAccess</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example output:</strong></td>
</tr>
<tr>
<td></td>
<td><code>1450111012: [INFO] 'SOAM-2' is accessible.  FIPS integrity verification test failed.  The authenticity of host 'ipfs (10.240.146.16)' can't be established.  RSA key fingerprint is ea:7f:0d:eb:56:4d:de:8b:04:a3:fe:72:de:a3:52. Are you sure you want to continue connecting [yes/no]? yes  Warning: permanently added 'ipfs,10.240.146.16' (RSA) to the list of known hosts</code></td>
</tr>
<tr>
<td></td>
<td><code>1450111015: [INFO] 'IPPE' is accessible.  FIPS integrity verification test failed.  The authenticity of host 'mp-2 (10.240.146.24)' can't be established.  RSA key fingerprint is 78:4e:acc:87:af:45:8d:cc:ce:bf:cc:89:87:35:74. 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</code></td>
</tr>
<tr>
<td></td>
<td><code>1450111017: [INFO] 'MP-2' is accessible.  FIPS integrity verification test failed.  The authenticity of host 'mp-1 (10.240.146.14)' can't be established.  RSA key fingerprint is c5:66:85:60:1d:89:fs:78:92:3e:ca:e8:31:bf:ef:99. Are you sure you want to continue connecting [yes/no]? yes  Warning: permanently added 'mp-1,10.240.146.14' (RSA) to the list of known hosts</code></td>
</tr>
<tr>
<td></td>
<td><code>1450111020: [INFO] 'MP-1' is accessible.</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If any server is not accessible, stop and contact My Oracle Support (MOS).</td>
</tr>
</tbody>
</table>
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</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>1. Establish an SSH session to any active SOAM that remained intact and operational (Log into an active SOAM server that was not recovered or did not need recovery).</td>
</tr>
<tr>
<td></td>
<td>2. Login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Check if the existing key file on active SOAM server is valid:</td>
</tr>
</tbody>
</table>
|      | ```
|      | $ cd /usr/TKLC/dpi/bin/
|      | $ ./sharedKrevo -validate
|      | **Note:** If output of above command shows that existing key file is not valid, contact My Oracle Support (MOS). |
|      | 4. Establish an SSH session to the active NOAM, login as **admusr**. |
|      | 5. Copy the key file to active NOAM: |
|      | ```
|      | $ cd /usr/TKLC/dpi/bin/
|      | $ ./sharedKrevo -copyKey -destServer <Active NOAM server name>
|
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>77.</th>
<th><strong>NOAM VIP:</strong> Copy key file to all the servers in topology (RADIUS only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Establish an SSH session to any of the active NOAM. Login as <code>admusr</code>.</td>
</tr>
<tr>
<td>2.</td>
<td>Copy the key file to all the servers in the topology:</td>
</tr>
<tr>
<td></td>
<td>$ cd /usr/TKLC/dpi/bin/</td>
</tr>
<tr>
<td></td>
<td>$ ./sharedKrevo -synchronize</td>
</tr>
<tr>
<td><strong>Example output:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[admusr@NOAM-1 bin]$ ./sharedKrevo -synchronize</td>
</tr>
<tr>
<td></td>
<td>FIPS integrity verification test failed.</td>
</tr>
<tr>
<td></td>
<td>14502003056: [INFO] Key file on Active NOAM and NOAM-2 are same.</td>
</tr>
<tr>
<td></td>
<td>14502003056: [INFO] NO NEED to sync key file to NOAM-2.</td>
</tr>
<tr>
<td></td>
<td>FIPS integrity verification test failed.</td>
</tr>
<tr>
<td></td>
<td>14502003056: [INFO] Key file on Active NOAM and SOAM-1 are same.</td>
</tr>
<tr>
<td></td>
<td>14502003056: [INFO] NO NEED to sync key file to SOAM-1.</td>
</tr>
<tr>
<td></td>
<td>FIPS integrity verification test failed.</td>
</tr>
<tr>
<td></td>
<td>14502003056: [INFO] Key file on Active NOAM and SOAM-2 are same.</td>
</tr>
<tr>
<td></td>
<td>14502003056: [INFO] NO NEED to sync key file to SOAM-2.</td>
</tr>
<tr>
<td></td>
<td>FIPS integrity verification test failed.</td>
</tr>
<tr>
<td></td>
<td>$ ./sharedKrevo -updateData</td>
</tr>
<tr>
<td><strong>Example output:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[admusr@NOAM-1 bin]$ ./sharedKrevo -updateData</td>
</tr>
<tr>
<td></td>
<td>14502003056: [INFO] Updating data on server 'NOAM-1'</td>
</tr>
<tr>
<td></td>
<td>14502003056: [INFO] Data updated to 'NOAM-1'</td>
</tr>
<tr>
<td></td>
<td>FIPS integrity verification test failed.</td>
</tr>
<tr>
<td></td>
<td>14502003056: [INFO] Updating data on server 'SOAM-2'</td>
</tr>
<tr>
<td></td>
<td>FIPS integrity verification test failed.</td>
</tr>
<tr>
<td></td>
<td>14502003056: [INFO] 1 row updated on 'SOAM-2'...</td>
</tr>
<tr>
<td></td>
<td>14502003056: [INFO] Data updated to 'SOAM-2'</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>78.</th>
<th><strong>SOAM VIP GUI:</strong> Examine all alarms</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to <strong>Alarms &amp; Events &gt; View Active</strong>.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Alarms &amp; Events" /></td>
</tr>
<tr>
<td></td>
<td>- <strong>View Active</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>View History</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>View Trap Log</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Examine all active alarms and refer to the on-line help on how to address them.</td>
</tr>
<tr>
<td></td>
<td>If needed, contact My Oracle Support (MOS).</td>
</tr>
</tbody>
</table>
Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>79.</td>
<td><strong>NOAM VIP GUI:</strong> Examine all alarms</td>
</tr>
<tr>
<td>80.</td>
<td>Back up and archive all the databases from the recovered system</td>
</tr>
<tr>
<td>81.</td>
<td>Recover IDIH, if configured</td>
</tr>
<tr>
<td>82.</td>
<td>SNMP workaround</td>
</tr>
</tbody>
</table>

1. Navigate to Alarms & Events > View Active.

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

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

If needed, contact My Oracle Support (MOS).

Execute the DSR Database Backup procedure to back up the configuration databases.

If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.

Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases:

1. If SNMP is not configured in DSR/SDS.
2. If SNMP is already configured and SNMPv3 is selected as enabled version.

4.4 Recovery Scenario 4 (Partial Server Outage with One NOAM Server and One SOAM Server Intact)

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

- Recover standby NOAM server by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover Query Server (if needed) by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
- Recover Standby SOAM server by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
- Recover MP/DP C-level servers by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
## Procedure 4. Recovery Scenario 4

### Workarounds

This procedure performs recovery if at least one NOAM server is intact and available and 1 SOAM server is intact and available. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Workarounds</th>
</tr>
</thead>
</table>
| 1.     | Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist. Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases:  
1. If SNMP is not configured in DSR.  
2. If SNMP is already configured and SNMPv3 is selected as enabled version. |
| 2.     | Gather the documents and required materials listed in Required Materials. |
| 3.     | Work with the hardware vendor to replace the failed equipment. |
| 4.     | 1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  
http://<Primary_NOAM_VIP_IP_ADDdress>  
2. Login as the guiadmin user: |

![Oracle System Login](image)
## Procedure 4. Recovery Scenario 4

### 5. Active NOAM: Set failed servers to OOS

1. Navigate to **Status & Manage > HA**.

2. Click **Edit**.

3. Set the Max Allowed HA Role option to **OOS** for the failed servers.

### 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>ZombieDRNOAM1</td>
<td>Observer</td>
<td>The maximum des</td>
</tr>
</tbody>
</table>

4. Click **OK**.

### 6. Recover PMAC and PMAC TVOE Host: Configure BIOS settings and update firmware

1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:
   - **HP DL380 Gen8**: Configure HP Gen 8 Server BIOS Settings
   - **Oracle X5-2/Netra X5-2/X6-2/X7-2**: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings
   - **HP DL380 Gen9**: Configure HP Gen9 Server BIOS Settings

2. Verify and/or upgrade server firmware by executing the **Upgrade Rack Mount Server Firmware** procedure from reference [8].
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>7.</strong> Recover PMAC, TVOE Hosts, and Switch: Backups available</td>
<td>If the PMAC is located on the failed rack mount server, execute this step; otherwise skip to step 10. This step assumes TVOE and PMAC backups are available. If backups are NOT available, <strong>skip this step</strong>. 1. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers. 2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup. 3. Proceed to step 9.</td>
</tr>
<tr>
<td><strong>8.</strong> Recover PMAC, TVOE Hosts, and Switch: Backups NOT available</td>
<td>If the PMAC is located on the failed rack mount server, execute this step; otherwise skip to step 10. This step assumes TVOE and PMAC backups are NOT available. If the TVOE and PMAC have already been restored, <strong>skip this step</strong>. Execute these procedures from reference [8]:  • <strong>Install and Configure TVOE on First RMS (PMAC Host)</strong>  • <strong>Install PMAC</strong>  • <strong>Initialize the PMAC Application</strong></td>
</tr>
<tr>
<td><strong>9.</strong> Configure PMAC (no backup)</td>
<td>If PMAC backup was <strong>NOT</strong> restored in step 7, execute this step; otherwise, skip this step. Execute these procedures from reference [8]:  • <strong>Configure PMAC Server (NetBackup Only)</strong>  • <strong>Add RMS to the PMAC Inventory</strong></td>
</tr>
<tr>
<td><strong>10.</strong> Install/Configure additional rack mount servers</td>
<td><strong>Note:</strong> If TVOE backups are available, refer Appendix G Restore TVOE Configuration from Backup Media; otherwise, execute this step. If TVOE backups were <strong>NOT</strong> performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step. 1. Execute these procedures from reference [8]:  • <strong>Install TVOE on Additional Rack Mount Servers</strong>  • <strong>Configure TVOE on Additional Rack Mount Servers</strong> 2. Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]:  • <strong>HP DL380 Gen8</strong>: Configure HP Gen 8 Server BIOS Settings  • <strong>Oracle X5-2/Netra X5-2/X6-2/X7-2</strong>: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings  • <strong>HP DL380 Gen9</strong>: Configure HP Gen9 Server BIOS Settings 3. Verify and/or upgrade server firmware by executing the <strong>Upgrade Rack Mount Server Firmware</strong> procedure from reference [8].</td>
</tr>
</tbody>
</table>
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 11.  | **□** Determine VM placement and socket pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 only)                                                                                                                                                                                                     | *HP DL380 GEN 8, skip this step.*  
Determine VM placement and pinning by following section 3.1, item 14.                                                                                                                                                                                                                       |
| 12.  | **□** Deploy redundant PMAC, if required                                                                                                                                                                                                                                                                                                                                 | Refer to the **Deploy Redundant PMAC (Optional)** procedure to re-deploy and configure any redundant PMACs previously configured.                                                                                                     |
| 13.  | **□** PMAC: Determine if the fdconfig file exists from the initial deployment  
1. Type:  
```
[admusr@melbourne-pmac-1 ~]$ ll /usr/TKLC/smac/etc/fdc/
```
2. Examine the results and verify if the *rms config file* `<hostname>.cfg` exists.  
*Note:* There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS.  
3. Skip to step 15.                                                                                                                                                                                                                     |
| 14.  | **□** Create fdconfig backup file, if it does not already exist  
Execute this step ONLY If the fdconfig backup file does NOT exist.  
Create the needed file(s) by executing the **Virtual Machine/Network Fast Deployment** section from reference [8].  
**WARNING**  
It is very important to ensure the file(s) created only affects the TVOE server(s) and the guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.                                                                                      |
| 15.  | **□** PMAC: Load ISOs into PMAC, if not done already  
If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the **Virtual Machine/Network Fast Deployment** section from reference [8].                                                                                                                                                                                                                     |
| 16.  | **□** PMAC: Edit/Update configuration file  
Edit the fdconfig file to include only the required/failed servers.  
**Notes:**  
- Comment out configuration items that are not needed.  
- Create a separate configuration file for EACH rack mount server being deployed.  
- The Cabinet ID in the config file needs to match the cabinet already defined in PMAC.  
The following items are mandatory:  
  - siteName  
  - tpdIso  
  - dsrlso (if DSR VMs are being configured)  
  - sdsIso (if SDS VMs are being configured)  
  - NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured)                                                                                                                      |
Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Procedure 4. Recovery Scenario 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>• XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured)</td>
</tr>
<tr>
<td>• XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured)</td>
</tr>
<tr>
<td>• DSRNOAM1XMIPADDRESS (if DSRNOAM1 is being configured)</td>
</tr>
<tr>
<td>• DSRNOAM2XMIPADDRESS (if DSRNOAM2 is being configured)</td>
</tr>
<tr>
<td>• DSRDRNOAM1XMIPADDRESS (if DSRDRNOAM1 is being configured)</td>
</tr>
<tr>
<td>• DSRDRNOAM2XMIPADDRESS (if DSRDRNOAM2 is being configured)</td>
</tr>
<tr>
<td>• SDSNOAM1XMIPADDRESS (if SDSNOAM1 is being configured)</td>
</tr>
<tr>
<td>• SDSNOAM2XMIPADDRESS (if SDSNOAM2 is being configured)</td>
</tr>
<tr>
<td>• SDSDRNOAM1XMIPADDRESS (if SDSDRNOAM1 is being configured)</td>
</tr>
<tr>
<td>• SDSDRNOAM2XMIPADDRESS (if SDSDRNOAM2 is being configured)</td>
</tr>
</tbody>
</table>

**Notes:**

- Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].
- Comment out SDS and DSR profile items if corresponding products are not used.
- For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9, refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].
- VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName.
- VM locations should not be changed from their RMSx format. Each RMS should correspond to a separate rack mount server.

**WARNING**

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

17. **PMAC:** Copy the backed up fdc file to the RMS directory

Copy the fdconfig backup file to the RMS directory.

```bash
$ sudo cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file>
/usr/TKLC/smac/etc/RMS/
```
## Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18. PMAC:</td>
<td>Execute the config.sh script.</td>
</tr>
</tbody>
</table>

**Execute config.sh** against the modified backup config file.

**Note:** If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again.

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

**Example output:**

```
[admin@5010441PMAC RMS]$ sudo ./config.sh rms.cfg
Validating cfg file...
Successful validation of cfg file.
Added Cabinet 101 to Fast Deployment File.
Added Zombie_TVOE1 to Fast Deployment File.
Added Zombie_TVOE2 to Fast Deployment File.
Added xml (bond0.4) to Fast Deployment File.
Added ini (bond0.3) to Fast Deployment File.
Added rep (bond1.10) to Fast Deployment File.
Added xsl (bond1.6) to Fast Deployment File.
Added xsl (bond1.7) to Fast Deployment File.
Added xsl (bond1.8) to Fast Deployment File.
Added xsl (bond1.9) to Fast Deployment File.
Added xsl (bond1.10) to Fast Deployment File.
Added xsl (bond1.11) to Fast Deployment File.
Added xsl (bond1.12) to Fast Deployment File.
Added xsl (bond1.13) to Fast Deployment File.
Added xsl (bond1.14) to Fast Deployment File.
Added xsl (bond1.15) to Fast Deployment File.
Added xsl (bond1.16) to Fast Deployment File.
Added xsl (bond1.17) to Fast Deployment File.
Added xsl (bond1.18) to Fast Deployment File.
Added xsl (bond1.19) to Fast Deployment File.
Added xsl (bond1.20) to Fast Deployment File.
Added xsl (bond1.21) to Fast Deployment File.
Added xsl (bond1.22) to Fast Deployment File.
Added Zombie_DSRKOM1 to Fast Deployment File.
Added Zombie_DSRKOM2 to Fast Deployment File.
Added Zombie_DSRKONAM1 to Fast Deployment File.
Added Zombie_DSRKONAM2 to Fast Deployment File.
Validating Fast Deployment File.....
Configuration file validation successful.
Validation complete
Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml
SUCCESS: OPERATION SUCCESS!!
```

[Image of command output]
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>19.</strong></td>
<td><strong>PMAC:</strong> Execute fast deployment&lt;br&gt;With the file generated from the config.sh script, execute the following command to start fast deployment:</td>
</tr>
</tbody>
</table>
|  | ```
$ screen
$ sudo fdconfig config --file=<fd_config.xml>
``` |
|  | **Note:** This is a long duration command. If the screen command was run before executing the fdconfig, perform a `screen -dr` to resume the screen session in the event of a terminal timeout, etc. |
| **20.** | **PMAC GUI:** Monitor the configuration<br>1. If not already done, establish a GUI session on the PMAC server.<br>2. Navigate to **Task Monitoring**. |
|  | ![Task Monitoring](image)
|  | **Main Menu: Task Monitoring**
|  | ![Task Monitoring Table](image)
|  | **Note:** If a failure occurs with fdconfig, logs can be accessed in `/var/TKLC/log/fdconfig/fdconfig.log` file.
|  | `[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:
|  | ![Task Dump](image)
|  | ![Task Dump](image)
|  | ![Task Dump](image)
|  | ![Task Dump](image)
|  | **Note:** If a failure occurs with fdconfig, logs can be accessed in `/var/TKLC/log/fdconfig/fdconfig.log` file.
|  | `[admusr@melbourne-pmac-1 fdconfig]$ sudo fdconfig restart --file=deploy_melbourne_20170329T202458_701b.fdcdb`


### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21.</td>
<td>PMAC: Repeat for each rack mount server configuration file</td>
<td>Repeat steps 13.-20. for each rack mount server/configuration file, if required.</td>
</tr>
</tbody>
</table>
| 22. | PMAC: Back up FDC file | 1. 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/
   ```  
   2. Change permissions:  
   ```bash
   $ sudo chmod 777 /usr/TKLC/smac/etc/fdc/<fdc_file>
   ``` |
| 23. | Perform CPU pinning | Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only) procedure from reference [8]. |
| 24. | NOAM GUI: Login | If the failed server is not OAM, then skip to step 47.  
   1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  
   ```text
   http://<Primary_NOAM_VIP_IP_Address>
   ```  
   2. Login as the `guiadmin` user: |

---

**Oracle System Login**

Welcome to the Oracle System Logon.

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 4. Recovery Scenario 4

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

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>28.</td>
<td>NOAM VIP GUI: Restart DSR application</td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Server</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the recovered standby NOAM server and click <strong>Restart</strong>.</td>
</tr>
<tr>
<td>29.</td>
<td><strong>Active NOAM</strong>: Correct the recognized authority table</td>
<td>1. Establish an SSH session to the active NOAM and login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Execute this command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo top.setPrimary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Using my cluster: A1789</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updating A1789.022: &lt;DSR_NOAM_B_hostname&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updating A1789.144: &lt;DSR_NOAM_A_hostname&gt;</td>
</tr>
<tr>
<td>30.</td>
<td>NOAM VIP GUI: Recover query servers. SDS only.</td>
<td>Execute the <strong>Configuring SDS Query Servers</strong> procedure, steps 1 and 4-7, from reference [8].</td>
</tr>
<tr>
<td></td>
<td><strong>Recover query servers. SDS only. If DSR, skip to step 33.</strong></td>
<td></td>
</tr>
</tbody>
</table>
**Procedure 4. Recovery Scenario 4**

<table>
<thead>
<tr>
<th>31.</th>
<th><strong>SDS NOAM VIP GUI:</strong> Set HA on query server. SDS only. If DSR, skip to step 33.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; HA.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Status &amp; Manage" /></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Edit.</strong></td>
</tr>
<tr>
<td></td>
<td>3. Select the query server and select <strong>Observer.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Observer" /></td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>32.</th>
<th><strong>SDS NOAM VIP GUI:</strong> Restart SDS application. SDS only. If DSR, skip to step 33.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Server.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Status &amp; Manage" /></td>
</tr>
<tr>
<td></td>
<td>2. Select the recovered query server and click <strong>Restart.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>33.</th>
<th><strong>NOAM VIP GUI:</strong> Recover the SOAM servers (<em>Standby, Spare</em> — Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>DSR:</strong> Execute the <strong>Configure the SOAM Servers</strong> procedure, steps 1-3 and 5-9, from reference [8].</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you are using NetBackup, also execute step 12.</td>
</tr>
<tr>
<td></td>
<td><strong>SDS:</strong> Execute the <strong>Configure the SDS DP SOAM Servers</strong> procedure, steps 1-3 and 5-8, from reference [8].</td>
</tr>
</tbody>
</table>
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
</table>
| 34.  | **NOAM VIP GUI:**  
|      | Set HA on standby NOAM  
|      | 1. Navigate to Status & Manage > HA.  
|      |   - Status & Manage  
|      |     - Network Elements  
|      |     - Server  
|      |     - HA  
|      |     - Database  
|      |     - KPIs  
|      |     - Processes  
|      |     - Tasks  
|      |     - Files  
|      | 2. Click **Edit**.  
|      | 3. Select the standby NOAM server and set it to **Active**.  
|      | 4. Click **OK**.  
| 35.  | **NOAM VIP GUI:**  
|      | Restart DSR application  
|      | 1. Navigate to Status & Manage > Server.  
|      | 2. Select the recovered standby NOAM server and click **Restart**.  
| 36.  | **Activate PCA feature.**  
|      | **DSR only.**  
|      | **If SDS, skip this step.**  
|      | If you have PCA installed in the system being recovered, re-activate PCA by executing the **PCA Activation on Active NOAM Network** procedure on the recovered standby NOAM server and the **PCA Activation on Stand By SOAM Network** procedure on the recovered standby SOAM from reference [7].
## Procedure 4. Recovery Scenario 4

### 37. NOAM VIP GUI: Recover the C-level servers (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs)

**DSR:**
- Execute the **Configure the MP Servers** procedure, steps 1 and 9-13, from reference [8].

**Note:**
- Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.

**SDS —** Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only:
- Execute the **Configure the SDS DP Servers** procedure, steps 1 and 5-8, from reference [8].
- Repeat this step for any remaining failed MP servers.

### 38. NOAM VIP GUI: Set HA on all C-level servers

1. Navigate to **Status & Manage > HA**.

2. Click **Edit**.

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

4. Click **OK**.
## Procedure 4. Recovery Scenario 4

### 39. NOAM VIP GUI:

**Restart DSR application on recovered C-level servers**

1. Navigate to **Status & Manage > Server**.
   - ![Status & Manage](image)
     - Network Elements
     - Server
     - HA
     - Database
     - KPIs
     - Processes
   - 2. Select the recovered C-level servers and click **Restart**.

### 40. Active NOAM:

**Perform keyexchange between the active-NOAM and recovered servers**

1. Establish an SSH session to the active NOAM, login as **admusr**.
2. Perform a keyexchange from the active NOAM to each recovered server:
   ```bash
   $ keyexchange admusr@<Recovered Server Hostname>
   ```

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

### 41. Active NOAM:

**Activate optional features.**

DSR only. If SDS, then skip step 43.

Establish an SSH session to the active NOAM and login as **admusr**.

**Note for PCA Feature Activation:**

If you have PCA installed in the system being recovered, re-activate the PCA by executing the **PCA Activation on Active NOAM Server** procedure on recovered active NOAM server and the **PCA Activation on Standby SOAM Server** procedure on the recovered standby SOAM server from [6].

**Notes:**
- If not all SOAM sites are recovered at this point, then repeat the activation for each “new” SOAM site that comes online.
- If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature.

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

**Note:** While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored:

```
イルド#31000{S/W fault}
```

### 42. MP Servers:

**Disable SCTP Auth Flag (DSR only).**

DSR only. If SDS, then skip step 43.

For SCTP connections without DTLS enabled, refer to the **Enable/Disable DTLS (SCTP Diameter Connections Only)** section in reference [8].

Execute this procedure on all failed MP servers.
Procedure 4. Recovery Scenario 4

43. **NOAM VIP GUI:**

    Fetch and store the database report for the newly restored data and save it.

1. Navigate to **Status & Manage > Database**.

    ![Status & Manage Menu]

2. Select the active NOAM server and click **Report**.

    The following screen displays:

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

    ```
    Database Status Report
    From: Active Network OAM6P on host ZombieNOAM1
    Report Version: 8.0.0.0.0-80.9.0
    User: guiadmin
    ```

    **General**
    **Hostname**: ZombieNOAM1
    **Database Birthday**: 2016-07-11 11:21:50 EDT
    **AppWorks Database Version**: 6.0
    **Application Database Version**: 

    **Capacities and Utilization**
    **Disk Utilization**: 8.4%
    **Memory Utilization**: 0.0%

3. Click **Save** and save the report to your local machine.
**Procedure 4. Recovery Scenario 4**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.</td>
<td><strong>Active NOAM:</strong> Verify replication between servers</td>
</tr>
</tbody>
</table>

1. Log into the active NOAM as `admusr` using SSH terminal.
2. Execute this command:

   ```
   $ sudo irepstat -m
   ```

**Example output:**

```
-- Policy 0 ActStb [DbReplication] -----------------------
Oahu-DAMP-1 -- Active
   BC From Oahu-SOAM-2 Active 0 0.50 0.15%cpu 25B/s A-me
   CC To Oahu-DAMP-2 Active 0 0.10 0.14%cpu 25B/s A-me

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

Oahu-IPFE-1 -- Active
   BC From Oahu-SOAM-2 Active 0 0.50 0.03%cpu 24B/s A=C3642.212

Oahu-IPFE-2 -- Active
   BC From Oahu-SOAM-2 Active 0 0.50 0.03%cpu 28B/s A=C3642.212

Oahu-NOAM-1 -- Stby
   AA From Oahu-NOAM-2 Active 0 0.25 0.03%cpu 23B/s

Oahu-NOAM-2 -- Active
   AA To Oahu-NOAM-1 Active 0 0.25 1%R 0.04%cpu 61B/s
   AB To Oahu-SOAM-2 Active 0 0.50 1%R 0.05%cpu 75B/s

Oahu-SOAM-1 -- Stby
   BB From Oahu-SOAM-2 Active 0 0.50 0.03%cpu 27B/s

Oahu-SOAM-2 -- Active
   AB From Oahu-NOAM-2 Active 0 0.50 0.03%cpu 24B/s
   BB To Oahu-SOAM-1 Active 0 0.50 1%R 0.04%cpu 32B/s
   BC To Oahu-IPFE-1 Active 0 0.50 1%R 0.04%cpu 21B/s
   BC To Oahu-SS7MP-2 Active 0 0.50 1%R 0.04%cpu 21B/s

irepstat (40 lines) (h)elp (m)erged
```
Procedure 4. Recovery Scenario 4

45. NOAM VIP GUI: Verify the database states

1. Navigate to Status & Manager > Database.

   - Network Elements
   - Server
   - HA
   - Database
   - KPIs
   - Processes

2. Verify the OAM Max HA Role as shown.

<table>
<thead>
<tr>
<th>Role</th>
<th>Server Type</th>
<th>Expected HA Role(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network OAM&amp;P</td>
<td>NO</td>
<td>Active/Standby</td>
</tr>
<tr>
<td>SYSTEM OAM</td>
<td>SOAM</td>
<td>Active/Standby/Spare</td>
</tr>
<tr>
<td>MP</td>
<td>DA MP(s)</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td>IPFE(s)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SS7MP(s)</td>
<td></td>
</tr>
<tr>
<td>MP</td>
<td>SBR(s)</td>
<td>Active/Standby/Spare</td>
</tr>
</tbody>
</table>

3. Verify the Status and OAM Repl Status is Normal and Repl Status=Allowed.

46. NOAM VIP GUI: Verify the HA status

1. Navigate to Status and Manage > HA.

2. Select the row for all of the servers.

3. Verify the HA Role is either Active or Standby.

<table>
<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>
Procedure 4. Recovery Scenario 4

47. SOAM VIP GUI: Verify the local node information. DSR only. If SDS, then skip to step 56.

1. Navigate to Diameter > Configuration > Local Node.

   - Diameter
     - Configuration
       - Capacity Summary
       - Connection Capacity Dashboard
       - Application IDs
       - CEX Parameters
       - Command Codes
     - Configuration Sets
       - Local Nodes

2. Verify all the local nodes are shown.

48. SOAM VIP GUI: Verify the peer node information. DSR only. If SDS, then skip to step 56.

1. Navigate to Diameter > Configuration > Peer Node.

   - Diameter
     - Configuration
       - Capacity Summary
       - Connection Capacity Dashboard
       - Application IDs
       - CEX Parameters
       - Command Codes
     - Configuration Sets
       - Local Nodes
       - Peer Nodes

2. Verify all the peer nodes are shown.

49. SOAM VIP GUI: Verify the connections information. DSR only. If SDS, then skip to step 56.

3. Navigate to Diameter > Configuration > Connections.

   - Diameter
     - Configuration
       - Capacity Summary
       - Connection Capacity Dashboard
       - Application IDs
       - CEX Parameters
       - Command Codes
     - Configuration Sets
       - Local Nodes
       - Peer Nodes
       - Peer Node Groups
       - Connections

4. Verify all the connections 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. If SDS, then skip to step 56.  
  1. Navigate to **Diameter > Maintenance > Connections**.  
  2. Select each connection and click **Enable**. Alternatively, enable all the connections by clicking **EnableAll**.  
  3. Verify the Operational State is **Available**.  
  **Note:** If a disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution. |
| 51.  | **SOAM VIP GUI:** Enable optional features. DSR only. If SDS, then skip to step 56.  
  1. Navigate to **Diameter > Maintenance > Applications**.  
  2. Select the optional feature application configured in step 72.  
  3. Click **Enable**. |
| 52.  | **SOAM VIP GUI:** Re-enable transports, if needed. DSR only. If SDS, then skip to step 56.  
  1. Navigate to **Transport Manager > Maintenance > Transport**.  
  2. Select each transport and click **Enable**.  
  3. Verify the Operational Status for each transport is **Up**. |
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th></th>
<th>SOAM VIP GUI: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 56.</th>
</tr>
</thead>
</table>
| 53. | 1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.  
| | - SS7/Sigtran  
| | - Configuration  
| | - Maintenance  
| | - Local SCCP Users  
| | - Remote Signaling Points  
| | - Remote MTP3 Users  
| | - Linksets  
| | - Links  
| | 2. Click the **Enable** button corresponding to MAPIWF Application Name.  
| | ![Enable Disable]  
| | 3. Verify the SSN Status is **Enabled**. |

<table>
<thead>
<tr>
<th></th>
<th>SOAM VIP GUI: Re-enable links, if needed. DSR only. If SDS, then skip to step 56.</th>
</tr>
</thead>
</table>
| 54. | 1. Navigate to **SS7/Sigtran > Maintenance > Links**.  
| | - SS7/Sigtran  
| | - Configuration  
| | - Maintenance  
| | - Local SCCP Users  
| | - Remote Signaling Points  
| | - Remote MTP3 Users  
| | - Linksets  
| | - Links  
| | 2. Click **Enable** for each link.  
| | ![Enable Disable]  
| | 3. Verify the Operational Status for each link is **Up**. |
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 55.  | **SOAM VIP GUI:** Reset remote MTP3 users, if needed. DSR only. If SDS, then skip to step 56.  
1. Navigate to SS7/Sigtran > Maintenance > Remote MTP Users.  
2. Click Reset for each record, if needed. |
| 56.  | **NOAM VIP:** Verify all servers in topology are accessible (RADIUS only)  
If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.  
1. Establish an SSH session to the NOAM VIP and login as `admusr`.  
2. Check if all the servers in the topology are accessible: |
|      | Example output: |
|      |   $ /usr/TKLC/dpi/bin/   
|      |   $ ./sharedKrevo -checkAccess   
|      |   ```
|      |   [admusr@NOAM-2 bin]$ ./sharedKrevo -checkAccess
|      |   FIPS integrity verification test failed.
|      |   1450723403: [INFO] 'NOAM-1' is accessible.
|      |   FIPS integrity verification test failed.
|      |   1450723403: [INFO] 'SOAM-1' is accessible.
|      |   FIPS integrity verification test failed.
|      |   1450723403: [INFO] 'SOAM-2' is accessible.
|      |   FIPS integrity verification test failed.
|      |   1450723404: [INFO] 'IPFE' is accessible.
|      |   FIPS integrity verification test failed.
|      |   1450723404: [INFO] 'MP-2' is accessible.
|      |   FIPS integrity verification test failed.
|      |   1450723404: [INFO] 'MP-1' is accessible.
|      |   [admusr@NOAM-2 bin]$ ``` |
|      | **Note:** If any server is not accessible, stop and contact My Oracle Support (MOS). |
| 57.  | **NOAM VIP:** Copy key file to all the servers in topology (RADIUS only)  
If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.  
1. Check if existing key file on active NOAM (the NOAM, which is intact and was not recovered) server is valid: |
Procedure 4. Recovery Scenario 4

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

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

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

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

$ ./sharedKrevo –synchronize

Example output:
```
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722738: [INFO] Synched key to IPFE
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722738: [INFO] Synched key to NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722738: [INFO] Synched key to NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722738: [INFO] Synched key to NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722738: [INFO] Synched key to NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2.
```

$ ./sharedKrevo –updateData

Example output:
## Procedure 4. Recovery Scenario 4

### 58. SOAM VIP GUI: Examine all alarms

1. Navigate to **Alarms & Events > View Active**.
   - **View Active**
   - **View History**
   - **View Trap Log**

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

   If needed, contact My Oracle Support (MOS).

### 59. NOAM VIP GUI: Examine all alarms

1. Navigate to **Alarms & Events > View Active**.
   - **View Active**
   - **View History**
   - **View Trap Log**

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

   If needed, contact My Oracle Support (MOS).

### 60. Restart oampAgent, if needed

*Note:* If **10012: The responder for a monitored table failed to respond to a table change** alarm displays, the oampAgent needs to be restarted.

1. Establish an SSH session to each server that has the alarm.
2. Login admusr
3. Execute the following commands:

   ```bash
   $ sudo pm.set off oampAgent
   $ sudo pm.set on oampAgent
   ```

### 61. Back up and archive all the databases from the recovered system

Execute the **DSR Database Backup** procedure to back up the configuration databases.

### 62. Recover IDIH

If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.
4.5 Recovery Scenario 5 (Both NOAM Servers Failed with DR-NOAM Available)

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

- Switch DR NOAM from secondary to primary
- Recover the failed NOAM servers by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
  - The database is intact at the newly active NOAM server and does not require restoration
- If applicable, recover any failed SOAM and MP servers by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
  - The database in intact at the active NOAM server and does not require restoration at the SOAM and MP servers
- Recover IDIH if necessary

Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Workarounds</th>
<th>Gather required materials</th>
<th>Switch DR NOAM to primary</th>
</tr>
</thead>
</table>
| 1. ☐   | Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist. Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases:
1. If SNMP is not configured in DSR.
2. If SNMP is already configured and SNMPv3 is selected as enabled version. | Gather the documents and required materials listed in Required Materials. | Refer to [13] DSR/SDS NOAM Failover User’s Guide. |
## Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td><strong>Recover failed SOAMs</strong>&lt;br&gt;Recover failed SOAMs&lt;br&gt;If ALL SOAM servers have failed, execute Procedure 2.&lt;br&gt;If ALL NOAM servers have failed, execute:&lt;br&gt;1. Procedure 4, steps 4. through 14.&lt;br&gt;2. Perform keyexchange between the newly active NOAM and the recovered NOAM PMAC.&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's PMAC server using the keyexchange utility, using the management IP address for the PMAC server.&lt;br&gt;When asked for the password, enter the password for the <code>admusr</code> user of the PMAC server.</td>
</tr>
<tr>
<td></td>
<td><code>$ keyexchange admusr@&lt;Recovered_Servers_PMAC_IP Address&gt;</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If keyexchange fails, edit <code>/home/admusr/.ssh/known_hosts</code> and remove blank lines. Retry the keyexchange commands.</td>
</tr>
<tr>
<td>5.</td>
<td><strong>Perform keyexchange 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;8. 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;9. When prompted for the password, enter the password for the <code>admusr</code> user of the recovered NOAM servers.</td>
</tr>
<tr>
<td></td>
<td><code>$ keyexchange admusr@&lt;Recovered_NOAM_Hostname&gt;</code></td>
</tr>
</tbody>
</table>
### Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Recover standby/spare SOAM and C-level servers</th>
<th>If necessary, refer to Procedure 3 to recover any standby or Spare SOAMs as well as any C-Level servers.</th>
</tr>
</thead>
</table>
| 6. | Recovered NOAM Servers: Activate optional features | Map-Diameter Interworking (MAP-IWF) and/or Policy and Charging Application (PCA) Only  
Activate the features Map-Diameter Interworking (MAP-IWF) and Policy and Charging Application (PCA) as follows:  
**For PCA:**  
Establish SSH sessions to the all the recovered NOAM servers and login as `admusr`. Refer [7] and execute **PCA Activation on Standby NOAM Server** on all recovered NOAM servers to re-activate PCA.  
**For MAP-IWF:**  
Establish SSH session to the recovered active NOAM, login as `admusr`. Refer to [5] to activate Map-Diameter Interworking (MAP-IWF).  
*Note:* While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored:  
```
ioad#31000{S/W Fault}
```

*Note:* If any of the MPs are failed and recovered, then restart these MP servers after activation of the feature. |
| 7. | Recovered NOAM Servers: Copy key file to all the servers in topology (RADIUS only) | If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.  
1. Check if existing key file on active NOAM (the NOAM, which is intact and was not recovered) server is valid:  
   ```
   $ cd /usr/TKLC/dpi/bin/
   $ ./sharedKrevo -validate
   ```  
   *Note:* If output of above command shows that existing key file is not valid, contact My Oracle Support (MOS).  
2. Copy the key file from active DR NOAM to recovered NOAMs.  
   ```
   $ ./sharedKrevo -copyKey -destServer <First NOAM server>
   $ ./sharedKrevo -copyKey -destServer <Second NOAM server>
   ``` |
## Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th>9.</th>
<th><strong>Primary NOAM</strong>: Modify DSR OAM process</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Establish an SSH session to the primary NOAM, login as <code>admusr</code>.</td>
</tr>
<tr>
<td></td>
<td>2. Retrieve the cluster ID of the recovered NOAM:</td>
</tr>
<tr>
<td></td>
<td>$ sudo iqt -fClusterID TopologyMapping where &quot;NodeID='&lt;DR_NOAM_Host_Name&gt;'&quot;</td>
</tr>
<tr>
<td></td>
<td>Server_ID NodeID ClusterID</td>
</tr>
<tr>
<td></td>
<td>1 Oahu-DSR-NOAM-2 <strong>A1055</strong></td>
</tr>
<tr>
<td></td>
<td>3. Execute this command to start the DSR OAM process on the recovered NOAM:</td>
</tr>
<tr>
<td></td>
<td>$ echo &quot;&lt;clusterID&gt;</td>
</tr>
</tbody>
</table>

| 10. | **Switch DR NOAM back to secondary** |
|     | Once the system has been recovered, refer to [13] DSR/SDS NOAM Failover User's Guide. |
Procedure 5. Recovery Scenario 5

11. **NOAM VIP:**
    Verify all servers in topology are accessible (RADIUS only).
    DSR only. If SDS, then skip to the next step.

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

1. Establish an SSH session to the NOAM VIP and login as **admusr**.
2. Check if all the servers in the topology are accessible:

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

   **Note:** If any server is not accessible, stop and contact My Oracle Support (MOS).

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

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

   **Example output:**

   ```
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   140722738: [INFO] Synched key to MP-2.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   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.
   140722758: [INFO] Synched key to MP-2.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   140722738: [INFO] Synched key to MP-1.
   [admusr@NOAM-2 bin]$ 
   ```

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

   **Example output:**

   ```
   [admusr@NOAM-1 bin]$ ./sharedKrevo -updateData
   140203518: [INFO] Updating data on server 'NOAM-1'
   140203519: [INFO] Data updated to 'NOAM-1'
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   140203520: [INFO] Updating data on server 'SOAM-2'
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   140203522: [INFO] 1 rows updated on 'SOAM-2'...
   140203522: [INFO] Data updated to 'SOAM-2'
   ```

   **Note:** If any errors display, stop and contact My Oracle Support (MOS).
Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step #</th>
<th>Workaround</th>
<th>Details</th>
</tr>
</thead>
</table>
- [Alarms & Events]  
  - [View Active]  
  - [View History]  
  - [View Trap Log]  
2. Verify the recovered servers are not contributing to any active alarms (Replication, Topology misconfiguration, database impairments, NTP, etc.) |
| 13.    | Recover IDIH | If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH. |

4.6 Recovery Scenario 6 (Database Recovery)

4.6.1 Recovery Scenario 6: Case 1

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

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

Procedure 6. Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th>Step #</th>
<th>Workaround</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Workarounds</td>
<td>Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.</td>
</tr>
</tbody>
</table>
### Procedure 6. Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th>2.</th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
</table>

1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:

```
http://<Primary_NOAM_VIP_IP_Address>
```

2. Login as the `guiadmin` user:

![Oracle System Login](image)

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.

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></th>
<th>NOAM VIP GUI: Set failed servers to OOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Navigate to Status &amp; Manage &gt; HA.</td>
</tr>
<tr>
<td></td>
<td>Select Edit.</td>
</tr>
<tr>
<td></td>
<td>Modifying HA attributes</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Modifying HA attributes" /></td>
</tr>
<tr>
<td></td>
<td>3. Set the Max Allowed HA Role option to OOS for the failed servers.</td>
</tr>
<tr>
<td></td>
<td>4. Click OK.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Server in Question: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Establish an SSH session to the server in question. Login as admusr.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Server in Question: Change runlevel to 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Bring the system to runlevel 3.</td>
</tr>
<tr>
<td></td>
<td>$ sudo init 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Server in Question: Recover system</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>Execute this command and follow the instructions appearing in the console prompt.</td>
</tr>
<tr>
<td></td>
<td>$ sudo /usr/TKLC/appworks/sbin/backout_restore</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Server in Question: Change runlevel to 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Bring the system back to runlevel 4.</td>
</tr>
<tr>
<td></td>
<td>$ sudo init 6</td>
</tr>
</tbody>
</table>
Procedure 6. Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td><strong>Server in Question:</strong> Verify the server</td>
</tr>
<tr>
<td></td>
<td>Verify if the processes are up and running.</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo pm.getprocs</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example output:</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Example output" /></td>
</tr>
<tr>
<td>9.</td>
<td><strong>NOAM VIP GUI:</strong> Set failed servers to active</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; HA.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Status &amp; Manage" /></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Edit.</strong></td>
</tr>
<tr>
<td></td>
<td>3. Select the failed server and set it to <strong>Active.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Modifying HA attributes" /></td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK.</strong></td>
</tr>
</tbody>
</table>
## Procedure 6. Recovery Scenario 6 (Case 1)

### 10. NOAM VIP: Verify all servers in topology are accessible (RADIUS only)

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

1. Establish an SSH session to the NOAM VIP and login as `admusr`.

2. Check if all the servers in the Topology are accessible:

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

### 11. NOAM VIP: Copy key file to all the servers in topology (RADIUS only)

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

1. Check if existing key file on active NOAM (The NOAM which is intact and was not recovered) server is valid:

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

If output of above command shows the existing key file is not valid, contact My Oracle Support (MOS).
### Procedure 6. Recovery Scenario 6 (Case 1)

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

```
$ ./sharedKrevo -synchronize
[admuser@NOAM-1 bin]$ ./sharedKrevo -synchronize
[admuser@NOAM-1 bin]$ ./sharedKrevo -updateData
```

**Note:** If any errors are present, stop and contact My Oracle Support (MOS).

12. **Backup and archive all the databases from the recovered system**

<table>
<thead>
<tr>
<th>Database Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute DSR Database Backup</td>
<td>To back up the Configuration databases.</td>
</tr>
</tbody>
</table>
4.6.2 Recovery Scenario 6: Case 2

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

Procedure 7. Recovery Scenario 6 (Case 2)

This procedure performs recovery if at least one NOAM server is available, but all SOAM servers in a site have failed. This includes any SOAM server that is in another location.

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Workarounds</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td>Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.</td>
</tr>
</tbody>
</table>
| 2.     | NOAM VIP GUI: Login | 1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: http://<Primary_NOAM_VIP_IP_Address>  
2. Login as the guiadmin user: |
Procedure 7. Recovery Scenario 6 (Case 2)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to <strong>Status &amp; Manage &gt; HA.</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Edit.</strong></td>
</tr>
<tr>
<td>3.</td>
<td><strong>NOAM VIP GUI:</strong> Set failed servers to OOS</td>
</tr>
<tr>
<td>4.</td>
<td><strong>Server in Question:</strong> Login</td>
</tr>
<tr>
<td>5.</td>
<td><strong>Server in Question:</strong> Stop httpd service</td>
</tr>
<tr>
<td>6.</td>
<td><strong>Server in Question:</strong> Take server out of service</td>
</tr>
<tr>
<td>7.</td>
<td><strong>Server in Question:</strong> Take server to DbUp state and start the application</td>
</tr>
</tbody>
</table>

1. **NOAM VIP GUI:** Set failed servers to OOS
   1. Navigate to **Status & Manage > HA.**
   2. Click **Edit.**
   3. Set the Max Allowed HA Role option to **OOS** for the failed servers.
   4. Click **OK.**

4. **Server in Question:** Login
   Establish an SSH session to the server in question. Login as **admusr.**

5. **Server in Question:** Stop httpd service
   Stop the httpd service.
   
   ```bash
   $ sudo bash -l
   
   Stop the HTTPD service before the database is down and start the HTTPD service after the database has started.
   $ service httpd stop
   
   6. **Server in Question:** Take server out of service
   Take the server out of service.
   
   ```bash
   $ prod.clobber

   7. **Server in Question:** Take server to DbUp state and start the application
   Take the server to Dbup and start the DSR application.
   
   ```bash
   $ prod.start`
## Procedure 7. Recovery Scenario 6 (Case 2)

<table>
<thead>
<tr>
<th>Server in Question: Start httpd service</th>
<th>Recovery Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>8. Start the httpd service.</td>
<td>1. Start the httpd service.</td>
</tr>
<tr>
<td></td>
<td>$ service httpd start</td>
</tr>
<tr>
<td></td>
<td>2. Exit out of root.</td>
</tr>
<tr>
<td></td>
<td>$ exit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NOAM VIP GUI: Set failed servers to active</th>
<th>Recovery Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>9. NOAM VIP GUI: Set failed servers to active</td>
<td>1. Navigate to Status &amp; Manage &gt; HA.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="HA attributes" /></td>
</tr>
<tr>
<td></td>
<td>2. Click Edit at the bottom of the screen.</td>
</tr>
<tr>
<td></td>
<td>3. Select the failed server and set it to Active.</td>
</tr>
<tr>
<td></td>
<td>4. Click OK.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NOAM VIP GUI: Restart DSR application</th>
<th>Recovery Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>10. NOAM VIP GUI: Restart DSR application</td>
<td>1. Navigate to Status &amp; Manage &gt; Server.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Server" /></td>
</tr>
<tr>
<td></td>
<td>2. Select each recovered server and click Restart.</td>
</tr>
</tbody>
</table>
## Procedure 7. Recovery Scenario 6 (Case 2)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.</td>
<td><strong>Server in Question:</strong> Verify the server state</td>
</tr>
<tr>
<td></td>
<td>1. Verify the processes are up and running:</td>
</tr>
<tr>
<td></td>
<td>$ sudo pm.getprocs</td>
</tr>
<tr>
<td></td>
<td><strong>Example output:</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image1" alt="Example output" /></td>
</tr>
<tr>
<td></td>
<td>2. Verify if replication channels are up and running:</td>
</tr>
<tr>
<td></td>
<td>$ sudo irepstat</td>
</tr>
<tr>
<td></td>
<td><strong>Example output:</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image2" alt="Example output" /></td>
</tr>
<tr>
<td></td>
<td>3. Verify if merging channels are up and running:</td>
</tr>
<tr>
<td></td>
<td>$ sudo inetmstat</td>
</tr>
<tr>
<td></td>
<td><strong>Example output:</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image3" alt="Example output" /></td>
</tr>
<tr>
<td>12.</td>
<td><strong>NOAM VIP:</strong> Verify all servers in topology are accessible (RADIUS Only). DSR only. If SDS, skip to step 14.</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>1. Establish an SSH session to the NOAM VIP and login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Check if all the servers in the Topology are accessible:</td>
</tr>
<tr>
<td></td>
<td>$ cd /usr/TKLC/dpi/bin/</td>
</tr>
<tr>
<td></td>
<td>$ ./sharedKrevo -checkAccess</td>
</tr>
</tbody>
</table>
### Procedure 7. Recovery Scenario 6 (Case 2)

<table>
<thead>
<tr>
<th></th>
<th><strong>NOAM VIP</strong>: Copy key file to all the servers in topology (RADIUS Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.</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>1. Check if existing key file on active NOAM (the NOAM which is intact and was not recovered) server is valid:</td>
</tr>
<tr>
<td></td>
<td>$ cd /usr/TKLC/dpi/bin/</td>
</tr>
<tr>
<td></td>
<td>$ ./sharedKrevo -validate</td>
</tr>
<tr>
<td></td>
<td>If output shows the existing key file is not valid, contact My Oracle Support (MOS).</td>
</tr>
<tr>
<td></td>
<td>2. Copy the key file to all the servers in the topology:</td>
</tr>
<tr>
<td></td>
<td>$ ./sharedKrevo -synchronize</td>
</tr>
<tr>
<td></td>
<td>$ ./sharedKrevo -updateData</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If any errors are present, stop and contact My Oracle Support (MOS).</td>
</tr>
<tr>
<td></td>
<td>14. Backup and archive all the databases from the recovered system</td>
</tr>
<tr>
<td></td>
<td>Execute DSR Database Backup to back up the Configuration databases.</td>
</tr>
</tbody>
</table>
5. **Resolve User Credential Issues after Database Restore**

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

5.1 **Restore a Deleted User**

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

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

5.2 **Keep a Restored User**

**Procedure 8. Keep Restored User**

<table>
<thead>
<tr>
<th>Step #</th>
<th>Before Restoration: Notify affected users before restoration</th>
<th>After Restoration: Log into the NOAM VIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Contact each user affected before the restoration and notify them that you will reset their password during this maintenance operation.</td>
<td></td>
</tr>
</tbody>
</table>
| 2.    | 1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  
<http://<Primary_NOAM_VIP_IP_Address>  
2. Login as the guiadmin user: |
Procedure 8. Keep Restored User

1. Navigate to Administration > Access Control > Users.

2. Select the user.

3. Click Change Password.

4. Type a new password.

5. Click Continue.

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 (l@#$%^*?)
### 5.3 Remove a Restored User

**Procedure 9. Remove the Restored User**

**Step #** | **Procedure** | **Description**
--- | --- | ---
1. | After Restoration: | Log into the NOAM VIP

1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:

\[
\text{http://<Primary_NOAM_VIP_IP_Address>}
\]

2. Login as the guiaadmin user:
Procedure 9. Remove the Restored User

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset user passwords</td>
<td><img src="image.png" alt="Diagram" /></td>
</tr>
</tbody>
</table>

2. Select the user.
3. Click **Delete**.

4. Click **OK** to confirm.

### 5.4 Restore a Modified User

These users have had a password change before creation of the backup and archive file. They are reverted by system restoration of that file.

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

**Before Restoration:**

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

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

**After Restoration:**

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

### 5.5 Restore an Archive that Does Not Contain a Current User

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

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

If the user is no longer desired, do not perform any additional steps. The user is permanently removed.
**Procedure 10. Restore an Archive That Does Not Contain a Current User**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Before Restoration: Notify affected users before restoration</td>
</tr>
<tr>
<td></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>
<tr>
<td>2.</td>
<td>Before Restoration: Log into the NOAM VIP</td>
</tr>
</tbody>
</table>
|        | 1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  

   `http://<Primary_NOAM_VIP_IP_Address>`  

|        | 2. Login as the `guiadmin` user: |

---

*Oracle System Login [Image]

*Log In*

Enter your username and password to log in

- **Username:** [Blank]
- **Password:** [Blank]

- [Blank] Change password

- [Log In]

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.

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

Copyright (c) 2010, 2016, Oracle and/or its affiliates. All rights reserved.
Procedure 10. Restore an Archive That Does Not Contain a Current User

3. **Before Restoration:** Record user settings

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Navigate to <strong>Administration &gt; Access Control &gt; Users</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Main Menu</td>
</tr>
<tr>
<td></td>
<td>Administration</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>General Options</td>
</tr>
<tr>
<td></td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td>Users</td>
</tr>
<tr>
<td></td>
<td>Groups</td>
</tr>
<tr>
<td></td>
<td>Sessions</td>
</tr>
<tr>
<td></td>
<td>Certificate Management</td>
</tr>
<tr>
<td></td>
<td>Authorized IPs</td>
</tr>
<tr>
<td></td>
<td>SFTP Users</td>
</tr>
<tr>
<td>2. Under each affected user, record the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Username</td>
</tr>
<tr>
<td></td>
<td>Account status</td>
</tr>
<tr>
<td></td>
<td>Remote Auth</td>
</tr>
<tr>
<td></td>
<td>Local Auth</td>
</tr>
<tr>
<td></td>
<td>Concurrent Logins Allowed</td>
</tr>
<tr>
<td></td>
<td>Inactivity Limit</td>
</tr>
<tr>
<td></td>
<td>Comment</td>
</tr>
<tr>
<td></td>
<td>Groups</td>
</tr>
</tbody>
</table>
Procedure 10. Restore an Archive That Does Not Contain a Current User

1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:

http://<Primary_NOAM_VIP_IP_Address>

2. Login as the guiadmin user:
Procedure 10. Restore an Archive That Does Not Contain a Current User

5. After restoration: recreate affected user

1. Navigate to Administration > Access Control > Users.

2. Click Insert.

3. Recreate the user using the data collected from step 3.

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

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

7. After Restoration: Reset the passwords
   See Procedure 8 for resetting passwords for a user.

6. IDIH Disaster Recovery

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

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

```xml
<infrastructure>
  ...
</infrastructure>

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

**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>
<th>PMAC GUI: Verify necessary IDIH images are available</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>1. Open web browser and enter: <a href="http://%3CPMAC_Mgmt_Network_IP%3E">http://&lt;PMAC_Mgmt_Network_IP&gt;</a>&lt;br&gt;2. Login as pmacadmin user:</td>
<td>1. Navigate to Software &gt; Manage Software Images.&lt;br&gt;2. Verify the current IDIH TVOE, TPD, Oracle, Application and Mediation images are listed.&lt;br&gt;3. Verify these values match the name in the <code>&lt;software&gt; &lt;/software&gt;</code> section in the <code>hostname-upgrade_xx-xx-xx.xml</code> file.</td>
</tr>
</tbody>
</table>

**Note:** If the necessary software images are not available, follow the instructions from the Load Application and TPD ISO onto PMAC Server procedure and steps 1-4 of IDIH Configuration from [8] to acquire and transfer the images.
### Procedure 11. IDIH Disaster Recovery Preparation

<table>
<thead>
<tr>
<th></th>
<th><strong>Oracle Guest:</strong></th>
<th><strong>Establish an SSH session to the Oracle guest, login as admusr.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Login</strong></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Perform a database health check:</td>
</tr>
<tr>
<td></td>
<td><strong>Oracle Guest:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Perform database health check</strong></td>
<td>$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i</td>
</tr>
</tbody>
</table>

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

This procedure performs disaster recovery for the IDIH by re-installing the mediation and application servers.

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>DESCRIPTION</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
</table>
| 1.     | PMAC GUI: Login | 1. Open web browser and enter:  

http://<PMAC_Mgmt_Network_IP>  

2. Login as **pmacadmin** user: |

![Oracle System Login](image)  

*Log In*  

Enter your username and password to log in  

Username: [ ]  

Password: [ ]  

Change password  

Log In  

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.  

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. |
| 2.     | Remove existing application server | 1. Navigate to **Main Menu > VM Management**.  

- [ ] Software  
  - [ ] Software Inventory  
  - [ ] Manage Software Images  
  - [ ] VM Management  

2. Select the application guest.  

3. Click **Delete**.  

![VM Management Options](image)  

- [ ] Upgrade  
- [ ] Patch |
### 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>3.</td>
<td>Remove existing mediation server</td>
</tr>
<tr>
<td></td>
<td>1. <strong>Navigate to</strong> <strong>Main Menu &gt; VM Management.</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Software</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Software Inventory</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Manage Software Images</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>VM Management</strong></td>
</tr>
<tr>
<td></td>
<td>2. <strong>Select the Mediation guest.</strong></td>
</tr>
<tr>
<td></td>
<td>3. <strong>Click Delete.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Edit Delete Clone" /></td>
</tr>
<tr>
<td>4.</td>
<td><strong>PMAC:</strong> Establish SSH session and login</td>
</tr>
<tr>
<td></td>
<td>Establish an SSH session to the PMAC, login as <strong>admusr.</strong></td>
</tr>
<tr>
<td>5.</td>
<td><strong>PMAC:</strong> Re-install the mediation and application servers</td>
</tr>
<tr>
<td></td>
<td>Execute this command (Enter your upgrade file):</td>
</tr>
<tr>
<td></td>
<td>- <code>$ cd /var/TKLC/smac/guest-dropin</code></td>
</tr>
<tr>
<td></td>
<td>- <code>$ screen</code></td>
</tr>
<tr>
<td></td>
<td>- <code>$ sudo fdconfig config --file=&lt;hostname-upgrade_xx-xx-xx&gt;.xml</code></td>
</tr>
</tbody>
</table>

---

**Warning**

If you run the fdconfig without **upgrade** in the XML filename, the database is destroyed and you lose all of the existing data.

**Note:**

**Note:** This is a long duration command (45-90 minutes). If the screen command was run before executing the fdconfig, perform a **screen -dr** to resume the screen session in the event of a terminal timeout etc.
## Procedure 12. IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

<table>
<thead>
<tr>
<th></th>
<th>PMAC GUI: Monitor the configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td></td>
</tr>
</tbody>
</table>

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

2. Navigate to **Task Monitoring**.

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

3. 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 guest-dropin]# sudo fdconfig config --file=d-ray_04-21-15.xml
   run Config
   Request to start a new configuration
   Running d-ray_04-21-15.xml configuration
   Configuration file processing complete
   Created a deployment database file: deploy_d-ray_201505117093944_630c.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
   ```
Appendix A. DSR Database Backup

Procedure 13. DSR Database Backup

This procedure backs up the provision and configuration information from an NOAM or SOAM server after the disaster recovery is complete.

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

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

<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. 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>2.</td>
<td>Login as the guiadmin user:</td>
</tr>
</tbody>
</table>

![Oracle System Login](image)
Procedure 13. DSR Database Backup

<table>
<thead>
<tr>
<th>2. NOAM/SOAM VIP: Backup configuration data for the system</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Database</strong>.</td>
</tr>
<tr>
<td>- <strong>Status &amp; Manage</strong></td>
</tr>
<tr>
<td>- Network Elements</td>
</tr>
<tr>
<td>- Server</td>
</tr>
<tr>
<td>- HA</td>
</tr>
<tr>
<td>- Database</td>
</tr>
<tr>
<td>- KPIs</td>
</tr>
<tr>
<td>- Processes</td>
</tr>
<tr>
<td>2. Select the active NOAM server and click <strong>Backup</strong>.</td>
</tr>
<tr>
<td>3. Make sure that the <strong>Configuration</strong> checkbox is marked.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Database Backup</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td><strong>Server: ZombieNOAM1</strong></td>
</tr>
<tr>
<td><strong>Select data for backup</strong></td>
</tr>
<tr>
<td><strong>Compression</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Archive Name</strong></td>
</tr>
<tr>
<td><strong>Comment</strong></td>
</tr>
<tr>
<td><strong>Ok</strong></td>
</tr>
<tr>
<td><strong>Cancel</strong></td>
</tr>
</tbody>
</table>

4. Enter a filename for the backup and click **OK**.
## Procedure 13. DSR Database Backup

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 3. NOAM/SOAM VIP: Verify the backup file existence | 1. Navigate to **Status & Manage > Files**.  
   - Select the active NOAM or SOAM tab.  
   - The files on this server display. Verify the existence of the backup file. |
| 4. NOAM/SOAM VIP: Download the file to a local machine | 1. From the previous step, select the backup file.  
   - Click **Download**.  
   - Click **OK** to confirm the download. |
| 5. Upload the image to secure location | Transfer the backed up image saved in the previous step to a secure location where the server backup files are located in case of system disaster recovery. |
| 6. Backup active SOAM | Repeat steps 2 through 5 to back up the active SOAM. |
### Procedure 13. DSR Database Backup

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Take Secured backup of key file (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>
<tr>
<td></td>
<td></td>
<td>1. Log into ssh shell of active NOAM server using user <code>admusr</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Take secure backup of updated key file <strong>RADIUS shared secret encryption key</strong> for disaster scenarios.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Encrypt the key file before backing up to secure customer setup:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ ./sharedKrevo -encr</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Copy the encrypted key file to secure customer setup:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ sudo scp /var/TKLC/db/filemgmt/DpiKf.bin.encr user@&lt;customer IP&gt;:&lt;path of customer setup&gt;</code></td>
</tr>
</tbody>
</table>

**Note:** The operator must strictly control access to the backed up key file. If the operator needs to encrypt this key file further using operator specified encryption techniques, the operator is recommended to do so; however, the operator is responsible to decrypt this file using operator-specific decryption techniques and copy the resulting `DpiKf.bin.encr` file securely to the file management folder if the key file needs to be restored for disaster recovery. Once the key file is backed up to the operator-provided server and path, it is the responsibility of the operator to ensure access to the backed up key file is extremely selective and restricted.
## Appendix B. Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only)

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

This procedure recovers a failed aggregation (4948E/4948E-F) switch.

**Prerequisites:**
- A copy of the networking xml configuration files
- A copy of HP miscellaneous firmware DVD or ISO
- IP address and hostname of the failed switch
- Rack mount position of the failed switch

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

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

| Step # | Recover failed Aggregation Switches: Cisco 4948E/4948E-F | 1. Log into the PMAC using SSH as admusr.
2. Remove the old SSH key of the switch from the PMAC by executing this command from a PMAC command shell:
   `<sudo ssh-keygen -R <4948_switch_IP>`
   **Note:** You need a copy of the HP Misc Firmware DVD or ISO (or firmware file obtained from the appropriate hardware vendor) and the original networking XML files custom for this installation. These are either stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.
   **Note:** Copy the switch appropriate init file and use it for respective switch:
   Older platform init files may not work on platform 7.2 systems. Copy the switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy `switch1A_4948_4948E_init.xml`.
4. The templates can be found using the following method:
   From the PMAC CLI:
   `df | grep -I DSR`
   **Sample output:**
   `/var/TKLC/smac/image/repository/DSR-8.4.0.0.0_84.9.0-x86_64.iso`  
   `/var/TKLC/smac/image/repository/DSR-8.4.0.0.0_84.9.0-x86_64.iso`
   `/var/TKLC/smac/image/repository/DSR-8.4.0.0.0_84.9.0-x86_64.iso`
   `/var/TKLC/smac/image/repository/DSR-8.4.0.0.0_84.9.0-x86_64.iso`
## Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F) (HP DL380 Gen 9 Only)

1. **Determine the applicable directory of the DSR release being recovered.**

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

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

2. **Locate the DSR_NetConfig_Templates.zip file.**

   **Example:**
   ```
   $ ll
   total 286
   -r--r--r-- 1 root root 611 Feb 21 19:18 change_ilo_admin_passwd.xml
   -r--r--r-- 1 root root 13346 Feb 21 19:18 DSR_NOAM_FD_RMS.xml
   dr-xr-xr-x 2 root root 2048 Feb 21 19:18 RMS
   ```

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

   **Example:**
   ```
   $ unzip DSR_NetConfig_Templates.zip
   ```

4. **Edit the desired file with site specific details.** The existing file from original deployment `/usr/TKLC/smac/etc/switch/xml` can be used as a reference.

5. **Copy the new init file to the `/usr/TKLC/smac/etc/switch/xml` dir.**

   **Example:**
   ```
   $ cp <switch_xml_file> /usr/TKLC/smac/etc/switch/xml/
   ```
Appendix C. Inhibit A and B Level Replication on C-level Servers

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

This procedure inhibits A and B level replication on all C-level servers of this site. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

1. **Active NOAM:** Login

Log into the active NOAM server using SSH as admusr.

2. **Active NOAM:** Inhibit replication on all C-level servers

Execute this command:

```
$ for i in $(iqt -p -z -h -fHostName NodeInfo where "nodeId like 'C*' and siteId='<SOAM Site_NE name of the site>'"); do iset -finhibitRepPlans='A B' NodeInfo where "nodeName='$i'"; done
```

**Note:** SOAM Site_NE name of the site can be found out by logging into the active NOAM GUI and navigating to Configuration > Server Groups.

The following figure shows more details, for example, if ServerSO1 belongs to the site being recovered, then siteID is SO_HPC03.

3. **Active NOAM:** Verify replication has been Inhibited

After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled. Verify replication inhibition on MPs by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site, for example, Site SO_HPC03 is set as A B.

```
$ iqt NodeInfo
```

**Example output:**

<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 A B</td>
<td>SO_HPC03</td>
<td></td>
</tr>
<tr>
<td>C2254.233</td>
<td>MP1</td>
<td>MP1</td>
<td>Active A B</td>
<td>SO_HPC03</td>
<td></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>Active NOAM:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Login</td>
<td>Log into the active NOAM server using SSH as admusr.</td>
</tr>
</tbody>
</table>
| 2.   | Un-Inhibit replication on all C-level servers | Execute this command: 

```bash
$ for i in $(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<SOAM_Site_NE_name>'"); do
iset -finhibitRepPlans='' NodeInfo where "nodeName='$i'";
done
```

**Note:** SOAM Site NE name of the site can be found out by logging into the active NOAM GUI and navigating to Configuration > Server Groups. Please see the snapshot below for more details, for example, if ServerSO1 belongs to the site being recovered, then siteID is SO_HPC03.

3. **Active NOAM: Verify replication has been Inhibited**

After executing above steps to un-inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled. Verify replication inhibition on MPs by analyzing NodeInfo output. The InhibitRepPlans field for all the MP servers for the selected site, for example, Site SO_HPC03 is set as A B.

```bash
$ sudo iqt NodeInfo
```

**Example output:**

```
nodeId  nodeName  hostName nodeCapability  inhibitRepPlans  siteId
A1386.099     NO1      NO1       Active                        NO_HPC03
B1754.109     SO1      SO1       Active                        SO_HPC03
C2254.131     MP2      MP2       Active             A B        SO_HPC03
C2254.233     MP1      MP1       Active             A B        SO_HPC03
```
## Appendix E. Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost)

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

This procedure inhibits A and B level replication on all C-level servers of this site when active, standby, and spare SOAMs are lost.

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Active NOAM:</th>
<th>Log into the active NOAM server using SSH as <code>admusr</code>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Active NOAM:</strong> Login</td>
<td>Execute the script from <code>/usr/TKLC/dsr/tools/InhibitReplication.sh</code>, if available. If the <code>/usr/TKLC/dsr/tools/</code> path does not have the <code>InhibitReplication.sh</code> script, then use this manual command. <code>/usr/TKLC/dsr/tools/InhibitReplication.sh --replication=inhibit --SO_SG_Name=&lt;SOAM server group name&gt;</code> Alternatively to the above script, if the script is not in the specific path:</td>
</tr>
</tbody>
</table>

*Note:* `SOAM_SG_NAME` is the name of the server group found by logging into the active NOAM GUI and navigating to **Configuration > Server Groups**.

For example, if SOAM1 belongs to the site being recovered, then the server group is **SO_SG**.

![Diagram of server groups](https://example.com/diagram.jpg)
Procedure 17. Inhibit A and B Level Replication on C-level Servers

3. Active NOAM: Verify replication has been inhibited

After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.

Verify replication inhibition on MPs by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO_SG is set as A B.

Execute this command:

```
$ iqt NodeInfo
```

Example 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>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>MF1</td>
<td>MF1</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 18. Un-Inhibit A and B Level Replication on C-Level Servers**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Active NOAM: Login</td>
<td>Log into the active NOAM server using SSH as <code>admusr</code>.</td>
</tr>
</tbody>
</table>
| 2.     | Active NOAM: Un-Inhibit replication on all C-level servers | Execute the script from `/usr/TKLC/dsr/tools/InhibitReplication.sh`, if available. If the `/usr/TKLC/dsr/tools/` path does not have the `InhibitReplication.sh` script, then use this manual command: 

```
```

*Note:* `SOAM_SG_NAME` is the name of the server group found by logging into the active NOAM GUI and navigating to **Configuration > Server Groups**.

For example, if SOAM1 belongs to the site being recovered, then the server group is SO_SG.
### Procedure 18. Un-Inhibit A and B Level Replication on C-Level Servers

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active NOAM:</strong> Verify replication has been Inhibited</td>
<td>After executing above steps to un-inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled. Verify replication inhibition on MPs by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO_SG is set as A B. Execute this command:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>$ sudo iqt NodeInfo</td>
<td>Example output:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>nodeId</td>
<td>nodeName</td>
<td>hostName</td>
<td>nodeCapability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A1386.099</td>
<td>NO1</td>
<td>NO1</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B1754.109</td>
<td>SO1</td>
<td>SO1</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C2254.131</td>
<td>MP2</td>
<td>MP2</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C2254.233</td>
<td>MP1</td>
<td>MP1</td>
<td>Active</td>
</tr>
</tbody>
</table>
### Appendix G. Restore TVOE Configuration from Backup Media

#### Procedure 19. Restore TVOE Configuration from Backup Media

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Install TVOE application</td>
<td>- If the PMAC is NOT hosted on the failed rack mount server, execute <strong>IPM Servers Using PMAC Application</strong> from reference [8].&lt;br&gt;- If the PMAC is hosted on the failed rack mount server, execute <strong>Installing TVOE on the Management Server</strong> from reference [8].</td>
</tr>
<tr>
<td>2.</td>
<td>Establish network connectivity</td>
<td>- If the PMAC is NOT hosted on the failed rack mount server, <strong>skip this step</strong>.&lt;br&gt;- If the PMAC is hosted on the failed rack mount server, execute <strong>TVOE Network Configuration</strong>, steps 1-11, from reference [8].&lt;br&gt;&lt;strong&gt;Note:&lt;/strong&gt; The IP address configured on the TVOE must be one accessible through the network of the machine currently holding the TVOE Backup ISO image. This could be a NetBackup master server, a customer PC, etc.</td>
</tr>
<tr>
<td>3.</td>
<td>Restore TVOE backup ISO image to the TVOE host (NetBackup)</td>
<td>If using NetBackup to restore the TVOE backup ISO image, then execute this step; otherwise, skip this step.&lt;br&gt;1. Execute <strong>Application NetBackup Client Installation Procedures</strong> from reference [8].&lt;br&gt;2. Interface with the NetBackup master server and initiate a restore of the TVOE backup ISO image.&lt;br&gt;&lt;strong&gt;Note:&lt;/strong&gt; Once restored, the ISO image is in <code>/var/TKLC/bkp/</code> on the TVOE server.</td>
</tr>
</tbody>
</table>
## Procedure 19. Restore TVOE Configuration from Backup Media

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| 4.   | Transfer TVOE backup ISO image to the TVOE host | Restore TVOE backup ISO using SCP. Using the IP of the TVOE host, transfer the backup ISO image to the TVOE.  
**Linux:**  
From the command line of a Linux machine use this command to copy the backup ISO image to the TVOE host:  
```bash  
# scp <path_to_image> tvoexfer@<TVOE_IP>:backup/  
```

**Notes:**  
- If the IP is an IPv4 address, then `<TVOE_IP>` is a normal dot-decimal notation (for example, 10.240.6.170).  
- If the IP is an IPv6 link local address, then `<TVOE_IP>` needs to be scoped. For example, `[fe80::21e:bff:fe76:5e1c%control]` where control is the name of the interface on the machine initiating the transfer and it must be on the same link as the interface on the TVOE host.  
- The control IP address of the TVOE can be used if the TVOE is NOT hosting the PMAC. This method requires first transferring the backup file to the PMAC, and then to the TVOE host.  

**IPv4 Example:**
```bash  
# scp /path/to/image.iso tvoexfer@10.240.6.170:backup/  
```

**IPv6 Example:**
```bash  
# scp /path/to/image.iso  
tvoexfer@[fe80::21e:bff:fe76:5e1c%control]:backup/  
```

**Windows:**  
Use WinSCP to copy the Backup ISO image into the `/var/TKLC/bkp` directory. Refer to [8], the Using WinSCP procedure, to copy the backup image to the customer system. |
| 5.   | TVOE Server: Login                         | Establish an SSH session to the TVOE server and login as `admusr`.                             |
Procedure 19. Restore TVOE Configuration from Backup Media

1. Restore the TVOE backup ISO by executing this command:

   $ sudo su - platcfg


3. Select the desired archive.

4. Click OK.

5. Click Restore Backup Archive.

6. Confirm restore.
### Procedure 19. Restore TVOE Configuration from Backup Media

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Wait for the restore to complete.</td>
</tr>
<tr>
<td>2.</td>
<td>Exit platcfg.</td>
</tr>
<tr>
<td>7.</td>
<td>Monitor TVOE backup process</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This typically takes less than 5 minutes.</td>
</tr>
<tr>
<td>8.</td>
<td><strong>TVOE Server:</strong> Exit restore backup menu</td>
</tr>
</tbody>
</table>

Exit the Restore Backup Menu.

```
1qqu Restore Backup Menu tqqk
  x  x
  Select Backup Media  x
  View Table of Contents  a  x
  Change Restore Dir  a  x
  Restore Backup Archive  x
  Exit  x
```

```
lu Backup and Restore Menu tqqk
  x  x
  Backup Platform(CD/DVD)  x
  Backup Platform(USB)  a  x
  Restore Platform  a  x
  Restore USB Archive  x
  Exit  x
```

### Procedure 19. Restore TVOE Configuration from Backup Media

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td>TVOE Server: Restart</td>
</tr>
</tbody>
</table>

1. Restart the TVOE server.

```
1qqqqu Maintenance Menu tqqqqqk
x x x
x Upgrade x
x Halt Server a x
x Backup and Restore a x
x Restart Server x
x Eject CDROM a x
x Save Platform Debug Logs a x
x Exit x
```

2. Click **Yes** to restart.

```
1qqqqqk 1qqqqqk
x x
x Do you wish to restart the server?
```

3. Confirm restart.

```
1qqqqqk 1qqqqqk
x x
x Are you sure you want to restart the server?
```
### Procedure 19. 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>

1. **TVOE Server:** Wait for restart to successfully complete.

2. **TVOE Server:** Verify storage pools are active.

   1. Login as `admusr`.
   2. Verify all storage pools are listed and are in the active state:

   ```bash
   $ sudo virsh -c "qemu:///system" pool-list
   
   [admusr@S01-0441-TVOE ~]$ sudo virsh -c "qemu:///system" pool-list
   
   Name         State   Autostart
   vqguests     active   yes
   
   [admusr@S01-0441-TVOE ~]$ 
   ```

   **Note:** If any storage pools are missing or inactive, contact My Oracle Support (MOS).
### Procedure 19. Restore TVOE Configuration from Backup Media

<table>
<thead>
<tr>
<th>Step</th>
<th>TVOE Server: Enable HIDS (Optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.</td>
<td><strong>Note:</strong> Enabling HIDS is optional. This step is skipped if HIDS is not required to be enabled. When enabling HIDS, update the baseline so the restored files are not reported as being tampered with. Execute these commands from the TVOE host remote console to enable HIDS and update the baseline:</td>
</tr>
</tbody>
</table>

- `$ /usr/TKLC/plat/bin/hidsMgr -initialize`
  - LOG: HIDS monitoring has been Initialized
  - HIDS baseline has been initialized
- `$ /usr/TKLC/plat/bin/hidsMgr --enable`
  - HIDS monitoring has successfully been enabled
  - **New State:** ENABLED
- `$ /usr/TKLC/plat/bin/hidsMgr --update --all`
  - HIDS baseline has successfully been updated
Procedure 19. Restore TVOE Configuration from Backup Media

13. TVOE Server: Verify alarms

 Verify alarms:

$ sudo su - platcfg

2. Click Diagnostics.

3. Click Alarm Manager.

4. Click Show Alarm Status.

If there are any failures, contact My Oracle Support (MOS).
## Appendix H. Restore PMAC from Backup

### Procedure 20. Restore PMAC from Backup Media

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

**Prerequisite:** TVOE management server has been restored.

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

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

### Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Deploy the PMAC guest&lt;br&gt;Execute Install PMAC from reference [8].</td>
</tr>
<tr>
<td>2.</td>
<td>PMAC: Login&lt;br&gt;Establish an SSH session to the PMAC server and login as admusr.</td>
</tr>
</tbody>
</table>
| 3. | Restore PMAC Backup image to the PMAC host<br>From the remote backup location, copy the backup file to the deployed PMAC. There are too many possible backup scenarios to cover them all here. This example is a simple scp from a redundant PMAC backup location. If using IPv6 addresses, the command requires shell escapes, for example, admusr@[<ipV6addr>]:/<file>  
**Note:** Execute the scp command from the recovered PMAC and the backup file is pulled/retrieved from the backup location.  
```bash
$ sudo /usr/bin/scp -p
admsur@<remoteserver>:/var/TKLC/smac/backup/*.pef
/var/TKLC/smac/backup/>
```
**Note:** It is important to copy the correct backup file to use in the restore. The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PMAC before the restoration of the data. |
| 4. | PMAC: Verify no Alarms are present<br>Verify no alarms are present.  
```bash
$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus
```
| 5. | Restore the PMAC Data from Backup<br>1. Restore the PMAC data from backup.  
```bash
$ sudo /usr/TKLC/smac/bin/pmacadm restore  
PM&C Restore been successfully initiated as task ID 1
```
2. Check the status of the background task.  
```bash
$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks
```
**Note:** The result eventually displays PMAC Restore successful. |
Procedure 20. Restore PMAC from Backup Media

<table>
<thead>
<tr>
<th></th>
<th>PMAC GUI: Login</th>
<th>1. Open web browser and navigate to the PMAC GUI.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2. Login as <strong>PMACadmin</strong> user:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>https://&lt;pmac_network_ip&gt;</strong></td>
</tr>
</tbody>
</table>

### Oracle System Login

```
Log In
Enter your username and password to log in
Username: [
Password: [ ]
Change password [ ]
Log In
```

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.

_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.

<table>
<thead>
<tr>
<th></th>
<th>PMAC GUI: Verify restore task completed</th>
<th>1. Navigate to <strong>Task Monitoring</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2. Verify the restore background task completed successfully.</td>
</tr>
</tbody>
</table>

**Note:** After the restore is complete, you should see **Add Enclosure** tasks start for all previously provisioning servers. These should be allowed to complete before continuing.

**Note:** After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior. ISO images are added in the next step.
Procedure 20. Restore PMAC from Backup Media

8. **PMAC GUI:** Verify system inventory
   1. Navigate to **Hardware > System Inventory.**
      - **Main Menu**
        - **Hardware**
          - **System Inventory**
            - **Cabinet 1**
            - **Cabinet 2**
            - **Cabinet 101**
            - **Cabinet Undesignated**
            - **FRU Info**
   2. Verify previously provisioned enclosures are present.

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

10. **PMAC:** Add ISO images to the PMAC
    - Re-add any needed ISO images to the PMAC by executing procedure **Load DSR, SDS (Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only), and TPD ISOs to the PMAC Server** from reference [8] for all required ISO images.
Procedure 21. Restore PMAC from Backup Server

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

**Prerequisite:** The TVOE management server has been restored.

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Execution</th>
</tr>
</thead>
</table>
| 1.   | Deploy the PMAC guest | Execute **Install PMAC** from reference [8].

**Note:** This procedure is for restoring from a NetBackup server, so specify the appropriate options when deploying PMAC for use with NetBackup.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Execution</th>
</tr>
</thead>
</table>
| 2.   | **PMAC TVOE Host:** Login | Establish an SSH session to the PMAC TVOE Host, login as **admusr**.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Execution</th>
</tr>
</thead>
</table>
| 3.   | **PMAC TVOE Host:** Log into PMAC guest console | 1. On the TVOE host, execute this command:

```
$sudo virsh list
```

This produces a listing of currently running virtual machines.


<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Execution</th>
</tr>
</thead>
</table>
| 4.   | Connect to console of the VM using the VM number obtained in step 3 | On the TVOE host, execute this command:

```
$sudo virsh console <PMAC-VMID>
```

Where PMAC-VMID is the VM ID you obtained in step 3:

```
[admusr@ahu-tvoe-1 ~]$ sudo virsh console 1
Connected to domain Oahu-PMAC
Escape character is "^".

Oracle Linux Server release 6.7
Kernel 2.6.32-573.3.1.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 21. Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</th>
<th>Execute these commands on the PMAC.</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>□</td>
<td>$ sudo /sbin/service iptables stop</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>$ sudo /usr/TKLC/smac/etc/services/netbackup start</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>Modified menu NBConfig</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>-- show</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>Set the following menus: NBConfig to visible=1</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>Modified menu NBInit</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>-- show</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>Set the following menus: NBInit to visible=1</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>Modified menu NBDeInit</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>-- show</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>Set the following menus: NBDeInit to visible=1</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>Modified menu NBInstall</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>-- show</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>Set the following menus: NBInstall to visible=1</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>Modified menu NBVerifyEnv</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>-- show</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>Set the following menus: NBVerifyEnv to visible=1</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>Modified menu NBVerify</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>-- show</td>
</tr>
<tr>
<td></td>
<td>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</td>
<td>Set the following menus: NBVerify to visible=1</td>
</tr>
</tbody>
</table>
### Procedure 21. Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC:</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>Verify the TPD platcfg backup menus are visible, then exit the TPD platcfg Utility</td>
<td>Verify the TPD platcfg backup menus are visible.</td>
</tr>
<tr>
<td></td>
<td>$ sudo /bin/su - platcfg</td>
<td><img src="image" alt="TPD platcfg Utility" /></td>
</tr>
</tbody>
</table>

**Note:** In the example image above of the TPD platcfg utility Main Menu the backup menu is identified as **NetBackup Configuration**.

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC:</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Verify the iptables rules are disabled on the PMAC guest</td>
<td>Verify the iptables rules are disabled on the PMAC guest.</td>
</tr>
</tbody>
</table>
|      | $ sudo /sbin/iptables -nL | **INPUT** (policy ACCEPT)  
Target prot opt source destination  
Chain FORWARD (policy ACCEPT)  
Target prot opt source destination  
Chain OUTPUT (policy ACCEPT)  
Target prot opt source destination |

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC:</th>
<th>Action</th>
</tr>
</thead>
</table>
**Note:** The **Initialize PMAC Application** and **Configure PMAC Application** prerequisites can be ignored. |

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 9.   | This step is likely executed by customer IT personnel.  
1. Log into the backup server as the appropriate user using the user password.  
2. Execute the appropriate commands to verify the PMAC backup exists for the desired date.  
**Note:** The actions and commands required to verify the PMAC backups exist and the commands required to perform backup and restore on the backup server are the responsibility of the site customer.  
**Note:** It is important to select the correct backup file to use in the restore. The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PMAC before the restoration of the data. |
### Procedure 21. Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| 10.  | **Backup Server:** Verify appropriate PMAC backup exists | This step is likely executed by customer IT personnel.  
1. Log into the backup server as the appropriate user using the user password.  
2. Execute the appropriate commands to verify the PMAC backup exists for the desired date.  
3. Execute the appropriate commands to restore the PMAC management server backup for the desired date.  
**Note:** The actions, and commands, required to verify the PMAC backups exist, and the commands required to perform backup and restore on the backup server are the responsibility of the site customer. |
| 11.  | **PMAC:** Verify no alarms are present | Verify no alarms are present.  
$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus |
| 12.  | Restore the PMAC data from backup |  
1. Restore the PMAC data from backup.  
   $ sudo /usr/TKLC/smac/bin/pmacadm restore  
   PM&C Restore been successfully initiated as task ID 1  
2. Check the status of the background task:  
   $ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks  
**Note:** The result eventually displays PMAC Restore successful. |
### Procedure 21. Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 13. | **PMAC GUI:** Login  
1. Open web browser and navigate to the PMAC GUI.  
   ![PMAC GUI](https://<pmac_network_ip>)  
2. Login as **PMACadmin** user: |

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 14. | **PMAC GUI:** Verify restore task completed  
1. Navigate to **Task Monitoring**.  
2. Verify the restore background task completed successfully.  
   **Note:** After the restore is complete, you should see **Add Enclosure** tasks start for all previously provisioning servers. These should be allowed to complete before continuing.  
   **Note:** After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior. ISO images are added in the next step. |
Procedure 21. Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.</td>
<td>PMAC GUI: Verify system inventory</td>
<td>1. Navigate to <strong>Hardware &gt; System Inventory</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Main Menu]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Hardware]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[System Inventory]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Cabinet 1]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Cabinet 2]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Cabinet 101]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Cabinet Undesignated]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[FRU Info]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Verify previously provisioned enclosures are present</td>
</tr>
<tr>
<td>16.</td>
<td>PMAC: Verify PMAC</td>
<td>Perform a system health check on the PMAC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This command should return no output on a healthy system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/smac/bin/sentry status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All processes should be running, displaying output similar to the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PM&amp;C Sentry Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sentryd started: Mon Jul 23 17:50:49 2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Current activity mode: ACTIVE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process PID Status StartTS NumR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>smacTalk 9039 running Tue Jul 24 12:50:29 2012 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>smacMon 9094 running Tue Jul 24 12:50:29 2012 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>snmpEventHandler 9176 running Tue Jul 24 12:50:29 2012 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fri Aug 3 13:16:35 2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Command Complete.</td>
</tr>
<tr>
<td>17.</td>
<td>PMAC: Add ISO images to the PMAC</td>
<td>Re-add any needed ISO images to the PMAC by executing procedure <strong>Load</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Application and TPD ISO onto PMAC Server</strong> from reference [8].</td>
</tr>
</tbody>
</table>
Appendix I. Restore Provisioning Database

Procedure 22. Restore Provisioning Database

This procedure restores the SDS provisioning database. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

1. **Primary SDS NOAM GUI:** Log into primary SDS NOAM GUI using its static IP (not the VIP).

2. **Primary SDS NOAM GUI:** Place the newly recovered standby NOAM into forced standby.
   1. Navigate to Status & Manage > HA.
   2. Click Edit.
   3. Move the newly recovered standby server to forced Standby.

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>rightsci-sds-a-a</td>
<td>Active</td>
<td>The maximum desired HA Role for rightsci-sds-a-a</td>
</tr>
<tr>
<td>rightsci-sds-a-b</td>
<td>Standby</td>
<td>The maximum desired HA Role for rightsci-sds-a-b</td>
</tr>
<tr>
<td>rightsci-sds-os</td>
<td>Observer</td>
<td>The maximum desired HA Role for rightsci-sds-os</td>
</tr>
</tbody>
</table>

3. **Primary SDS NOAM GUI:** Restore provisioning data.
   1. Navigate to Status & Manage > Database.
   2. Select the active NOAM and click Restore.

Main Menu: Status & Manage -> Database

3. Select the Provisioning backup file from the list (which was previously placed...
### Procedure 22. Restore Provisioning Database

In the `/var/TKLC/db/filemgmt/backup` directory in step 5 of section 2.6.2) and click OK.

**Note:** You must use a provisioning only backup file. Combined backup files contain configuration and provisioning data and cause catastrophic issues, which could lead to a complete re-installation.

#### Main Menu: Status & Manage -> Database [Restore]

<table>
<thead>
<tr>
<th>Database Restore</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select archive to Restore on server: mrsync-sds-N0-a</strong></td>
</tr>
<tr>
<td>- backupBackup.sds rhgnc-sds-N0-b.Configuration NETWORK_OAMP_20170316_021512.AUTO.tar.gz</td>
</tr>
<tr>
<td>- backupBackup.sds rhgnc-sds-N0-b.Provisioning NETWORK_OAMP_20170316_021512.AUTO.tar.gz</td>
</tr>
<tr>
<td>- backupBackup.sds rhgnc-sds-N0-b.Configuration NETWORK_OAMP_20170317_021512.AUTO.tar.gz</td>
</tr>
<tr>
<td>- backupBackup.sds rhgnc-sds-N0-b.Provisioning NETWORK_OAMP_20170317_021512.AUTO.tar.gz</td>
</tr>
<tr>
<td>- backupBackup.sds rhgnc-sds-N0-b.Configuration NETWORK_OAMP_20170318_021512.AUTO.tar.gz</td>
</tr>
<tr>
<td>- backupBackup.sds rhgnc-sds-N0-b.Provisioning NETWORK_OAMP_20170318_021512.AUTO.tar.gz</td>
</tr>
<tr>
<td>- backupBackup.sds rhgnc-sds-N0-b.Configuration NETWORK_OAMP_20170319_021512.AUTO.tar.gz</td>
</tr>
<tr>
<td>- backupBackup.sds rhgnc-sds-N0-b.Provisioning NETWORK_OAMP_20170319_021512.AUTO.tar.gz</td>
</tr>
<tr>
<td>- backupBackup.sds rhgnc-sds-N0-b.Configuration NETWORK_OAMP_20170320_021512.AUTO.tar.gz</td>
</tr>
<tr>
<td>- backupBackup.sds rhgnc-sds-N0-b.Provisioning NETWORK_OAMP_20170320_021512.AUTO.tar.gz</td>
</tr>
</tbody>
</table>

4. Verify compatibility and click OK to restore.

#### Main Menu: Status & Manage -> Database [RestoreConfirm]

<table>
<thead>
<tr>
<th>Database Restore Confirm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The selected database came from rhgnc-sds-N0-b on 03/27/2017 at 02:15:12 GMT and contains the following comment: Highly sensitive.</strong></td>
</tr>
</tbody>
</table>

4. **Primary SDS NOAM GUI:**

   1. Wait 60 seconds for the restore to begin.
   2. Monitor the Info tab under the **Status & Manage > Database** screen and look for the following message:
      
      ```
      Restore on <Active_NO_hostname> status MAINT_IN_PROGRESS.
      ```
   3. Wait for the restore to complete by looking for the following message:
      
      ```
      Success: - Restore on rhgnc-sds-N0 status MAINT_CMD_SUCCESS.
      ```

   **Note:** Refresh the Info tab manually to see updated status by navigating to **Status & Manage > Database** again and selecting the Info tab.
Procedure 22. Restore Provisioning Database

5. **Primary SDS NOAM GUI: Uninhibit servers**

   Uninhibit all servers in the following staggered arrangement:
   1. Uninhibit active NOAM.
   
   Refresh/monitor the **Status & Manage > Database** screen until a valid DB Level displays for the active NOAM.
   2. Uninhibit **standby** NOAM/Query server.
   
   Refresh/monitor the **Status & Manage > Database** screen until a valid DB Level displays for the standby NOAM/Query server.
   3. Uninhibit active SOAMs.
   
   Refresh/monitor the **Status & Manage > Database** screen until a valid DB Level displays for the active SOAMs.
   4. Uninhibit **standby** SOAMs/DPs.
   
   Refresh/monitor the **Status & Manage > Database** screen until a valid DB Level displays for the standby SOAMs/DPs.

6. **Recover Pdbrelay (if needed)**

   Verify whether PDB Relay is **Enabled** by following the instructions in Appendix J Recover PDB Relay.

7. **Primary SDS NOAM GUI: Enable provisioning**

   Navigate to **Status & Manage > Database** and click **Enable Provisioning**.

   ![Image of Status & Manage > Database screen with enabled provisioning](image-url)
### Procedure 22. Restore Provisioning Database

**8. NOAM GUI: Remove NO from forced standby**

1. Navigate to **Status & Manage > HA** and click **Edit**.
2. Select the server, which was moved to forced standby in step 2, change **Max HA Role** to **Active**, and click **OK**.

**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>rightnc-sds-NO-a</td>
<td>Active</td>
<td>The maximum desired HA Role for rightnc-sds-NO-a</td>
</tr>
<tr>
<td>rightnc-sds-NO-b</td>
<td>Active</td>
<td>The maximum desired HA Role for rightnc-sds-NO-b</td>
</tr>
<tr>
<td>rightnc-sds-QS</td>
<td>Observer</td>
<td>The maximum desired HA Role for rightnc-sds-QS</td>
</tr>
</tbody>
</table>
# Appendix J. Recover PDB Relay

## Procedure 23. Recover PDB Relay

<table>
<thead>
<tr>
<th>STEP #</th>
<th>NOAM VIP console:</th>
<th>Execute following command on console of Active NOAM server (accessed via the VIP) and compare the output:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 0</td>
<td>Determine if pdbrelay is enabled</td>
<td>$ iqt -zhp -fvalue ProvOptions where &quot;var='pdbRelayEnabled'&quot; TRUE</td>
</tr>
</tbody>
</table>

Proceed to next step only if the result of above command is true.

<table>
<thead>
<tr>
<th>STEP #</th>
<th>NOAM VIP GUI:</th>
<th>Unmark the PDB Relay Enabled checkbox on the SDS &gt; Configuration &gt; Options screen and click Apply.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. 0</td>
<td>Disable pdbrelay</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STEP #</th>
<th>NOAM VIP Console:</th>
<th>Execute following command on console:</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. 0</td>
<td>Emergency restart (start from beginning of Cmd log)</td>
<td>$ iset -fvalue=0 ProvOptions where &quot;var='pdbRelayMsgLogTimeStamp'&quot;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STEP #</th>
<th>NOAM VIP GUI:</th>
<th>Mark the PDB Relay Enabled checkbox on the SDS &gt; Configuration &gt; Options screen and click Apply.</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. 0</td>
<td>Enable pdbrelay</td>
<td></td>
</tr>
</tbody>
</table>
Appendix K. SNMP Configuration

Procedure 24. Configure SNMP

This workaround configures SNMP with SNMPv2c and SNMPv3 as the enabled versions for SNMP traps configuration since PMAC does not support SNMPv3. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

1. (Workaround) NOAM VIP GUI: Login

   **Note:** This workaround step should be performed only in the following cases:
   1. If SNMP is not configured.
   2. If SNMP is already configured and SNMPv3 is selected as enabled version.

   **Note:** This is a workaround step to configure SNMP with ‘SNMPv2c and SNMPv3’ as the enabled versions for SNMP Traps configuration, since PMAC does not support SNMPv3.

1. If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server.

2. Open the web browser and enter a URL of:

   http://<Primary_NOAM_VIP_IP_Address>

3. Log into the NOAM GUI as the guiadmin user:

   ![Oracle System Login](image)

   Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.
**Procedure 24. Configure SNMP**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to Administration &gt; Remote Servers &gt; SNMP Trapping.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the Server Group tab for SNMP trap configuration:</td>
</tr>
<tr>
<td>3.</td>
<td>Type the <strong>IP address</strong> or <strong>hostname</strong> of the Network Management Station (NMS) where you want to forward traps. This IP should be reachable from the NOAM's XMI network. If already configured SNMP with <strong>SNMPv3</strong> as enabled version, another server needs to be configured here.</td>
</tr>
<tr>
<td>4.</td>
<td>Continue to fill in additional secondary, tertiary, etc., <strong>Manager IPs</strong> in the corresponding slots if desired.</td>
</tr>
<tr>
<td>5.</td>
<td>Set the <strong>Enabled Versions</strong> as <strong>SNMPv2c and SNMPv3</strong>.</td>
</tr>
<tr>
<td>6.</td>
<td>Check <strong>Traps Enabled</strong> checkboxes for the Manager servers being configured.</td>
</tr>
<tr>
<td>7.</td>
<td>Type the <strong>SNMP Community Name</strong>.</td>
</tr>
<tr>
<td>8.</td>
<td>Leave all other fields at their default values.</td>
</tr>
<tr>
<td>9.</td>
<td>Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
### Procedure 24. Configure SNMP

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 3.   | **NOAMP VIP:** Enable traps from individual servers (optional)  
**Note:** By default SNMP traps from MPs are aggregated and displayed at the active NOAMP. If, instead, you want every server to send its own traps directly to the NMS, then execute this procedure.  
This procedure requires all servers, including MPs, to have an XMI interface on which the customer SNMP target server (NMS) is reachable.  
1. Navigate to Administration > Remote Servers > SNMP Trapping.  
2. Make sure the **Enabled** checkbox is marked.  
3. Click **Apply** and verify the data is committed. |

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 4.   | **PMAC GUI:** Update the TVOE host SNMP community string  
1. Establish an SSH session to the PMAC.  
2. Login as **admuser** user:  
3. Update the TVOE host community string with this command:  
```
$ 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 are updated. All those servers that match the existing Site Specific Community String are not updated again until the string name is changed. |
## Appendix L. Backup Directory

### Procedure 25. Backup Directory

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>NOAM/SOAM VIP Console: Determine if backup directory exists</td>
</tr>
<tr>
<td>2.</td>
<td>NOAM/SOAM VIP Console: Create backup directory</td>
</tr>
</tbody>
</table>

#### 1. NOAM/SOAM VIP Console: Determine if backup directory exists

1. Execute this command an active NOAM/SOAM server console (accessed using the VIP) and compare the output.

   ```
   $ cd /var/TKLC/db/filemgmt/
   $ ls -ltr
   ```

2. Look for the backup directory in the output.

3. Make sure the directory is already created with correct permission. The directory looks like this:

   ```
   drwxrwx--- 2 awadmin awadm 4096 Dec 19 02:15 backup
   ```

4. If the directory is already there with correct permissions, then skip steps 2 and 3.

5. If directory does not have the correct permissions, then go to step 3.

#### 2. NOAM/SOAM VIP Console: Create backup directory

1. Go to the backup directory location.

   ```
   cd /var/TKLC/db/filemgmt/
   ```

2. Create backup directory.

   ```
   $ mkdir backup
   ```

3. Verify directory has been created.

   ```
   $ ls -ltr /var/TKLC/db/filemgmt/backup
   ```

*Note:* A **No such file or directory** error message should not display. The directory should show as empty with the total as 0 for content.
### Procedure 25. Backup Directory

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td><strong>NOAM/SOAM VIP Console:</strong> Change permissions of backup directory</td>
<td>1. Verify directory has been created.</td>
</tr>
</tbody>
</table>
|      |                                                                                                  | ```bash
ls -ltr /var/TKLC/db/filemgmt/backup
```                                                                                           |
|      |                                                                                                  | *Note:* A *No such file or directory* error message should not display. The directory should show as empty with the total as 0 for content. |
|      |                                                                                                  | 2. Change permissions for the backup directory.                                                    |
|      |                                                                                                  | ```bash
chmod 770 /var/TKLC/db/filemgmt/backup
```                                                                                           |
|      |                                                                                                  | 3. Change ownership of backup directory.                                                           |
|      |                                                                                                  | ```bash
sudo chown -R awadmin:awadm /var/TKLC/db/filemgmt/backup
```                                                                                           |
|      |                                                                                                  | 4. Directory displays as follows:                                                                  |
|      |                                                                                                  | ```bash
drwxrwx--- 2 awadmin awadm 4096 Dec 22 02:15
backup
```                                                                                           |
| 4.   | **NOAM/SOAM VIP Console:** Copy the backup file to the backup directory                           | 1. Copy the backup file to the backup directory.                                                    |
|      |                                                                                                  | ```bash
cp BACKUPFILE /var/TKLC/db/filemgmt/backup
```                                                                                           |
|      |                                                                                                  | 2. Change permissions of files in the backup directory.                                             |
|      |                                                                                                  | ```bash
chmod 666 Backup.*
```                                                                                           |
|      |                                                                                                  | 3. Change ownership of files in the backup directory.                                               |
|      |                                                                                                  | ```bash
sudo chown -R awadmin:awadm Backup.*
```                                                                                           |
Appendix M. netConfig
backupConfiguration/restoreConfiguration/upgradeFirmware with TPD cipher change

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

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

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

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

This procedure prepares the PM&C to avoid the cipher mismatch issue with Cisco switches. This is performed before the netConfig backup, restore or upgrade operations.

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>□ Turn off cipher list</td>
<td>From the PMAC shell enter the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/usr/bin/sudo /bin/vi /etc/ssh/sshd_config</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Add # in the beginning of the following three lines to comment them out, the result is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>#Ciphers aes256-ctr,aes192-ctr,aes128-ctr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>#MaxAuthTries 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>#LoginGraceTime 1m</td>
</tr>
<tr>
<td>2</td>
<td>□ Restart sshd</td>
<td>/usr/bin/sudo service sshd restart</td>
</tr>
<tr>
<td>STEP #</td>
<td>Procedure</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 3      | Run the netConfig backupConfiguration/restoreConfiguration/upgradeFirmware command | For a backup operation: 
[admusr@pmac ~]$ /usr/bin/sudo /usr/TKLC/plat/bin/netConfig backupConfiguration --device=<switch_name> service=<ssh_service> filename=<switch_name>-backup  
For a restore operation: 
[admusr@pmac ~]$ /usr/bin/sudo /usr/TKLC/plat/bin/netConfig restoreConfiguration --device=<switch_name> service=<ssh_service> filename=<switch_name>-backup  
For a upgrade operation: 
[admusr@pmac ~]$ /usr/bin/sudo /usr/TKLC/plat/bin/netConfig upgradeFirmware --device=<switch_name> service=<ssh_service> filename=<Cisco IOS> |

**Procedure 27. Resume cipher list after backupConfiguration/restoreConfiguration/upgradeFirmware command**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1      | Resume the cipher list | From the PMAC shell enter the following: 
/usr/bin/sudo /bin/vi /etc/ssh/sshd_config  
Uncomment the three lines:  
Ciphers aes256-ctr,aes192-ctr,aes128-ctr  
MaxAuthTries 4  
LoginGraceTime 1m |
| 2      | Restart sshd | /usr/bin/sudo service sshd restart |
Appendix N. My Oracle Support (MOS)

My Oracle Support

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

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

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select 1.
   - For non-technical issues such as registration or assistance with MOS, select 2.

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

Emergency Response

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

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

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

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

Locate Product Documentation on the Oracle Help Center

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

2. Click Industries.
3. Under the Oracle Communications subheading, click the Oracle Communications documentation link. The Communications Documentation page appears. Most products covered by
these documentation sets display under the headings **Network Session Delivery and Control Infrastructure** or **Platforms**.

4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release displays. To download a file to your location, right-click the PDF link, select **Save target as** (or similar command based on your browser), and save to a local folder.