Oracle Communications DSR C-Class Disaster Recovery User’s Guide, Release 8.2

Copyright © 2017, 2018 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 Optional Features ........................................................................................................................................ 8  
2. **General Description** ............................................................................................................................... 8  
   2.1 Complete Server Outage (All Servers) ........................................................................................................ 9  
   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 .......................................................... 10  
   2.5 Partial Service Outage with Corrupt Database ....................................................................................... 10  
3. **Procedure Overview** ............................................................................................................................. 10  
   3.1 Required Materials ..................................................................................................................................... 10  
   3.2 Disaster Recovery Strategy ...................................................................................................................... 11  
4. **Disaster Recovery Procedure** ............................................................................................................... 13  
   4.1 Recovery Scenario 1 (Complete Server Outage) ....................................................................................... 13  
   4.2 Recovery Scenario 2 (Partial Server Outage with One NOAM Server Intact and ALL SOAMs Failed) 47  
   4.3 Recovery Scenario 3 (Partial Server Outage with All NOAM Servers Failed and One SOAM Server Intact) ............................................................................................................................................... 73  
   4.4 Recovery Scenario 4 (Partial Server Outage with One NOAM Server and One SOAM Server Intact) 96  
   4.5 Recovery Scenario 5 (Both NOAM Servers Failed with DR-NOAM Available) ..................................... 116  
   4.6 Recovery Scenario 6 (Database Recovery) .............................................................................................. 124  
      4.6.1 Recovery Scenario 6: Case 1 .................................................................................................................. 124  
      4.6.2 Recovery Scenario 6: Case 2 ................................................................................................................ 130  
5. **Resolve User Credential Issues after Database Restore** ....................................................................... 135  
   5.1 Restore a Deleted User ............................................................................................................................. 135  
   5.2 Keep a Restored User ............................................................................................................................... 135  
   5.3 Remove a Restored User .......................................................................................................................... 137  
   5.4 Restore a Modified User .......................................................................................................................... 138  
   5.5 Restore an Archive that Does Not Contain a Current User ................................................................. 138  
6. **IDIH Disaster Recovery** ......................................................................................................................... 143  
   Appendix A. **DSR Database Backup** ........................................................................................................ 148  
   Appendix B. **Recover/Replace Failed 3rd Party Components (Switches, OAs)** ..................................... 152  
   Appendix C. **Inhibit A and B Level Replication on C-level Servers** ......................................................... 157
Appendix D.  Un-Inhibit A and B Level Replication on C-level Servers ........................................... 158
Appendix E.  Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost) ................................................................. 159
Appendix F.  Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost) .................................................. 161
Appendix G.  Restore TVOE Configuration from Backup Media .......................................................... 162
Appendix H.  Restore PMAC from Backup ......................................................................................... 169
Appendix I.  Configure TVOE Hosts ................................................................................................. 178
Appendix J.  Create NOAM/SOAM Virtual Machines ................................................................. 188
Appendix K.  SNMP Configuration .................................................................................................. 196
Appendix L.  Backup Directory ........................................................................................................ 200
Appendix M.  My Oracle Support (MOS) ...................................................................................... 201

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

List of Figures
Figure 1.  Determining Recovery Scenario ..................................................................................... 12

List of Procedures
Procedure 1.  Recovery Scenario 1 ................................................................................................. 14
Procedure 2.  Recovery Scenario 2 ................................................................................................ 48
Procedure 3.  Recovery Scenario 3 ................................................................................................ 74
Procedure 4.  Recovery Scenario 4 ................................................................................................ 97
Procedure 5.  Recovery Scenario 5 ................................................................................................ 116
Procedure 6.  Recovery Scenario 6 (Case 1) ............................................................................... 125
Procedure 7.  Recovery Scenario 6 (Case 2) ............................................................................... 130
Procedure 8.  Keep Restored User ............................................................................................... 135
Procedure 9.  Remove the Restored User ..................................................................................... 137
Procedure 10.  Restore an Archive That Does Not Contain a Current User ......................... 139
Procedure 11.  IDIH Disaster Recovery Preparation .............................................................. 143
Procedure 12.  IDIH Disaster Recovery (Re-Install Mediation and Application Servers) ........ 145
Procedure 13.  DSR Database Backup ....................................................................................... 148
Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F) ........................................... 152
Procedure 15. Recover a Failed Enclosure Switch (Cisco 3020) ............................................................... 154
Procedure 16. Recover a Failed Enclosure Switch (HP 6120XG, HP 6125XLG, HP 6125G) .................... 154
Procedure 17. Recover a Failed Enclosure OA ......................................................................................... 157
Procedure 18. Inhibit A and B Level Replication on C-level Servers .................................................... 157
Procedure 19. Un-Inhibit A and B Level Replication on C-level Servers ............................................. 158
Procedure 20. Inhibit A and B Level Replication on C-level Servers .................................................... 159
Procedure 21. Un-Inhibit A and B Level Replication on C-Level Servers ............................................ 161
Procedure 22. Restore TVOE Configuration from Backup Media .......................................................... 162
Procedure 23. Restore PMAC from Backup Media ................................................................................ 169
Procedure 24. Restore PMAC from Backup Server ............................................................................... 172
Procedure 25. Configure TVOE ............................................................................................................. 178
Procedure 26. Create NOAM Guest VMs .............................................................................................. 188
Procedure 27. Create SOAM Guest VMs ............................................................................................... 192
Procedure 28. Configure SNMP .......................................................................................................... 196
Procedure 29. Backup Directory .......................................................................................................... 200
1. Introduction

This document describes procedures used to execute disaster recovery for DSR. This includes recovery of partial or complete loss of one or more DSR servers. The audience for this document includes GPS groups such as software engineering, product verification, documentation, customer service, software operations, and first office application. This document can be executed by Oracle customers as long as Oracle Customer Service personnel are involved and/or consulted. Executing this procedure also involves referring to and executing procedures in existing support documents.

Note: Components dependent on DSR might need to be recovered as well, for example, SDS, IDIH, and PMAC.

1.1 References

[1] TPD Initial Product Manufacture
[2] Platform 7.2 Configuration Procedure Reference
[7] DSR MAP-Diameter IWF Feature Activation Procedure
[8] DSR C-Class Software Installation and Configuration Procedure Part 2/2
[9] DSR GLA Feature Activation Procedure
[10] DSR C-Class Hardware and Software Installation
[12] SDS C-Class Disaster Recovery Guide
[14] DSR DTLS Feature Activation Procedure
[16] DCA Framework and Application Activation and Deactivation Guide

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>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>HP c-Class</td>
<td>HP blade server offering</td>
</tr>
</tbody>
</table>
### 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>
</tbody>
</table>
## 1.4 Optional Features

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

### Table 3. Optional Features

<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>
<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>

### 2. General Description

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

### Table 4. Recovery Scenarios

<table>
<thead>
<tr>
<th>Procedure</th>
<th>State of NOAM and/or SOAM server(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery of the entire network from a total outage</td>
<td>• All NOAM servers failed.</td>
</tr>
<tr>
<td>Recovery Scenario 1 (Complete Server Outage)</td>
<td>• All SOAM servers failed.</td>
</tr>
<tr>
<td>recovery</td>
<td>• MP servers may or may not have failed.</td>
</tr>
<tr>
<td>Recovery of one or more servers with at least one NOAM server intact</td>
<td>• At least 1 NOAM server is intact and available.</td>
</tr>
<tr>
<td>Recovery Scenario 2 (Partial Server Outage with One NOAM Server Intact and ALL SOAMs Failed)</td>
<td>• All SOAM servers failed.</td>
</tr>
<tr>
<td>recovery</td>
<td>• MP servers may or may not have failed.</td>
</tr>
<tr>
<td>Recovery of the NOAM pair with one or more SOAM servers intact</td>
<td>• All NOAM servers failed.</td>
</tr>
<tr>
<td>Recovery Scenario 3 (Partial Server Outage with All NOAM Servers Failed and One SOAM Server Intact)</td>
<td>• At least 1 SOAM server out of active, standby, spare is intact and available.</td>
</tr>
<tr>
<td>recovery</td>
<td>• MP servers may or may not have failed.</td>
</tr>
</tbody>
</table>
### Procedure

<table>
<thead>
<tr>
<th>Procedure</th>
<th>State of NOAM and/or SOAM server(s)</th>
</tr>
</thead>
</table>
| 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.  
• At least 1 SOAM server out of active, standby, spare is intact and available.  
• 1 or more MP servers have failed. |
| Recovery Scenario 4 (Partial Server Outage with One NOAM Server and One SOAM Server Intact) | |
| 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  
• 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) |
| Recovery of one or more server with corrupt databases that cannot be restored using replication from the active parent node. | |
| 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, OA, or 6120/6125/3020 switches, refer to Recover/Replace Failed 3rd Party Components (Switches, OAs).

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 at least one NOAM server is intact. All SOAM servers have failed and are recovered using base recovery of hardware and software. Database is restored on the SOAM server and replication recovers 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 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. Oracle Tekelec Platform Distribution (TPD) Media (64 bits).
6. Platform Management and Configuration (PMAC) ISO or SW.
7. DSR CD-ROM (or ISO image file on USB Flash) of the target release.
8. TVOE Platform Media (64 bits).
9. The XML configuration files used to configure the switches, available on the PMAC server (or PMAC backup).
10. The switch backup files taken after the switch is configured, available on the PMAC server (or PMAC backup).
11. The network element XML file used for the blades initial configuration.
12. The HP firmware upgrade pack (or customer-provided firmware).
13. NetBackup Files if they exist. This may require the assistance of the customer’s NetBackup administrator.
14. PMAC and TVOE backups (if available).
15. Latest RADIUS shared secret encryption key file backup (DpiKf.bin.encr).
16. List of activated and enabled features.
17. IDIH CD-ROM (or ISO image file on USB Flash) of the target release (if IDIH is being recovered).

**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.

**Note:** NOAMs are deployed using the fast deployment tool from the PMAC. In scenarios where both NOAMs are failed, this fast deployment file is used. In scenarios where only one NOAM is failed, the fast deployment file is NOT used.

**SUDO**
As a non-root user (admusr), many commands (when run as admusr) now require the use of sudo.

### 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.
4. From the failure conditions, determine the Recovery Scenario and procedure to follow (using Figure 1. Determining Recovery Scenario and Table 4. Recovery Scenarios.
5. Execute appropriate recovery procedures (listed in Table 4. Recovery Scenarios).
Figure 1. Determining Recovery Scenario
4. 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.HPC02-NO2.FullDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2
```

4.1 Recovery Scenario 1 (Complete Server Outage)

For a complete server outage, NOAM servers are recovered using recovery procedures of base hardware and software and then executing a database restore to the active NOAM/SOAM servers. All other servers are recovered using recovery procedures of base hardware and software.

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 and blades
  - Recover the base hardware. (By replacing the hardware and executing hardware configuration procedures) — Reference [10] for the DSR base hardware installation procedure
- Recover the NOAM servers by recovering executing the fast deployment xml file
  - Recover the NOAM database
  - Reconfigure the DSR application
- Recover the SOAM servers by recovering base hardware/software and/or VM image
- Recover the SOAM database
- Reconfigure the DSR Application
- Recover all MP servers by recovering base hardware and software
  - Reconfigure the signaling interface and routes on the MPs. The DSR software automatically reconfigures the signaling interface from the recovered database
  - Reference [8] for the applicable DSR software installation/configuration guide if any existing routes need to be altered
- Restart process and re-enable provisioning replication

**Note:** Any other applications DR recovery actions (SDS and IDIH) may occur in parallel. These actions can/should be worked simultaneously; doing so would allow faster recovery of the complete solution, that is, stale DB on DP servers do not receive updates until SDS-SOAM servers are recovered. Section 6.6 for IDIH disaster recovery and [12] for SDS 7.2/7.3 disaster recovery.

**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>

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 settings by executing the **Configure the RMS and Blade Server BIOS Settings** procedure from reference [10].
   2. Verify and/or upgrade server firmware by executing the **Upgrade Management Server Firmware** procedure from reference [10].

**Note:** As indicated in [10], repeat for additional rack mount servers, if equipped.
**Procedure 1. Recovery Scenario 1**

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC, TVOE Hosts, and Switch Recovery: Backups available</th>
<th>PMAC, TVOE Hosts, and Switch Recovery: Backups NOT available</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>This step assumes TVOE and PMAC backups are available, if backups are <strong>NOT</strong> available, <strong>skip this step</strong>.</td>
<td>This step assumes TVOE and PMAC backups are <strong>NOT</strong> available. If the TVOE and PMAC have already been restored, <strong>skip this step</strong>.</td>
</tr>
<tr>
<td></td>
<td>1. Restore the PMAC TVOE host backup by executing Appendix G Restore TVOE Configuration from Backup Media.</td>
<td>1. Execute the <strong>Configure and IPM Management Server</strong> section from reference [10].</td>
</tr>
<tr>
<td></td>
<td>2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup.</td>
<td>2. Execute the <strong>Install PMAC</strong> procedure from reference [10].</td>
</tr>
<tr>
<td></td>
<td>3. Recover failed OAs, aggregation, and enclosure switches by referring to Appendix B Recover/Replace Failed 3rd Party Components (Switches, OAs).</td>
<td>3. Execute the <strong>Configure Aggregation Switches</strong> procedure from reference [10] to recover Cisco 4948 aggregation switches, if needed.</td>
</tr>
<tr>
<td></td>
<td>4. Verify/Update blade server firmware by executing the <strong>Server Blades Installation Preparation</strong> section from reference [10].</td>
<td>4. Execute the <strong>Configure PMAC Application</strong> procedure from reference [10].</td>
</tr>
<tr>
<td></td>
<td>5. Install TVOE on ALL failed TVOE servers as needed by executing the <strong>Install TVOE on Blade Servers</strong> procedure from reference [10].</td>
<td>5. Execute the <strong>HP C-7000 Enclosure Configuration</strong> procedure from reference [10] to recover and configure any failed OAs, if needed.</td>
</tr>
<tr>
<td></td>
<td>6. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on <strong>ALL</strong> failed TVOE host blade servers.</td>
<td>6. Execute the <strong>Enclosure and Blades Setup</strong> procedure from reference [10].</td>
</tr>
<tr>
<td></td>
<td>7. Proceed to step 7.</td>
<td>7. Execute the <strong>Configure Enclosure Switches</strong> procedure from reference [10] to recover enclosure switches, if needed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. Verify/Update Blade server firmware by executing the <strong>Server Blades Installation Preparation</strong> procedure from reference [10].</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. Install and configure TVOE on failed rack mount servers by executing the <strong>Installing TVOE on Rack Mount Server(s)</strong> procedure from reference [10].</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10. Install and configure TVOE on failed TVOE blade servers by executing the <strong>Install TVOE on Blade Servers</strong> procedure from reference [10].</td>
</tr>
</tbody>
</table>
## Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
</table>
| **7.** Execute Fast Deployment File for NOAMs | The backup fdconfig file used during the initial DSR installation is available on the PMAC, if a database backup was restored on the PMAC. If a backup fast deployment xml is NOT available, execute **Configure NOAM Servers** from reference [8]. If a backup fast deployment xml is already present on the PMAC, execute this procedure: 1. Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade has been performed since initial installation). 2. Execute these commands:  

    ```
    $ cd /usr/TKLC/smac/etc
    $ screen
    $ sudo fdconfig config --file=<Created_FD_File>.xml
    ``` |
| **8.** Obtain latest database backup and network configuration data | 1. Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. 2. Obtain most recent **RADIUS shared secret encryption key** file DpiKf.bin.encr from external backup sources. (Only when the RADIUS Key Revocation MOP has been executed on the system).  

    **Note:** Shared secret encryption key file needs to be handled by someone authorized to handle shared secrets information.  

    **Note:** From Required Materials list; use site survey documents and Network Element report (if available) to determine network configuration data. |
| **9.** Execute DSR installation procedure for the first NOAM | 1. Configure the first NOAM server by executing **Configure the First NOAM NE and Server** section from reference [8]. 2. Configure the NOAM server group by executing the **Configure the NOAM Server Group** section from reference [8].  

    **Note:** Use the backup copy of network configuration data and site surveys (Step 2). |
| **10.** NOAM GUI: Login | Log into the NOAM GUI as the guiadmin user: |

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

11. **NOAM GUI:** Upload the backup database file

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

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

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

2. Click **Disable Provisioning**.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM GUI: Verify the archive contents and database compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.</td>
<td>1. Select the active NOAM server and click <strong>Compare</strong>.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Comparison screen" /></td>
</tr>
<tr>
<td></td>
<td>2. Click the button for the restored database file uploaded as a part of step 11 of this procedure.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Database Compare screen" /></td>
</tr>
<tr>
<td></td>
<td>3. <strong>Verify</strong> the output window matches the screen below.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Database Archive Compare screen" /></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Archive Contents and Database Compatibilities must be the following:</td>
</tr>
<tr>
<td></td>
<td><strong>Archive Contents:</strong> Configuration data.</td>
</tr>
<tr>
<td></td>
<td><strong>Database Compatibility:</strong> The databases are compatible.</td>
</tr>
<tr>
<td></td>
<td><strong>Node Type Compatibility:</strong> The node types are compatible.</td>
</tr>
<tr>
<td></td>
<td><strong>Topology Compatibility:</strong> THE TOPOLOGY IS NOT COMPATIBLE. CONTACT ORACLE CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE.</td>
</tr>
<tr>
<td></td>
<td>Discrepancies:</td>
</tr>
<tr>
<td></td>
<td>- Server A1560.012 on network XNI is in the current topology but not the selected backup file.</td>
</tr>
<tr>
<td></td>
<td>- Server A1560.012 on network XNI is in the current topology but not the selected backup file.</td>
</tr>
<tr>
<td></td>
<td>- Server A0630.235 on network XNI is in the selected backup file but not the current topology.</td>
</tr>
<tr>
<td></td>
<td>- Server D2594.011 on network XNI is in the selected backup file but not the current topology.</td>
</tr>
<tr>
<td></td>
<td>- Server C0422.000 on network XNI is in the selected backup file but not the current topology.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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:</td>
</tr>
<tr>
<td></td>
<td><strong>Topology Compatibility</strong></td>
</tr>
<tr>
<td></td>
<td>THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility.</td>
</tr>
<tr>
<td></td>
<td>4. If the verification is successful, click <strong>Back</strong> and continue to next step in this procedure.</td>
</tr>
</tbody>
</table>
Procedure 1. Recovery Scenario 1

14. Active NOAM: Restore the database

1. From Status & Manage > Database.
2. Select the active NOAM server and click Restore.

3. Select the backup provisioning and configuration file.

4. Click OK.

5. If you get errors related to the warnings highlighted in the previous step, then it is expected. If no other errors display, then mark the Force checkbox and click OK to proceed with the DB restore.

Database Restore Confirm

Incompatible archive selected

The selected database came from ZombieNOA

Archive Contents
Configuration data
Database Compatibility
The databases are compatible.

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

Force Restore? [ ] Force

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>Description</th>
</tr>
</thead>
</table>
| 15.  | **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) |
| 16.  | **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).  
  **Note:** Do not pay attention to alarms until all the servers in the system are completely restored.  
  **Note:** 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>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td><strong>Active NOAM</strong>: Set failed servers to OOS</td>
</tr>
<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>Set the Max Allowed HA Role option to <strong>OOS</strong> for the failed servers.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.</td>
<td><strong>Active NOAM</strong>: Login</td>
</tr>
<tr>
<td></td>
<td>Log into the recovered active NOAM using SSH terminal as <strong>admusr</strong> user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.</td>
<td><strong>NOAM VIP GUI</strong>: Recover standby NOAM</td>
</tr>
<tr>
<td>1.</td>
<td>Install the second NOAM server by executing the <strong>Configure the Second NOAM Server</strong> procedure, steps 3-5 and 7, from reference [8].</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Execute step 6 if NetBackup is used.</td>
</tr>
<tr>
<td>2.</td>
<td>If NetBackup is used, execute the <strong>Install NetBackup Client</strong> procedure from reference [8].</td>
</tr>
</tbody>
</table>
Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.</td>
<td><strong>NOAM VIP GUI:</strong> Set HA on standby NOAM</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 standby NOAM 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>
<tr>
<td>21.</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><img src="image" alt="Status &amp; Manage" /></td>
</tr>
<tr>
<td></td>
<td>2. Select the recovered standby NOAM server and click <strong>Restart.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Restart button" /></td>
</tr>
</tbody>
</table>
### Procedure 1. Recovery Scenario 1

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **22. NOAM VIP GUI:** Perform key exchange with export server | **1.** Navigate to Administration > Remote Servers > Data Export.  
   - Administration  
     - General Options  
     - Access Control  
     - Software Management  
     - Remote Servers  
       - LDAP Authentication  
       - SNMP Trapping  
       - Data Export  
       - DNS Configuration  
   
   **2.** Click **SSH Key Exchange** at the bottom of the screen.  
   ![SSH Key Exchange](image)  
   **3.** Type the **Password** and click **OK**.  
   ![Password](image) |
| **23. NOAM VIP GUI:** Stop replication to the C-level servers of this site | **!!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. |
| **24. Configure SOAM TVOE server blades** | If the TVOE restore has already been executed (step 5), skip this step.  
   If a TVOE backup of the SOAM server blades is not available, execute **Configure SOAM TVOE Server Blades** from reference [8]. |
| **25. Create and IPM SOAM VMs** |  
   **1.** Execute **Create SOAM Guest VMs** for the failed SOAM VMs and MP blades from reference [8].  
   **2.** Execute **IPM Blades and VMs** for the failed SOAM VMs and MP blades from reference [8].  
   **3.** Execute **Install the Application** for the failed SOAM VMs and MP blades from reference [8]. |
## Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26.</td>
<td>Recover active SOAM server</td>
</tr>
</tbody>
</table>
| 1. | Execute **Configure the SOAM Servers**, steps 1-3 and 5-8, from reference [8].  
   *Note:* If you are using NetBackup, also execute step 10.  
   2. If you are using NetBackup, execute **Install NetBackup Client** from reference [8]. |
| 27. | NOAM VIP GUI: Set HA on the SOAM server |
| 1. | Navigate to **Status & Manage > HA**.  
   1. **Status & Manage**  
      - Network Elements  
      - Server  
      - HA  
      - Database  
      - KPIs  
      - Processes  
      - Tasks  
      - Files  
   2. Click **Edit**.  
   3. Select the SOAM server and set it to **Active**.  
   4. Click **OK**. |
| 28. | NOAM VIP GUI: Restart DSR application |
| 1. | Navigate to **Status & Manage > Server**.  
   1. **Status & Manage**  
      - Network Elements  
      - Server  
      - HA  
      - Database  
      - KPIs  
      - Processes  
      - Tasks  
      - Files  
   2. Select the recovered SOAM server and click **Restart**. |
Procedure 1. Recovery Scenario 1

29. **NOAM VIP GUI:** Upload the backed up SOAM database file

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

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

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

   ![Upload Page](image)

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

   ![Upload Page](image)

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>Step</th>
<th>Action</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><code>http://&lt;Recovered_SOAM_IP_Address&gt;</code></td>
</tr>
<tr>
<td>3.</td>
<td>Login as the <code>guiadmin</code> 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 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>31.</td>
<td><strong>SOAM GUI</strong>: Verify the archive contents and database compatibility</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Status &amp; Manage &gt; Database</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the <strong>Active SOAM</strong> server and click <strong>Compare</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Click the button for the restored database file uploaded as a part of step 29. of this procedure.</td>
</tr>
<tr>
<td>4.</td>
<td>Verify the output window matches the screen below.</td>
</tr>
</tbody>
</table>

**Database Compare**

```
Select archive to compare on server:?
Archive: backup@backup.DSR.com
```

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 32.  | **Recovered SOAM GUI:**  

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.dst2
   
   Ok Cancel
   ```

3. Click **OK**.

   *Database Restore Confirm*

   ```
   Compatible archive.
   ```

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.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 33.  | **Recovered SOAM GUI:**  

Monitor and confirm database restoral  

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

**Note:** Do not pay attention to alarms until all the servers in the system are completely restored.

**Note:** The Configuration and Maintenance information 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: Login</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>34.</td>
<td>Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[http://&lt;Primary_NOAM_VIP_IP_Address&gt;]</td>
<td></td>
</tr>
<tr>
<td>35.</td>
<td>Login as the <code>guiadmin</code> user:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Recover the remaining SOAM servers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>35.</td>
<td>Recover the remaining SOAM servers (standby, spare) by repeating these steps for each SOAM server:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Execute <strong>Configure the SOAM Servers</strong>, steps 1-3 and 5-8, from reference [8].</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you are using NetBackup, also execute step 10.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. If you are using NetBackup, execute <strong>Install NetBackup Client</strong> from reference [8].</td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 1.  Recovery Scenario 1

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>36.</strong></td>
<td><strong>NOAM VIP GUI:</strong></td>
<td><strong>Set HA on the remaining SOAMs</strong></td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; HA.</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Status &amp; Manage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Network Elements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- HA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Database</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- KPIs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Processes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Tasks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Files</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Edit</strong> at the bottom of the screen.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Select the recovered 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>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>37.</strong></td>
<td><strong>NOAM VIP GUI:</strong></td>
<td><strong>Restart DSR application</strong></td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Server.</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Status &amp; Manage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Network Elements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- HA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Database</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- KPIs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Processes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Select the recovered standby SOAM server and click <strong>Restart.</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Recovery Scenario 1

#### Procedure 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 38. NOAM VIP GUI: Start replication on the recovered standby SOAM | Un-Inhibit (start) replication to the recovered **standby SOAM**.  
1. Navigate to **Status & Manage > Database**.  
2. Click **Allow Replication** on the recovered standby SOAM server.  
3. Verify the replication on all servers is allowed. This can be done by checking **Repl status** column of respective server. |
| 39. SOAM VIP GUI: Verify the local node info | 1. Navigate to **Diameter > Configuration > Local Node**.  
2. Verify all the local nodes are shown. |
| 40. SOAM VIP GUI: Verify the peer node info | 1. Navigate to **Diameter > Configuration > Peer Node**.  
2. Verify all the peer nodes are shown. |
### Procedure 1. Recovery Scenario 1

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **41.** | **SOAM VIP GUI:** Verify the connections info | 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. |
|   |   |   |
| **42.** | **SOAM VIP GUI:** Enable connections, if needed | 1. Navigate to **Diameter > Maintenance > Connections.**  
- **Maintenance**  
  - **Route Lists**  
  - **Route Groups**  
  - **Peer Nodes**  
  - **Connections**  
  2. Select each connection and click **Enable.** Alternatively, you can enable all the connections by clicking **EnableAll.**  
  - **EnableAll**  
  - **Disable**  
  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 |
|   | **Active NOAM:** Activate optional features | Establish an SSH session to the active NOAM, login as **admusr.**  
**Note for PCA Activation:**  
If you have PCA installed in the system being recovered, re-activate PCA by executing **PCA Activation on Entire Server on Recovered NOAM Server** from [13].  
**Note:** If not all SOAM sites are recovered at this point, then you should repeat activation for each *new* SOAM site that comes online.  
**Note:** If any of the MPs are failed and recovered, then restart these MP servers after activation of the feature.  
Refer to 1.4 Optional Features to activate any features previously activated. |
Procedure 1.  Recovery Scenario 1

44. **NOAM VIP GUI:** Start replication on working C-level servers

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

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

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

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

   ![Status & Manage]
   - Network Elements
   - Server
   - HA
   - Database
   - KPIs
   - Processes

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)
   - 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)

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>
</tbody>
</table>
## Procedure 1. Recovery Scenario 1

### 45. SOAM VIP GUI:
Perform key exchange with export server

1. Navigate to Administration > Remote Servers > Data Export.
   - Remote Servers
     - LDAP Authentication
     - SNMP Trapping
     - Data Export
     - DNS Configuration
   2. Click **SSH Key Exchange**.
   3. Type the **Password** and click **OK**.

### 46. NOAM VIP GUI:
Recover the C-level server (DA-MP, SBRs, IPFE, SS7-MP)

1. Execute **Configure MP Blade Servers**, steps 1, 7, 11-14, and 17, from reference [8].
   
   **Note:** Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.

2. Repeat this step for any remaining failed MP servers.

### 47. 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 **Standby**, set it to **Active**.
   4. Click **OK**.
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Restart DSR application on the recovered C-level servers</th>
</tr>
</thead>
</table>
| 1. | Navigate to **Status & Manage > Server**. | ![Diagram](image1.png)  
   | Select the recovered C-level servers and click **Restart**. | ![Diagram](image2.png) |
### Procedure 1. Recovery Scenario 1

#### 49. NOAM VIP GUI: Start replication on all C-level servers

- **Un-inhibit (start) replication to the ALL C-level servers.**
  1. Navigate to Status & Manage > Database.

    ![Status & Manage menu]

    Image description: The Status & Manage menu is expanded to show several sub-menus including Network Elements, Server, HA, Database, KPIs, and Processes.

    ![Database sub-menu]

    Image description: The Database sub-menu is expanded to show several options.

    ![Allow Replication button]

    Image description: There is a button labeled “Allow Replication”.

  2. If the Repl Status is set to Inhibited, click **Allow Replication** using this order:
     - Active NOAM Server
     - Standby NOAM Server
     - Active SOAM Server
     - Standby SOAM Server
     - Spare SOAM Server *(if applicable)*
     - 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)

  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>

#### 50. Active NOAM: Perform key exchange between the active-NOAM and recovered servers

1. Establish an SSH session to the active NOAM, login as **admusr**.
2. Perform a key exchange from the active NOAM to each recovered server:

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

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

<table>
<thead>
<tr>
<th>51.</th>
<th><strong>NOAM VIP GUI:</strong> Fetch and store the database report for the newly restored data and save it</th>
</tr>
</thead>
</table>

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

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

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

- The following screen displays:

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

- **dsr Database Status Report**
- **Report Generated:** Tue Oct 11 13:24:26 2016 EDT
- **From:** Active Network OAM&P on host ZombieNOAM1
- **Report Version:** 8.0.0.0.0-80.9.0
- **User:** guiadmin

### General

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

### Capacities and Utilization

- **Disk Utilization:** 8.4%: 580M used of 7.0G total, 6.0G available
- **Memory Utilization:** 0.0%: used of total, 0X available

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

<table>
<thead>
<tr>
<th>Active NOAM: Verify replication between servers</th>
<th>1. Log into the active NOAM using SSH terminal as <strong>admusr</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Execute this command:</td>
</tr>
<tr>
<td></td>
<td>$ sudo irepstat -m</td>
</tr>
</tbody>
</table>

**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 & Manage > Database.

   - NOAM VIP GUI: Verify the database states

   Navigate to Status & Manage > 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 the 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>ZombieSOAM1</td>
<td>System OAM</td>
<td>N/A</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>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>ZombieSOAM2</td>
<td>MP</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM1</td>
<td>MP</td>
<td>Active</td>
</tr>
</tbody>
</table>
Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>54.</td>
<td><strong>NOAM VIP GUI:</strong> Upload the backed up RADIUS key file (RADIUS only)</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Status &amp; Manage &gt; Files</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>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>3.</td>
<td>Click <strong>Browse</strong>.</td>
</tr>
<tr>
<td>4.</td>
<td>Locate the <strong>DpiKf.bin.encr</strong> file.</td>
</tr>
<tr>
<td>5.</td>
<td>Click <strong>Upload</strong>.</td>
</tr>
</tbody>
</table>

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

- 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>55.</th>
<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 using SSH terminal as **admusr** user.

2. Copy the key file:

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

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

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

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

56. **NOAM VIP**: Copy and distribute the RADIUS key file on active NOAM (RADIUS only) — Part 2

Distribute key file to all the servers in the topology:

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

Example output:

```
1450723210: [INFO] Key file on Active NOAM and IPFE are same.
1450723210: [INFO] NO NEED to sync key file to IPFE.
FIPS integrity verification test failed.
1450723210: [INFO] Key file on Active NOAM and MP-2 are same.
1450723210: [INFO] NO NEED to sync key file to MP-2.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723211: [INFO] Key file on Active NOAM and MP-1 are same.
1450723211: [INFO] NO NEED to sync key file to MP-1.
[admusr@NOAM-2 bin]$ ./sharedKrevo -updateData
1450723226: [INFO] Updating data on server 'NOAM-2'
1450723227: [INFO] Data updated to 'NOAM-2'.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723228: [INFO] Updating data on server 'SOAM-2'
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450723230: [INFO] 1 rows updated on 'SOAM-2'...
1450723230: [INFO] Data updated to 'SOAM-2'
[admusr@NOAM-2 bin]$ 
```

**Note**: For any errors refer My Oracle Support (MOS).

57. **NOAM VIP GUI**: Verify the HA status

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

   ![Status and Manage](image)

   - Status
   - 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>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></th>
<th>NOAM GUI: Enable provisioning</th>
</tr>
</thead>
</table>
| 58. | Navigate to Status & Manage > Database.  
   | - Click Enable Provisioning.  
   | - Click OK. |

<table>
<thead>
<tr>
<th></th>
<th>SOAM GUI: Enable site provisioning</th>
</tr>
</thead>
</table>
| 59. | Navigate to Status & Manage > Database.  
   | - Click Enable Site Provisioning.  
   | - Click OK. |

<table>
<thead>
<tr>
<th></th>
<th>MP Servers: Disable SCTP Auth Flag</th>
</tr>
</thead>
</table>
| 60. | For SCTP connections without DTLS enabled, refer to the Disable/Enable DTLS Feature Activation Guide [14].  
   | Execute this procedure on all failed MP servers. |
## Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>SOAM VIP GUI: Enable connections, if needed</th>
<th>SOAM VIP GUI: Enable optional features</th>
<th>SOAM VIP GUI: Re-enable transports, if needed</th>
</tr>
</thead>
</table>
| 61.  | Navigate to **Diameter > Maintenance > Connections.**  
   1. Enable connections by clicking **Enable**. Alternatively, enable all the connections by clicking **EnableAll**.  
   2. 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. |
| 62.  | Navigate to **Diameter > Maintenance > Applications.**  
   1. Select the optional feature application configured in step 43.  
   2. Click **Enable**. |
| 63.  | Navigate to **Transport Manager > Maintenance > Transport.**  
   1. Select each transport and click **Enable**.  
   2. Verify the Operational Status for each transport is **Up**. |
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th></th>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
</table>
| 64. | **SOAM VIP GUI:** Re-enable MAPIWF application, if needed | 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.  
   3. Verify the SSN Status is **Enabled**. |
| 65. | **SOAM VIP GUI:** Re-enable links, if needed | 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.  
   3. Verify the Operational Status for each link is **Up**. |
| 66. | **SOAM VIP GUI:** Examine all alarms | 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). |
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>67.</td>
<td><strong>NOAM VIP GUI:</strong> Examine all alarms</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to Alarms &amp; Events &gt; View Active.</td>
</tr>
<tr>
<td></td>
<td>- Alarms &amp; Events</td>
</tr>
<tr>
<td></td>
<td>- View Active</td>
</tr>
<tr>
<td></td>
<td>- View History</td>
</tr>
<tr>
<td></td>
<td>- 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>68.</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>69.</td>
<td>Backup 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>70.</td>
<td>Recover IDIH</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>71.</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.</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 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; detailed steps are in Procedure 2. The major activities are summarized as follows:

- Recover *standby NOAM* server (if needed) by recovering base hardware, software, and the database
  - 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** 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 servers

### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Workarounds</th>
<th>Gather required materials</th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
</table>
| 1.     | Refer to Appendix 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. | 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

Log In

Enter your username and password to log in

Username: |
Password: |

[Change password]  
[Log In]
## Procedure 2. Recovery Scenario 2

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td><strong>Active NOAM:</strong> Set failed servers to OOS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Status &amp; Manage &gt; HA.</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Edit.</strong></td>
<td></td>
</tr>
</tbody>
</table>

### 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>ZombieDRNNOAM1</td>
<td>Active StandBy</td>
<td>The maximum des</td>
</tr>
</tbody>
</table>

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

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Replace failed equipment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HW vendor to replace the failed equipment.</td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td><strong>RMS NOAM Failure:</strong> Configure BIOS settings and update firmware</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the failed server is <strong>NOT</strong> a rack mount server, <strong>skip to step 10.</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Configure and verify the BIOS settings by executing procedure <strong>Configure the RMS and Blade Server BIOS Settings</strong> from reference [10].</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Verify and/or upgrade server firmware by executing procedure <strong>Upgrade Management Server Firmware</strong> from reference [10].</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.</td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td><strong>RMS NOAM Failure:</strong> Backups available</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the failed server is <strong>NOT</strong> a rack mount server, <strong>skip to step 10.</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This step assumes that TVOE and PMAC backups are available, if backups are <strong>NOT</strong> available, <strong>skip this step.</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing Restore PMAC from Backup.</td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>RMS NOAM Failure: Backups NOT available</th>
<th>HP-Class Blade Failure: Configure blade server iLO, update firmware/BIOS settings</th>
<th>HP-Class Blade Failure: Backups available</th>
<th>HP-Class Blade Failure: Backups NOT available</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>If the failed server is NOT a rack mount server, <strong>skip to step 10</strong>. This step assumes that TVOE and PMAC backups <strong>NOT</strong> are available, if the TVOE and PMAC have already been restored, <strong>skip this step</strong>. If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. <strong>Configure and IPM Management Server</strong> from reference [10]. 2. <strong>Install PMAC</strong> from reference [10]. 3. <strong>Configure PMAC Application</strong> from reference [10]. If the PMAC is <strong>NOT</strong> located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. <strong>Installing TVOE on Rack Mount Server(s)</strong> from reference [10].</td>
<td>If the failed server is <strong>NOT</strong> an HP C-Class Blade, <strong>skip to step 14</strong>. 1. Execute <strong>Configure Blade Server iLO Password for Administrator Account</strong> from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing <strong>Server Blades Installation Preparation</strong> from reference [10]</td>
<td>If the failed server is <strong>NOT</strong> an OAM type HP C-Class Blade, <strong>skip to step 14</strong>. This step assumes TVOE backups are available. If backups are <strong>NOT</strong> available, <strong>skip this step</strong>. 1. Install and configure TVOE on failed TVOE blade servers by executing <strong>Install TVOE on Blade Servers</strong> from reference [10]. 2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers.</td>
<td>If the failed server is <strong>NOT</strong> an OAM type HP C-Class Blade, <strong>skip to step 14</strong>. This step assumes TVOE backups are <strong>NOT</strong> available: 1. Install and configure TVOE on failed TVOE blade servers by executing <strong>Install TVOE on Blade Servers</strong> from reference [10]. 2. Configure the NOAM and/or SOAM failed TVOE server blades by executing <strong>Configure SOAM TVOE Server Blades</strong> from reference [8]. <strong>Note:</strong> Although the title of the procedure is related to SOAMs only, execute this procedure for any failed NOAMs located on TVOE server blades.</td>
</tr>
<tr>
<td>9.</td>
<td>Recover failed OAs, aggregation and enclosure switches, if needed. Backups Available: 1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) section to recover failed OAs, aggregation, and enclosure switches Backups NOT Available: 1. Execute <strong>HP C-7000 Enclosure Configuration</strong> from reference [10] to recover and configure any failed OAs, if needed. 2. Execute <strong>Configure Enclosure Switches</strong> from reference [10] to recover enclosure switches, if needed.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Procedure 2. Recovery Scenario 2

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>13.</td>
<td>Create VMs</td>
<td>Execute Create NOAM/SOAM Virtual Machines to create the NOAM and SOAM VMs on failed TVOE servers.</td>
</tr>
</tbody>
</table>
| 14. | IPM and install DSR application on failed guest/servers | 1. Execute **IPM Blades and VMs** for the failed SOAM VMs and MP blades from reference [8].  
2. Execute **Install the Application Software** for the failed SOAM VMs and MP blades from reference [8]. |
| 15. | Install NetBackup client (Optional) | If NetBackup is used, execute **Install NetBackup Client** from reference [8]. |
| 16. | 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: |

![Oracle System Login](https://example.com/oracle-login.png)
### Recovery Scenario 2

#### Procedure 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Description</th>
</tr>
</thead>
</table>
| 17. | NOAM VIP GUI: Export the initial configuration | If the failed server is NOT a NOAM server, skip to step 24.  
1. Navigate to **Configuration > Servers**.  
2. From the GUI screen, select the failed NOAM server and click **Export** to generate the initial configuration data for that server. |
| 18. | NOAM VIP GUI: Copy configuration file to failed NOAM server | 1. Obtain a terminal session to the NOAM VIP, login as the **admusr** user.  
2. Configure the failed NOAM server:  
   ```bash  
   $ sudo scp -r /var/TKLC/db/filemgmt/TKLCCfgData.<Failed_NOAM_Hostname>.sh admusr@<Failed_NOAM_control_IP_address>:/var/tmp/TKLCCfgData.sh  
   ``` |
| 19. | Failed NOAM Server: Verify the configuration was called and reboot the server | 1. Establish an SSH session to the failed NOAM server, login as the **admusr** user.  
   The automatic configuration daemon looks for the file named **TKLCCfgData.sh** in the /var/tmp directory, implements the configuration in the file, and asks the user to reboot the server.  
   2. Verify awpushcfg was called by checking the following file.  
   ```bash  
   $ sudo cat /var/TKLC/appw/logs/Process/install.log  
   ```  
   Verify this message displays:  
   `[SUCCESS] script completed successfully!`  
   3. Reboot the server:  
   ```bash  
   $ sudo init 6  
   ```  
   4. Wait for the server to reboot. |
### Procedure 2. Recovery Scenario 2

#### 20. Failed NOAM Server:

- **Configure networking for dedicated NetBackup interface (Optional)**

**Note:** Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.

Obtain a terminal window to the failed NOAM server, logging in as the `admusr`.

```
$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup
    --type=Ethernet --onboot=yes
    --address=<NO2_NetBackup_IP_Adress>
    --netmask=<NO2_NetBackup_NetMask>
```

```
$ sudo /usr/TKLC/plat/bin/netAdm add
    --route=net
    --device=netbackup
    --address=<NO1_NetBackup_Network_ID>
    --netmask=<NO2_NetBackup_NetMask>
    --gateway=<NO2_NetBackup_Gateway_IP_Address>
```

#### 21. Failed NOAM Server:

- **Verify server health**

Execute this command on the 2nd NOAM server and make sure no errors are returned:

```
$ sudo syscheck
Running modules in class hardware...OK
Running modules in class disk...OK
Running modules in class net...OK
Running modules in class system...OK
Running modules in class proc...OK
LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td><strong>NOAM VIP GUI:</strong> Set HA on standby NOAM</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; HA</strong>.</td>
</tr>
<tr>
<td></td>
<td>- [Diagram of HA page]</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Edit</strong> at the bottom of the screen.</td>
</tr>
<tr>
<td></td>
<td>3. Select the standby NOAM server and set it to <strong>Active</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>23.</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>- [Diagram of Server page]</td>
</tr>
<tr>
<td></td>
<td>2. Select the recovered standby NOAM server and click <strong>Restart</strong>.</td>
</tr>
</tbody>
</table>
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.</td>
<td><strong>NOAM VIP GUI:</strong> Stop replication to the C-level servers of this site &lt;br&gt; <strong>!!Warning!!</strong> &lt;br&gt; Before continuing this procedure, replication to C-level servers at the SOAM site being recovered MUST be inhibited. &lt;br&gt; Failure to inhibit replication to the working C-level servers results in the database being destroyed! &lt;br&gt; <strong>If the spare SOAM is also present in the site and lost</strong>, execute 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. &lt;br&gt; <strong>If the spare SOAM is NOT deployed in the site</strong>, execute Inhibit A and B Level Replication on C-Level Servers to inhibit replication to working C-level servers before continuing.</td>
</tr>
<tr>
<td>25.</td>
<td>Recover active SOAM server &lt;br&gt; 1. Execute <strong>Configure the SOAM Servers</strong>, steps 1-3 and 5-8, from reference [8]. &lt;br&gt; <strong>Note:</strong> If you are using NetBackup, also execute step 10. &lt;br&gt; 2. If you are using NetBackup, execute <strong>Install NetBackup Client</strong> from reference [8].</td>
</tr>
<tr>
<td>26.</td>
<td><strong>NOAM VIP GUI:</strong> Set HA on SOAM server &lt;br&gt; 1. Navigate to <strong>Status &amp; Manage &gt; HA</strong>. &lt;br&gt; 2. Click <strong>Edit</strong> at the bottom of the screen. &lt;br&gt; 3. Select the SOAM server and set it to <strong>Active</strong>. &lt;br&gt; 4. Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>27. NOAM VIP GUI:</th>
<th>28. NOAM VIP GUI:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restart DSR</td>
<td>Upload the</td>
</tr>
<tr>
<td>application</td>
<td>backed up</td>
</tr>
<tr>
<td></td>
<td>SOAM database</td>
</tr>
<tr>
<td></td>
<td>file</td>
</tr>
</tbody>
</table>

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

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

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

2. Select the recovered SOAM server and click **Restart**.

### 28. NOAM VIP GUI: Upload the backed up SOAM database file

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

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

3. Click **Browse** and locate the backup file.
4. Check **This is a backup file** checkbox.
5. 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 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>29.</th>
<th>Recovered SOAM GUI: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td></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>![Recovered_SOAM_IP_Address]</td>
</tr>
<tr>
<td></td>
<td>3. Login as the <strong>guiadmin</strong> user:</td>
</tr>
</tbody>
</table>

---

**Oracle System Login**

![Oracle Login Page]

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 3.0, 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

<table>
<thead>
<tr>
<th>30.</th>
<th>Recovered SOAM GUI: Verify the archive contents and database compatibility</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 28 of this procedure.</td>
</tr>
</tbody>
</table>

**Database Compare**

*Select archive to compare on server 2*

Archive: backupBackup.DSR.Zom

*Ok Cancel*

4. **Verify** the output window matches the screen below.

**Database Archive Compare**

The selected database came from ZombieSOAM1 on 1

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

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

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

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

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

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

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

### 31. Recovered SOAM GUI: Restore the database

1. Select the active SOAM server and click **Restore**.
2. Select the backup provisioning and configuration file.

   ![Database Restore](image)

   - **Database Restore**: Select archive to Restore on server: Zombie SOAM2
     - Select archive: backupBackup of Zombie SOAM2 Configs
     - Archive: backupBackup of Zombie SOAM2 Configs

3. Click **OK**.

4. If you get an error for Node Type Compatibility, that is expected. If no other errors display, mark the **Force** checkbox and click **OK** to proceed with the DB restore.

   ![Database Restore Confirm](image)

   - **Database Restore Confirm**: Compatible archive.
     - The selected database came from Zombie SOAM2
     - Archive Contents: Configuration data
     - Database Compatibility: The databases are compatible.

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

### 32. Recovered SOAM GUI: Monitor and Confirm database restoral

Wait for **5-10 minutes** for the system to stabilize with the new topology:

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

**Note**: Do not pay attention to alarms until all the servers in the system are completely restored.

**Note**: The Configuration and Maintenance information is in the same state it was when backed up during initial backup.
## Procedure 2. Recovery Scenario 2

### 33. **NOAM VIP GUI:** Recover the remaining SOAM servers

- Recover the remaining SOAM servers *(standby, spare)* by repeating these steps for each SOAM server:
  1. Execute **Configure the SOAM Servers**, steps 1-3 and 5-8, from reference [8].

  *Note:* If you are using NetBackup, also execute step 10.

  2. If you are using NetBackup, execute **Install NetBackup Client** from reference [8].

### 34. **NOAM VIP GUI:** Start replication on the recovered SOAMs

- Un-Inhibit (start) replication to the recovered SOAM servers
  1. Navigate to **Status & Manage > Database**.

    - Click **Allow Replication** on the recovered SOAM servers.

    - Verify the replication on all SOAMs servers is allowed. This can be done by checking **Repl status** column of respective server.

### 35. **NOAM VIP GUI:** Set HA on the recovered standby SOAM server

- Set HA on the recovered standby SOAM server
  1. Navigate to **Status & Manage > HA**.

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

    - Select the recovered standby SOAM server and set it to **Active**.

    - Click **OK**.
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| **36.** NOAM VIP GUI: Restart DSR application | 1. Navigate to **Status & Manage > Server**.  
   - **Status & Manage**  
     - **Network Elements**  
     - **Server**  
     - **HA**  
     - **Database**  
     - **KPIs**  
     - **Processes**  
   2. Select the recovered standby SOAM server and click **Restart**. |
| **37.** SOAM GUI: Enable provisioning | 1. Navigate to **Status & Manage > Database**.  
   - **Status & Manage**  
     - **Network Elements**  
     - **Server**  
     - **HA**  
     - **Database**  
     - **KPIs**  
     - **Processes**  
     - **Tasks**  
     - **Files**  
   2. Click **Enable Site Provisioning**.  
   3. A confirmation window displays. Click **OK** to enable provisioning. |
| **38.** SOAM VIP GUI: Verify local node information | 1. Navigate to **Diameter > Configuration > Local Node**.  
   - **Diameter**  
     - **Configuration**  
       - **Capacity Summary**  
       - **Connection Capacity Dashb**  
       - **Application Ids**  
       - **CEX Parameters**  
       - **Command Codes**  
       - **Configuration Sets**  
       - **Local Nodes**  
   2. Verify all the local nodes are shown. |
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>39.</td>
<td><strong>SOAM VIP GUI:</strong> Verify the peer node information.</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>40.</td>
<td><strong>SOAM VIP GUI:</strong> Verify the connections information.</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>
</tbody>
</table>
Procedure 2. Recovery Scenario 2

41. **NOAM VIP GUI:** Start replication on working C-level servers

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

**If the spare SOAM is also present in the site and lost,** execute 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 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)
   - 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)

3. Verify the replication on all the working 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>
### Procedure 2. Recovery Scenario 2

|   | **NOAM VIP GUI:** | **Execute the Configure MP Blade Servers procedure, steps 1, 7, 11-14, and 17, from reference [8].**  
| Note: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.  
| Repeat this step for any remaining failed MP servers. |
|---|---|---|
| **42.** | **Recover the C-level servers (DA-MP, SBRs, IPFE, SS7-MP)** |  
| | **Execute the Configure MP Blade Servers procedure, steps 1, 7, 11-14, and 17, from reference [8].**  
| Note: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.  
| Repeat this step for any remaining failed MP servers. |
| | **Procedure 2. Recovery Scenario 2** |
| **43.** | **Set HA on all C-level servers** |
| 1. | Navigate to **Status & Manage > HA.**  
| 2. | Click **Edit** at the bottom of the screen.  
| 3. | For each recovered C-level with a Max Allowed HA Role set to **Standby**, set it to **Active.**  
| 4. | Click **OK.** |
| **44.** | **Restart DSR application on the recovered C-level servers** |
| 1. | Navigate to **Status & Manage > Server.**  
| 2. | Select the recovered C-level servers and click **Restart.**
Procedure 2. Recovery Scenario 2

45. **NOAM VIP GUI:** Start replication on ALL C-level servers

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

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

   ![Status & Manage](image)

   - 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)
      - 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).

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>

46. **Active NOAM:** Perform keyexchange between the active-NOAM and recovered servers

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

2. Execute this command to perform a keyexchange from the active NOAM to each recovered server:

   ```
   $ keyexchange admusr@<Recovered Server Hostname>
   ```
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 47.  | **Active NOAM:** Activate optional features | Establish an SSH session to the active NOAM and login as `admu`.  
**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 Standby NOAM server** procedure on the recovered standby NOAM server, and the **PCA Activation on Active SOAM Server** procedure on the recovered active SOAM server from [13].  
Refer to 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}
```
**Note:** If any of the MPs are failed and recovered, then restart these MP servers after activation of the feature. |
| 48.  | **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**.  
3. Click **Save** and save the report to your local machine. |
Procedure 2. Recovery Scenario 2

49. Active NOAM: Verify replication between servers

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

2. Execute this command:

   $ sudo irepstat -m

   Example output:

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

   irepstat ( 40 lines) (h)elp (m)erged
Procedure 2. Recovery Scenario 2

50. **NOAM VIP GUI:** Verify the database states

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

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

<table>
<thead>
<tr>
<th>Network Element</th>
<th>Server</th>
<th>Role</th>
<th>OAM Max HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieDRNOAM</td>
<td>ZombieDRNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM2</td>
<td>Network OAM&amp;P</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM2</td>
<td>System OAM</td>
<td>N/A</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM1</td>
<td>System OAM</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM</td>
<td>ZombieDRNOAM2</td>
<td>Network OAM&amp;P</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieMPF2</td>
<td>MP</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSSLMPF2</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSSLMPF1</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>

51. **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>ZombieDRNOAM1</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>ZombieSOAM1</td>
<td>Active</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>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>52.</td>
<td><strong>MP Servers</strong>: Disable SCTP auth flag</td>
<td>For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [14]. Execute this procedure on all failed MP servers.</td>
</tr>
</tbody>
</table>
| 53. | **SOAM VIP GUI**: Enable connections, if needed | 1. Navigate to Diameter > Maintenance > Connections.  
   - Select each connection and click **Enable**. Alternatively, you can enable all the connections by clicking **EnableAll**.  
   - Verify the Operational State is **Available**.  
   - **Note**: If disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution.  
| 54. | **SOAM VIP GUI**: Enable optional features | 1. Navigate to Diameter > Maintenance > Applications.  
   - Select the optional feature application configured in step 47.  
   - Click **Enable**.  
| 55. | **SOAM VIP GUI**: Re-enable transports, if needed | 1. Navigate to Transport Manager > Maintenance > Transport.  
   - Select each transport and click **Enable**.  
   - Verify the Operational Status for each transport is **Up**. |
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>56.</td>
<td><strong>SOAM VIP GUI:</strong> Re-enable MAPIWF application, if needed</td>
</tr>
</tbody>
</table>
|     | 1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users.**<br>   - **Local SCCP Users**<br>     - **Remote Signaling Points**<br>     - **Remote MTP3 Users**<br>     - **Linksets**<br>     - **Links**<br> 2. Click the **Enable** button corresponding to MAPIWF Application Name.<br>   ![Enable and Disable buttons](image)
|     | 3. Verify the SSN Status is **Enabled.** |
| 57. | **SOAM VIP GUI:** Re-enable links, if needed |
|     | 1. Navigate to **SS7/Sigtran > Maintenance > Links.**<br>   - **Local SCCP Users**<br>     - **Remote Signaling Points**<br>     - **Remote MTP3 Users**<br>     - **Linksets**<br>     - **Links**<br> 2. Click **Enable** for each link.<br>   ![Enable and Disable buttons](image)
|     | 3. Verify the Operational Status for each link is **Up.** |
| 58. | **SOAM VIP GUI:** Examine All alarms |
|     | 1. Navigate to **Alarms & Events > View Active.**<br>   - **View Active**<br>   ![View Active, View History, View Trap Log](image)<br> 2. Examine all active alarms and refer to the on-line help on how to address them.  
If needed, contact My Oracle Support (MOS).
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>59.</td>
<td><strong>NOAM VIP GUI:</strong> Examine all alarms</td>
</tr>
<tr>
<td></td>
<td>1. Log into the NOAM VIP if not already logged in.</td>
</tr>
<tr>
<td></td>
<td>2. Navigate to <strong>Alarms &amp; Events &gt; View Active.</strong></td>
</tr>
</tbody>
</table>
|      |   - **Alarms & Events**
|      |     - **View Active**
|      |     - **View History**
|      |     - **View Trap Log** |
|      | 3. Examine all active alarms and refer to the on-line help on how to address them. |
| 60.  | **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. Login as **admusr.** |
|      | 2. Check if all the servers in the Topology are accessible: |
|      | ```
|      | $ cd /usr/TKLC/dpi/bin/
|      | $ ./sharedKrevo -checkAccess
|      | ```
|      | Example output: |
|      | ![Example output](image)
| 61.  | **NOAM VIP:** Copy key file to all the servers in topology (RADIUS only) |
|      | If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator. |
|      | 1. Check if existing key file on active NOAM (the NOAM, which is intact and was not recovered) server is valid: |
|      | ```
|      | $ cd /usr/TKLC/dpi/bin/
|      | $ ./sharedKrevo -validate
|      | ```
|      | Example output: |
|      | ![Example output](image)
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:

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

   Example output:

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

   Example output:

   ```
   [admusr@NOAM-2 bin]$ ./sharedKrevo -updateData
   ```

   Example output:
Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>62.</td>
<td>Backup and archive all the databases from the recovered system. Execute Appendix A DSR Database Backup to back up the Configuration databases.</td>
</tr>
<tr>
<td>63.</td>
<td>Recover IDIH if IDIH were affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.</td>
</tr>
</tbody>
</table>

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

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 any failed SOAM and MP servers by recovering base hardware and software
  - Recover the base hardware
  - Recover the software

Database is already intact at one SOAM server and does not require restoration at the other SOAM and MP servers.
## Procedure 3.  Recovery Scenario 3

This procedure performs recovery if ALL NOAM servers are failed but 1 or more SOAM servers are intact. This includes any SOAM server that is in another location (spare SOAM server).

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

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

### Step 1. Gather required materials

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

### Step 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.

### Step 3. Replace failed equipment

HW vendor to replace the failed equipment.

### Step 4. RMS NOAM Failure:  
Configure BIOS settings and update firmware

If the failed server is NOT a rack mount server, **skip to step 8**.

1. Configure and verify the BIOS settings by executing procedure **Configure the RMS and Blade Server BIOS Settings** from reference [10].
2. Verify and/or upgrade server firmware by executing procedure **Upgrade Management Server Firmware** from reference [10].

**Note:** Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.

### Step 5. RMS NOAM Failure:  
Backups Available

If the failed server is NOT a rack mount server, **skip to step 8**.

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

Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media.

If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing Restore PMAC from Backup.

### Step 6. RMS NOAM Failure:  
Backups NOT available

If the failed server is NOT a rack mount server, **skip to step 8**.

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

If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures:

1. **Configure and IPM Management Server** from reference [10].
2. **Install PMAC** from reference [10].
3. **Configure PMAC** from reference [10].

If the PMAC is **NOT** located on the same TVOE host as the failed NOAM, Execute the following sections/procedures:

1. **Installing TVOE on Rack Mount Server(s)** from reference [10].
Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Recover failed aggregation/enclosure switches, and OAs</td>
</tr>
<tr>
<td>8.</td>
<td>HP-Class Blade Failure: Configure blade server iLO, update firmware/BIOS settings</td>
</tr>
<tr>
<td>9.</td>
<td>HP-Class Blade Failure: Backups available</td>
</tr>
<tr>
<td>10.</td>
<td>HP-Class Blade Failure: Backups NOT available</td>
</tr>
<tr>
<td>11.</td>
<td>Execute fast deployment file for NOAMs</td>
</tr>
</tbody>
</table>

Recover failed OAs, aggregation and enclosure switches, if needed.

**Backups Available:**

1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches.

**Backups NOT Available, execute:**

1. **HP C-7000 Enclosure Configuration** from reference [10] to recover and configure any failed OAs, if needed.
2. **Configure Enclosure Switches** from reference [10] to recover enclosure switches, if needed.

If the failed server is NOT an HP C-Class Blade, **skip to step 11.**

1. Execute **Configure Blade Server iLO Password for Administrator Account** from reference [10].
2. Verify/Update Blade server firmware and BIOS settings by executing **Server Blades Installation Preparation** from reference [10].

If the failed server is NOT an OAM type HP C-Class Blade, **skip to step 11.**

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

1. Install and configure TVOE on failed TVOE blade servers by executing **Install TVOE on Blade Servers** from reference [10].
2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on **ALL** failed TVOE Host blade servers.

If the failed server is NOT an OAM type HP C-Class Blade, **skip to step 11.**

This step assumes TVOE backups are **NOT** available.

Install and configure TVOE on failed TVOE blade servers by executing section **Install TVOE on Blade Servers** from reference [10].

The backup fdconfig file used during the initial DSR installation is available on the PMAC, if a database backup was restored on the PMAC.

If a backup fast deployment xml is **NOT** available, execute **Configure NOAM Servers** from reference [8].

If a backup fast deployment xml is already present on the PMAC, execute the following procedure:

1. Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade has been performed since initial installation).
2. Execute these commands:

   ```
   $ cd /usr/TKLC/smac/etc
   $ screen
   $ sudo fdconfig config --file=<Created_FD_File>.xml
   ```
**Procedure 3. Recovery Scenario 3**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.</td>
<td>Obtain latest database backup and network configuration data. Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. 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.</td>
</tr>
</tbody>
</table>
| 13.  | Execute DSR installation procedure for the first NOAM.  
1. Configure the first NOAM server by executing procedure Configure the First NOAM NE and Server from reference [8].  
2. Configure the NOAM server group by executing procedure Configure the NOAM Server Group from reference [8].  
*Note:* Use the backup copy of network configuration data and site surveys (step 2). |
| 14.  | NOAM GUI: Login  
Log into the NOAM GUI as the guiadmin user: |

![Oracle System Login](image)
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>15.</th>
<th><strong>NOAM GUI:</strong></th>
<th>Upload the backed up database file</th>
</tr>
</thead>
</table>

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

![Status & Manage > Files]

2. Select the active NOAM server.

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

![Upload File]

- 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.

4. Click **Browse** and locate the backup file.

5. Check **This is a backup file** checkbox.

6. Click **Upload**.
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 16. | **NOAM GUI:**  
    Disable provisioning |
| 1. | Navigate to **Status & Manage > Database.** |
| | ![Diagram](image1.png) |
| 2. | Click **Disable Provisioning.** |
| | ![Diagram](image2.png) |
| 3. | A confirmation window displays. Click **OK** to disable provisioning. |
| | ![Diagram](image3.png) |
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th></th>
<th>NOAM GUI: Verify the archive contents and database compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td>1. Select the <strong>Active NOAM</strong> server and click <strong>Compare</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Click the button for the restored database file uploaded as a part of Step 15 of this procedure.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Verify the output window matches the screen below.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A database mismatch regarding the Topology Compatibility and possibly User compatibility (due to authentication) displays. These warnings are expected. If these are the only mismatches, proceed; otherwise, stop and contact My Oracle Support (MOS) to ask for assistance.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Archive Contents and Database Compatibilities must be the following:</td>
</tr>
<tr>
<td></td>
<td><strong>Archive Contents</strong>: Configuration data.</td>
</tr>
<tr>
<td></td>
<td><strong>Database Compatibility</strong>: The databases are compatible.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The following is expected output for Topology Compatibility Check since we are restoring from existing backed up database to database with just one NOAM:</td>
</tr>
<tr>
<td></td>
<td><strong>Topology Compatibility</strong></td>
</tr>
<tr>
<td></td>
<td><strong>THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. If the verification is successful, click <strong>Back</strong>.</td>
</tr>
</tbody>
</table>
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.</td>
<td><strong>Active NOAM</strong>: Restore the database</td>
</tr>
</tbody>
</table>

1. Navigate to **Status & Manage > Database**.
2. Select the **Active NOAM** server and click **Restore**.
3. Select the backup provisioning and configuration file.
4. Click **OK**.
5. If you get errors related to the warnings highlighted in the previous step, that is expected. If no other errors display, mark the **Force** checkbox and click **OK** to proceed with the DB restore.

#### Database Restore Confirm

**incompatible archive selected**

The selected database came from ZombieNOA

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

**Confirm archive "backup/Backup.dsr.ZombieNOA"**

- Force Restore? 
  - Force
  - Force restore

**Note:** After the restore has started, the user is logged out of XMI NO GUI since the restored Topology is old data.
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>No.</th>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 19. | 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: |

   ![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.

| 20. | NOAM VIP GUI: Monitor and confirm database restoral | Wait for **5-10 minutes** for the System to stabilize with the new topology:  
Monitor the Info tab for **Success**. This indicates the restore is complete and the system is stabilized.  
Ignore the following 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).  

**Note:** Do not pay attention to alarms until all the servers in the system are completely restored.  

**Note:** The Configuration and Maintenance information is in the same state it was when backed up during initial backup. |
Procedure 3. Recovery Scenario 3

21. **Active NOAM:**
   - Set failed servers to OOS

   1. Navigate to **Status & Manage > HA**.
      - Click **Edit**.
   2. **Modifying HA attributes**
      - **Hostname** | **Max Allowed HA Role** | **Description**
        - ZombieNOAM1 | Active | The maximum des
        - ZombieNOAM2 | Active | The maximum des
        - ZombieDRNOAM1 | OOS | The maximum des

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

22. **Active NOAM:**
   - Login

23. **NOAM VIP GUI:**
   - Recover standby NOAM

   Install the second NOAM server by executing procedure **Configure the Second NOAM Server**, steps 3-5, 7 from reference [8].

   **Note:** Execute step 6 if NetBackup is used.
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 24.  | **NOAM VIP GUI:** Set HA on standby NOAM  
1. Navigate to **Status & Manage > HA.**  
   ![Diagram of NOAM VIP GUI](image1.png)  
   2. Click **Edit.**  
   3. Select the standby NOAM server and set it to **Active.**  
   ![Modifying HA attributes](image2.png)  
   4. Click **OK.** |
| 25.  | **NOAM VIP GUI:** Restart DSR application  
1. Navigate to **Status & Manage > Server.**  
   ![Diagram of NOAM VIP GUI](image3.png)  
   2. Select the recovered standby NOAM server and click **Restart.** |
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26.</td>
<td><strong>Active NOAM:</strong> Correct the recognized authority table</td>
</tr>
<tr>
<td></td>
<td>1. Establish an SSH session to the active NOAM and login as <code>admusr</code>.</td>
</tr>
<tr>
<td></td>
<td>2. Execute this command:</td>
</tr>
</tbody>
</table>
|     | ```
|     | $ sudo top.setPrimary
|     | --- Using my cluster: A1789
|     | --- Updating A1789.022: <DSR_NOAM_B_hostname>
|     | --- Updating A1789.144: <DSR_NOAM_A_hostname>
|     | ``` |
| 27. | Install NetBackup client (Optional) |
|     | If NetBackup is used, execute **Install NetBackup Client** from reference [8]. |
| 28. | **NOAM VIP GUI:** Perform Keyexchange with export server |
|     | 1. Navigate to Administration > Remote Servers > Data Export. |
|     | ![Administration tree](image) |
|     | 2. Click the **Task Name** and click **Key Exchange**. |
|     | ![Task Name selection](image) |
|     | 3. **Type the Password** and click **OK**. |
|     | ![Password entry](image) |
|     | 4. Repeat for each task. |
Procedure 3. Recovery Scenario 3

### 29. NOAM VIP GUI: Recover failed SOAM servers

Recover failed SOAM servers (standby, spare) by repeating these steps for each SOAM server:

1. Execute the **Configure the SOAM Servers** procedure, steps 1-3 and 5-8, from reference [8].
   
   **Note**: If you are using NetBackup, also execute step 10.

2. If you are using NetBackup, execute the **Install NetBackup Client** procedure from reference [8].

### 30. NOAM VIP GUI: Set HA on standby SOAM

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

2. Click **Edit**.

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

4. Click **OK**.
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **31.** | **NOAM VIP GUI:** Restart DSR application  
1. Navigate to Status & Manage > Server.  
2. Select the recovered standby SOAM server and click **Restart**.  

| **32.** | **NOAM VIP GUI:** Recover the C-level server (DA-MP, SBRs, IPFE, SS7-MP)  
1. Navigate to Status & Manage > Server.  
2. Select the recovered standby SOAM server and click **Restart**.  
3. Execute **Configure MP Blade Servers**, Steps 1, 7, 11-14, and 17, from reference [8].  
   **Note:** Also, execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. Repeat this step for any remaining failed MP servers.  

| **33.** | **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**.  

<table>
<thead>
<tr>
<th>Server</th>
<th>Desired HA Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieDAMP1</td>
<td><strong>Active</strong></td>
<td>The maximum desired HA Role for ZombieDAMP1</td>
</tr>
<tr>
<td>ZombieDAMP2</td>
<td><strong>Active</strong></td>
<td>The maximum desired HA Role for ZombieDAMP2</td>
</tr>
</tbody>
</table>
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 34.  | **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.**  |
| 35.  | **NOAM VIP 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. A confirmation window displays. Click **OK** to enable Provisioning.  |
| 36.  | **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>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 37. | **Active NOAM:** Activate optional features<br>Establish an SSH session to the active NOAM, login as **admusr**.  
**Note For PCA Feature Activation:**<br>If you have PCA installed in the system being recovered, re-activate PCA by executing **PCA Activation on Active NOAM server** on the recovered active NOAM server and **PCA Activation on Standby SOAM server** on the recovered standby SOAM from [13].  
Refer to 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}
```
**Note:** If any of the MPs are failed and recovered, then restart these MP servers after activation of the feature. |
| 38. | **NOAM VIP GUI:**<br>Fetch and store the database report for the newly restored data and save it<br>1. Navigate to **Status & Manage > Database**.<br>2. Select the active NOAM server and click **Report**.<br>The following screen is displayed:<br>**Main Menu: Status & Manage -> Database [Report]**<br>3. Click **Save** and save the report to your local machine. |
## Procedure 3. Recovery Scenario 3

### Active NOAM: Verify replication between servers

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

   ```
sudo irepstat -m
   ```

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

### NOAM VIP GUI: Verify the database states

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

   ![Status & Manager > Database]

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

<table>
<thead>
<tr>
<th>Network Element</th>
<th>Server</th>
<th>Role</th>
<th>OAM Max HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieDRNOAM</td>
<td>ZombieDRNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM2</td>
<td>Network OAM&amp;P</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM1</td>
<td>System OAM</td>
<td>N/A</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>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>ZombieDAMP2</td>
<td>MP</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSS7MP2</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSS7MP1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombiePFE1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombiePFE2</td>
<td>MP</td>
<td>Active</td>
</tr>
</tbody>
</table>
Procedure 3. Recovery Scenario 3

41. **NOAM VIP GUI:** Verify the HA status
   1. Navigate to **Status & 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>ZoombaNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZoombaNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZoombaRRNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZoombaRRNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZoombaSOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZoombaSOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Standby</td>
</tr>
</tbody>
</table>

42. **SOAM VIP GUI:** Verify the local node info
   1. Navigate to **Diameter > Configuration > Local Node**.
   2. Verify all the local nodes are shown.

43. **SOAM VIP GUI:** Verify the peer node info
   1. Navigate to **Diameter > Configuration > Peer Node**.
   2. Verify all the peer nodes are shown.
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 44.  | **SOAM VIP GUI:** Verify the connections info | 1. Navigate to **Diameter > Configuration > Connections**.  
   - Ensure all connections are shown. |
| 45.  | **SOAM VIP GUI:** Enable Connections, if needed | 1. Navigate to **Diameter > Maintenance > Connections**.  
   - Select each connection and click **Enable**. Alternatively, enable all connections by clicking **Enable All**.  
   - 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. |
| 46.  | **SOAM VIP GUI:** Enable optional features | 1. Navigate to **Diameter > Maintenance > Applications**.  
   - Select the optional feature application configured in step 36.  
   - Click **Enable**. |
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>SOAM VIP GUI: Re-enable transports, if needed</th>
<th>SOAM VIP GUI: Re-enable MAPIWF application, if needed</th>
<th>SOAM VIP GUI: Re-enable links, if needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>47.</td>
<td>Navigate to <strong>Transport Manager &gt; Maintenance &gt; Transport</strong>. Select each transport and click <strong>Enable</strong>. Verify the Operational Status for each transport is <strong>Up</strong>.</td>
<td>Navigate to <strong>SS7/Sigtran &gt; Maintenance &gt; Local SCCP Users</strong>. Click the <strong>Enable</strong> button corresponding to MAPIWF Application Name. Verify the SSN Status is <strong>Enabled</strong>.</td>
<td>Navigate to <strong>SS7/Sigtran &gt; Maintenance &gt; Links</strong>. Click <strong>Enable</strong> for each link. Verify the Operational Status for each link is <strong>Up</strong>.</td>
</tr>
<tr>
<td>48.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>49.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>50.</th>
<th><strong>NOAM VIP:</strong> Verify all servers in topology are accessible (RADIUS Only)</th>
</tr>
</thead>
</table>

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

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

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

**Example output:**

```
1450112012: [INFO] 'SOAM-2' is accessible.
FIPS integrity verification test failed.
The authenticity of host 'ipfe (10.240.146.16)' can't be established.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ipfe,10.240.146.16' (RSA) to the list of known hosts.
1450112015: [INFO] 'IFFE' is accessible.
FIPS integrity verification test failed.
The authenticity of host '10.240.146.24' can't be established.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'IFFE,10.240.146.24' (RSA) to the list of known hosts.
1450112017: [INFO] 'MF-2' is accessible.
FIPS integrity verification test failed.
The authenticity of host 'mp-2 (10.240.146.14)' can't be established.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'MF-2,10.240.146.14' (RSA) to the list of known hosts.
1450112020: [INFO] 'MF-1' is accessible.
```

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

<table>
<thead>
<tr>
<th></th>
<th><strong>SOAM VIP:</strong> Copy key file to all the servers in topology (RADIUS only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>51.</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 <code>admusr</code>.</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
|   | Example output: ```
|   | ```
|   | [admusr@NOAM-2 bin]$ ./sharedKrevo -validate
|   | FIPS integrity verification test failed.
|   | 1450723458: [INFO] Key file for 'NOAM-1' is valid
|   | 1450723458: [INFO] Key file for 'NOAM-2' is valid
|   | FIPS integrity verification test failed.
|   | FIPS integrity verification test failed.
|   | 1450723459: [INFO] Key file for 'SOAM-1' is valid
|   | FIPS integrity verification test failed.
|   | FIPS integrity verification test failed.
|   | 1450723460: [INFO] Key file for 'SOAM-2' is valid
|   | FIPS integrity verification test failed.
|   | FIPS integrity verification test failed.
|   | 1450723461: [INFO] Key file for 'IPFE' is valid
|   | FIPS integrity verification test failed.
|   | FIPS integrity verification test failed.
|   | 1450723461: [INFO] Key file for 'MP-2' is valid
|   | FIPS integrity verification test failed.
|   | FIPS integrity verification test failed.
|   | 1450723462: [INFO] Key file for 'MP-1' is valid
|   | [admusr@NOAM-2 bin]$ |
|   | ```
|   | 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 SOAM, 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

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

1. Establish an SSH session to any of the active NOAM. Login as admusr.
2. Copy the key file to all the servers in the topology:

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

   **Example output:**
   ```
   $ ./sharedKrevo updateData
   ```

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

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).
Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
</table>
| 54. | **NOAM VIP GUI:** Examine all alarms  
   1. Log into the NOAM VIP if not already logged in.  
   2. Navigate to **Alarms & Events > View Active.**  
   3. Examine all active alarms and refer to the online help on how to address them.  
   If needed, contact My Oracle Support (MOS). |
| 55. | Restore GUI usernames and passwords  
   If applicable, execute Resolve User Credential Issues after Database Restore to recover the user and group information restored. |
| 56. | Backup and archive all the databases from the recovered system  
   Execute DSR Database Backup to back up the Configuration databases. |
| 57. | Recover IDIH  
   If IDIH were affected, refer to IDIH Disaster Recovery to perform disaster recovery on IDIH. |
| 58. | SNMP workaround  
   Refer SNMP Configuration to configure SNMP as a workaround in the following cases:  
   1. If SNMP is not configured in DSR.  
   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
- The database is intact at the active NOAM server and does not require restoration at the standby NOAM server
  - Recover any failed SO and MP servers by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- The database is intact at the active NOAM server and does not require restoration at the SO and MP servers
- Re-apply signaling networks configuration if the failed blade is an MP

**Procedure 4. Recovery Scenario 4**

<table>
<thead>
<tr>
<th>Step #</th>
<th>Workarounds</th>
<th>Gather required materials</th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
</table>
| 1.     | Revert from signaling networks configuration if the failed blade is an MP. 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. | Refer to SNMP Configuration to configure SNMP as a workaround in the following cases: 1. If SNMP is not configured in DSR 2. If SNMP is already configured and SNMPv3 is selected as enabled version | Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  
http://<Primary_NOAM_VIP_IP_Address>  
  2. Login as the guiadmin user: |
## Recovery Scenario 4

### Active NOAM

1. Navigate to **Status & Manage > HA**.
2. **Edit**.
3. Set the Max Allowed HA Role to **OOS** for the failed servers.
4. **Select OK**.

### RMS NOAM Failure

1. **Configure BIOS settings and update firmware**.
2. **Verify and/or upgrade server firmware**.

**Note:** Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.

### RMS NOAM Failure: Backups available

1. **Restore the TVOE backup** by executing Restore TVOE Configuration from Backup Media.
2. **If the PMAC is located on the same TVOE host as the failed NOAM**, restore the PMAC backup by executing Restore PMAC from Backup.
### Procedure 4. Recovery Scenario 4

#### 7. RMS NOAM Failure: Backups NOT available

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

If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures:

1. **Configure and IPM Management Server** from reference [10].
2. **Install PMAC** from reference [10].
3. **Configure PMAC** from reference [10].

If the PMAC is NOT located on the same TVOE host as the failed NOAM, execute the following sections/procedures:

1. **Installing TVOE on Rack Mount Server(s)** from reference [10].

#### 8. Recover failed aggregation/enclosure switches, and OAs

Recover failed OAs, aggregation and enclosure switches, if needed.

Backups Available:

1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches

Backups NOT available, execute:

1. **HP C-7000 Enclosure Configuration** from reference [10] to recover and configure any failed OAs, if needed.
2. **Configure Enclosure Switches** from reference [10] to recover enclosure switches, if needed.

#### 9. HP-Class Blade Failure: Configure blade server iLO, update firmware/BIOS settings

If the failed server is **NOT** an HP C-Class Blade, **skip to step 12**.

1. **Configure Blade Server iLO Password for Administrator Account** from reference [10].
2. Verify/Update blade server firmware and BIOS settings by executing **Server Blades Installation Preparation** from reference [10].

#### 10. HP-Class Blade Failure: Backups available

If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 13**. This step assumes that TVOE backups are available, if backups are **NOT** available, **skip this step**.

1. Install and configure TVOE on failed TVOE blade servers by executing **Install TVOE on Blade Servers** from reference [10].
2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers.

#### 11. HP-Class Blade Failure: Backups NOT available

If the failed server is **NOT** an OAM HP C-Class Blade, **skip to step 13**. This step assumes that TVOE backups are **NOT** available

1. Install and configure TVOE on failed TVOE blade servers by executing **Install TVOE on Blade Servers** from reference [10].
2. Configure the NOAM and/or SOAM failed TVOE server blades by executing **Configure SOAM TVOE Server Blades** from reference [8].

**Note:** Although the title of the procedure is related to SOAMs only, execute this procedure for any failed NOAMs located on TVOE server blades.
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.</td>
<td>Create VMs</td>
<td>Execute Create NOAM/SOAM Virtual Machines to create the NOAM and SOAM VMs on failed TVOE servers.</td>
</tr>
</tbody>
</table>
| 13.  | IPM and install DSR application on failed guest/servers | 1. Execute IPM Blades and VMs for the failed SOAM VMs and MP blades from reference [8].  
2. Execute Install the Application Software for the failed NOAM and SOAM VMs and MP blades from reference [8]. |
| 14.  | Install NetBackup client (Optional) | If NetBackup is used, execute Install NetBackup Client from reference [8]. |
| 15.  | 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:  
   
   [Insert URL]  
   
   2. Login as the guiadmin user:  
   
   ![Oracle System Login](image) |
| 16.  | Exchange SSH keys between PMAC and failed NOAM server | 1. Use the PMAC GUI to determine the Control Network IP address of the failed NOAM server VM. From the PMAC GUI, navigate to Software > Software Inventory.  
2. Note the IP address for the failed NOAM server VM.  
3. Log into the PMAC terminal as the admusr.  
4. From a terminal window connection on the PMAC as the admusr user, exchange SSH keys for admusr between the PMAC and the failed NOAM server VM control network IP address. When prompted for the password, enter the password for the admusr user of the NOAM server.  
   
   `$ keyexchange admusr@<NO2_Control_IP_Address>` |

**Note:** If Key exchange fails, edit /home/admusr/.ssh/known_hosts and remove blank lines, and retry the keyexchange commands.
## Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 17.  | **NOAM VIP GUI:** Export the initial configuration  
   1. Navigate to **Configuration > Servers.**  
   2. From the GUI screen, select the failed NOAM server and click **Export** to generate the initial configuration data for that server. |
| 18.  | **NOAM VIP:** Copy configuration file to failed NOAM server  
   1. Obtain a terminal session to the NOAM VIP, login as the **admusr.**  
   2. Use the **awpushcfg** utility to copy the configuration file created in the previous step from the `/var/TKLC/db/filemgmt` directory on the active NOAM to the failed NOAM server, using the Control network IP address for the failed NOAM VM.  
   The configuration file has a filename like `TKLCCfgData.<hostname>.sh`.  
   $ sudo awpushcfg  
   3. The awpushcfg utility is interactive, so the user is prompted for the following:  
      - IP address of the local PMAC server: Use the local control network address from the PMAC.  
      - Username: Use **admusr**  
      - Control network IP address for the target server: In this case, enter the control IP for the failed NOAM VM.  
      - Hostname of the target server: Enter the server name from Step 17. |
| 19.  | **Failed NOAM Server:** Verify awpushcfg was called and reboot the server  
   1. Establish an SSH session to the failed NOAM server, login as the **admusr** user.  
   2. The automatic configuration daemon looks for the file named `TKLCCfgData.sh` in the `/var/tmp` directory, implements the configuration in the file, and asks the user to reboot the server.  
   3. Verify awpushcfg was called by checking the following file  
      $ sudo cat /var/TKLC/appw/logs/Process/install.log  
      Verify this message displays:  
      `[SUCCESS] script completed successfully!`  
   4. Now reboot the server:  
      $ sudo init 6  
   5. Wait for the server to reboot |
### Procedure 4. Recovery Scenario 4

#### 20. Failed NOAM Server: Configure networking for dedicated NetBackup interface (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong></td>
<td>Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.</td>
</tr>
<tr>
<td>Obtain a terminal window to the failed NOAM server, logging in as the <code>admusr</code>.</td>
<td></td>
</tr>
</tbody>
</table>

```
$ sudo /usr/TKLCL/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP_Address> --netmask=<NO2_NetBackup_NetMask>
```

```
$ sudo /usr/TKLCL/plat/bin/netAdm add --route=net --device=netbackup --address=<NO1_NetBackup_Network_ID> --netmask=<NO2_NetBackup_NetMask> --gateway=<NO2_NetBackup_Gateway_IP_Address>
```

#### 21. Failed NOAM Server: Verify server health

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute this command on the 2nd NOAM server and make sure no errors are returned:</td>
<td></td>
</tr>
</tbody>
</table>

```
$ sudo syscheck
Running modules in class hardware...OK
Running modules in class disk...OK
Running modules in class net...OK
Running modules in class system...OK
Running modules in class proc...OK
LOG LOCATION: /var/TKLCL/log/syscheck/fail_log
```
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td><strong>NOAM VIP GUI:</strong> Set HA on standby NOAM</td>
</tr>
</tbody>
</table>
|      | 1. Navigate to **Status & Manage > HA.**  
|      |   - **Hostname** | **Max Allowed HA Role** | **Description** |
|      | ZombieNOAM1 | Active | The maximum |
|      | ZombieNOAM2 | Active | The maximum |
|      | ZombieNRNOAM1 | Standby | Spare |
|      | 2. Click **Edit.**  
|      | 3. Select the standby NOAM server and set it to **Active.**  
|      | Modifying **HA attributes** |
|      | 4. Click **OK.** |
| 23.  | **NOAM VIP GUI:** Restart DSR application  
|      | 1. Navigate to **Status & Manage > Server.**  
|      | 2. Select the recovered standby NOAM server and click **Restart.** |
| 24.  | **NOAM VIP GUI:** Recover failed SOAM servers  
|      | Recover failed SOAM servers (standby, spare) by repeating these steps for each SOAM server:  
|      | 1. Execute **Configure the SOAM Servers,** steps 1-3 and 5-8, from reference [8].  
|      |   - **Note:** If you are using NetBackup, also execute step 10.  
|      | 2. If you are using NetBackup, execute **Install NetBackup Client** from reference [8]. |
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>25.</td>
<td><strong>NOAM VIP GUI</strong>: Set HA on standby SOAM</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; HA</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>4. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>26.</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 SOAM server and click <strong>Restart</strong>.</td>
</tr>
<tr>
<td>27.</td>
<td><strong>NOAM VIP GUI</strong>: Recover the C-level server (DA-MP, SBRs, IPFE, SS7-MP)</td>
</tr>
</tbody>
</table>
|      | 1. Execute **Configure MP Blade Servers**, steps 1, 7, 11-14, and 17, from reference [8].  
  **Note**: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. |
|      | 2. Repeat this step for any remaining failed MP servers. |
## Procedure 4. Recovery Scenario 4

### 28. 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**.

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

1. Navigate to **Status & Manage > Server**.
2. Select the recovered C-level servers and click **Restart**.

### 30. Active NOAM: Login

1. Log into the recovered active NOAM using SSH terminal as **admusr** user.

### 31. Active NOAM: Perform key exchange between the active-NOAM and recovered servers

1. Establish an SSH session to the active NOAM, login as **admusr**.
2. Perform a key exchange from the active NOAM to each recovered server:

   ```bash
   $ keyexchange admusr@<Recovered Server Hostname>
   ```
### Procedure 4.  Recovery Scenario 4

|   | Active NOAM: Activate optional features | Establish an SSH session to the active NOAM, login as `admusr`. **Note For PCA Feature Activation:**
|   |   | If you have PCA installed in the system being recovered, re-activate PCA by executing **PCA Activation on Standby NOAM Server** on the recovered standby NOAM server and **PCA Activation on Standby SOAM server** on the recovered standby SOAM server from [13].
|   |   | Refer to 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}`
|   |   | **Note:** If any of the MPs are failed and recovered, then restart these MP servers after activation of the feature.

|   | MP Servers: Disable SCTP auth flag (DSR Only) | DSR Only, SDS **Skip This Step.**
|   |   | For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [14].
|   |   | Execute this procedure on all failed MP servers. |
### Procedure 4. Recovery Scenario 4

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

   ![Status & Manage](image)

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

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

   ![Report and Init](image)

   The following screen is displayed:

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

   ![Database Status Report](image)

   From: Active Network OAM6 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 : 6.3
   Application Database Version :

   Capacities and Utilization
   ---------------------------------
   Disk Utilization 8.4%: 585M used of 7.0G total, 6.0G available
   Memory Utilization 0.0%: used of total, 0M available

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

<table>
<thead>
<tr>
<th></th>
<th>Active NOAM: Verify replication between servers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>35.</td>
<td>1. Log into the active NOAM using SSH terminal as <code>admusr</code>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Execute this command:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>sudo irepstat -m</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example output:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>-- Policy 0 ActStb [DbReplication] ---------------</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RDU06-MP1 -- Stby</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>BC From RDU06-SO1 Active 0 0.50 ^0.17%cpu 42B/s A=none</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>CC From RDU06-MP2 Active 0 0.10 ^0.17 0.88%cpu 32B/s A=none</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RDU06-MP2 -- Active</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>BC From RDU06-SO1 Active 0 0.50 ^0.10%cpu 33B/s A=none</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>CC To RDU06-MP1 Active 0 0.10 0.08%cpu 20B/s A=none</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RDU06-NO1 -- Active</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>AB To RDU06-SO1 Active 0 0.50 1%R 0.03%cpu 21B/s</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RDU06-SO1 -- Active</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>AB From RDU06-NO1 Active 0 0.50 ^0.04%cpu 24B/s</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>BC To RDU06-MP1 Active 0 0.50 1%R 0.04%cpu 21B/s</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>BC To RDU06-MP2 Active 0 0.50 1%R 0.07%cpu 21B/s</code></td>
<td></td>
</tr>
</tbody>
</table>
Procedure 4. Recovery Scenario 4

36. **NOAM VIP GUI**: Verify the database states

<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>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM2</td>
<td>System OAM</td>
<td>N/A</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM1</td>
<td>System OAM</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM</td>
<td>ZombieDRNOAM2</td>
<td>Network OAM&amp;P</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSAMP2</td>
<td>MP</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSAMP1</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>

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

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

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

37. **NOAM VIP GUI**: Verify the HA status

<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>ZombieNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM1</td>
<td>Standby</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>

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

   - Navigate to **Status & Manage**
    - **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**.
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>SOAM VIP GUI:</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>38.</td>
<td>Verify the local node info</td>
<td>1.</td>
<td>Navigate to <strong>Diameter &gt; Configuration &gt; Local Nodes</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.</td>
<td>Verify all the connections are shown.</td>
</tr>
<tr>
<td>39.</td>
<td>Verify the peer node info</td>
<td>1.</td>
<td>Navigate to <strong>Diameter &gt; Configuration &gt; Peer Node</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.</td>
<td>Verify all the peer nodes are shown.</td>
</tr>
<tr>
<td>40.</td>
<td>Verify the connections info</td>
<td>1.</td>
<td>Navigate to <strong>Diameter &gt; Configuration &gt; Connections</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.</td>
<td>Verify all the connections are shown.</td>
</tr>
</tbody>
</table>
### Procedure 4. Recovery Scenario 4

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

1. Navigate to **Diameter > Maintenance > Connections**.

    - **Maintenance**
    - **Route Lists**
    - **Route Groups**
    - **Peer Nodes**
    - **Connections**

2. Select each connection and click **Enable**. Alternatively, you can 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.

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

1. Navigate to **Diameter > Maintenance > Applications**.

    - **Maintenance**
    - **Route Lists**
    - **Route Groups**
    - **Peer Nodes**
    - **Connections**
    - **Egress Throttle Groups**
    - **Applications**

2. Select the optional feature application configured in step 32.

3. Click **Enable**.

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

1. Navigate to **Transport Manager > Maintenance > Transport**.

    - **Transport Manager**
    - **Configuration**
    - **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>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.</td>
<td><strong>SOAM VIP GUI</strong>: Re-enable MAPIWF application, if needed</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>SS7/Sigtran &gt; Maintenance &gt; Local SCCP Users</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>SS7/Sigtran</strong>&lt;br&gt;  - <strong>Configuration</strong>&lt;br&gt;  - <strong>Maintenance</strong>&lt;br&gt;  - Local SCCP Users&lt;br&gt;  - Remote Signaling Points&lt;br&gt;  - Remote MTP3 Users&lt;br&gt;  - Linksets&lt;br&gt;  - Links</td>
</tr>
<tr>
<td>2.</td>
<td>Click the <strong>Enable</strong> button corresponding to MAPIWF Application Name.</td>
</tr>
<tr>
<td>3.</td>
<td>Verify the SSN Status is <strong>Enabled</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>45.</td>
<td><strong>SOAM VIP GUI</strong>: Re-enable links, if needed</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>SS7/Sigtran &gt; Maintenance &gt; Links</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>SS7/Sigtran</strong>&lt;br&gt;  - <strong>Configuration</strong>&lt;br&gt;  - <strong>Maintenance</strong>&lt;br&gt;  - Local SCCP Users&lt;br&gt;  - Remote Signaling Points&lt;br&gt;  - Remote MTP3 Users&lt;br&gt;  - Linksets&lt;br&gt;  - Links</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Enable</strong> for each link.</td>
</tr>
<tr>
<td>2.</td>
<td>Verify the Operational Status for each link is <strong>Up</strong>.</td>
</tr>
</tbody>
</table>
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>46.</td>
<td><strong>NOAM VIP:</strong> Verify all servers in topology are accessible (RADIUS Only)</td>
<td>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</td>
</tr>
<tr>
<td></td>
<td>1. Establish an SSH session to the NOAM VIP and login as <code>admusr</code>.</td>
<td>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>2. Check if all the servers in the Topology are accessible:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>$ cd /usr/TKLC/dpi/bin/</code></td>
<td>Example output:</td>
</tr>
<tr>
<td></td>
<td><code>$ ./sharedKrevo -checkAccess</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example output:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>FIPS integrity verification test failed.</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>1450723084: [INFO] 'NOAM-1' is accessible.</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>FIPS integrity verification test failed.</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>1450723084: [INFO] 'SOAM-1' is accessible.</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>FIPS integrity verification test failed.</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>1450723084: [INFO] 'SOAM-2' is accessible.</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>FIPS integrity verification test failed.</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>1450723085: [INFO] 'IPFE' is accessible.</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>FIPS integrity verification test failed.</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>1450723085: [INFO] 'MP-2' is accessible.</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>FIPS integrity verification test failed.</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>1450723086: [INFO] 'MP-1' is accessible.</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>[admusr@NOAM-2 bin]$</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If any of the servers are not accessible, stop and contact My Oracle Support (MOS).</td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>47.</td>
<td><strong>NOAM VIP:</strong> Copy key file to all the servers in topology (RADIUS Only)</td>
</tr>
<tr>
<td>1.</td>
<td>Check if existing key file on active NOAM server is valid:</td>
</tr>
<tr>
<td></td>
<td><code>$ ./sharedKrevo -validate</code></td>
</tr>
</tbody>
</table>
| | ![Output of the command showing validation results](image)
| | If output of above command shows that existing key file is not valid, then contact My Oracle Support (MOS). |
| 2. | Copy the key file to all the servers in the Topology: |
| | `$ ./sharedKrevo -synchronize` |
| | ![Output of the command showing synchronization results](image) |
| | `$ ./sharedKrevo -updateData` |
| | ![Output of the command showing data update results](image) |
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>48.</td>
<td>SOAM VIP GUI: Examine all alarms</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Alarms &amp; Events &gt; View Active</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Examine all active alarms and refer to the on-line help on how to address them. If needed, contact My Oracle Support (MOS).</td>
</tr>
<tr>
<td>49.</td>
<td>NOAM VIP GUI: Examine all alarms</td>
</tr>
<tr>
<td></td>
<td>1. Log into the NOAM VIP if not already logged in.</td>
</tr>
<tr>
<td></td>
<td>2. Navigate to <strong>Alarms &amp; Events &gt; View Active</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Examine all active alarms and refer to the on-line help on how to address them. If needed, contact My Oracle Support (MOS).</td>
</tr>
<tr>
<td>50.</td>
<td>Restart oampAgent, if needed</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If alarm 10012: The responder for a monitored table failed to respond to a table change is raised, the oampAgent needs to be restarted.</td>
</tr>
<tr>
<td></td>
<td>1. Establish an SSH session to each server that has the alarm, login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Execute these commands:</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo pm.set off oampAgent</code></td>
</tr>
<tr>
<td></td>
<td><code>$ sudo pm.set on oampAgent</code></td>
</tr>
<tr>
<td>51.</td>
<td>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>
<tr>
<td>52.</td>
<td>Recover IDIH</td>
</tr>
<tr>
<td></td>
<td>If IDIH were affected, refer to IDIH Disaster Recovery to perform disaster recovery on IDIH.</td>
</tr>
</tbody>
</table>
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

Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Workarounds Refer to SNMP Configuration to configure SNMP as a workaround in the following cases: 1. If SNMP is not configured in DSR. 2. If SNMP is already configured and SNMPv3 is selected as enabled version.</td>
</tr>
<tr>
<td>2.</td>
<td>Gather required materials Gather the documents and required materials listed in Required Materials section.</td>
</tr>
<tr>
<td>3.</td>
<td>Switch DR NOAM to primary Refer to DSR/SDS 8.x NOAM Failover User’s Guide [17].</td>
</tr>
<tr>
<td>4.</td>
<td>Recover failed SOAMs If ALL SOAM servers have failed, execute Procedure 2.</td>
</tr>
</tbody>
</table>

This procedure performs recovery if both NOAM servers have failed but a DR NOAM is available. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.
### Procedure 5.  Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | Establish a GUI session on the DR-NOAM server by using the VIP IP address of the DR-NOAM server. Open the web browser and enter a URL of:  

```
http://<Primary_DR-NOAM_VIP_IP_Address>
```

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

![Oracle System Login](image-url)
## Procedure 5. Recovery Scenario 5

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.</strong></td>
<td><strong>DR-NOAM VIP GUI:</strong> Set failed NOAM servers to standby</td>
</tr>
<tr>
<td></td>
<td><strong>1.</strong> Navigate to <strong>Status &amp; Manage &gt; HA.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>2.</strong> Click <strong>Edit.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Modifying HA attributes</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Hostname</strong></td>
</tr>
<tr>
<td>ZombieNOAM1</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM2</td>
<td>OOS</td>
</tr>
<tr>
<td>ZombieDRNOAM1</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>3.</strong> Set the Max Allowed HA Role option to <strong>OOS</strong> for the failed servers.</td>
</tr>
<tr>
<td></td>
<td><strong>4.</strong> Click <strong>OK.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Ok</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>7.</strong></td>
<td><strong>RMS NOAM Failure:</strong> Configure BIOS settings and update firmware</td>
</tr>
<tr>
<td></td>
<td>If the failed server is <strong>NOT</strong> a rack mount server, <strong>skip to step 11.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>1.</strong> Configure and verify the BIOS settings by executing procedure <strong>Configure the RMS and Blade Server BIOS Settings</strong> from reference [10].</td>
</tr>
<tr>
<td></td>
<td><strong>2.</strong> Verify and/or upgrade server firmware by executing procedure <strong>Upgrade Management Server Firmware</strong> from reference[10].</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.</td>
</tr>
<tr>
<td><strong>8.</strong></td>
<td><strong>RMS NOAM Failure:</strong> Backups available</td>
</tr>
<tr>
<td></td>
<td>If the failed server is <strong>NOT</strong> a rack mount server, <strong>skip to step 11.</strong></td>
</tr>
<tr>
<td></td>
<td>This step assumes that TVOE and PMAC backups are available, if backups are <strong>NOT</strong> available, <strong>skip this step.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>1.</strong> Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media.</td>
</tr>
<tr>
<td></td>
<td><strong>2.</strong> If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing Restore PMAC from Backup.</td>
</tr>
</tbody>
</table>
### Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th></th>
<th>Recover failed aggregation/enclosure switches, and OAs</th>
<th>Recover failed OAs, aggregation and enclosure switches, if needed. <strong>Backups available:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Recover failed OAs, aggregation and enclosure switches, if needed. <strong>Backups available:</strong></td>
<td>1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches. <strong>Backups NOT available, execute:</strong></td>
</tr>
<tr>
<td></td>
<td>1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches.</td>
<td>1. <strong>HP C-7000 Enclosure Configuration</strong> from reference [10] to recover and configure any failed OAs, if needed.</td>
</tr>
<tr>
<td></td>
<td>2. <strong>Configure Enclosure Switches</strong> from reference [10] to recover enclosure switches, if needed.</td>
<td>2. <strong>Configure Enclosure Switches</strong> from reference [10] to recover enclosure switches, if needed.</td>
</tr>
</tbody>
</table>

| 10 | RMS NOAM Failure: Backups NOT available | If the failed server is **NOT** a rack mount server, **skip to step 11.** |
|    |                                          | This step assumes that TVOE and PMAC backups are **NOT** available, if the TVOE and PMAC have already been restored, **skip this step.** |
|    |                                          | If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures: |
|    |                                          | 1. **Configure and IPM Management Server** from reference [10]. |
|    |                                          | 2. **Install PMAC** from reference [10]. |
|    |                                          | 3. **Configure PMAC** from reference [10]. |
|    |                                          | If the PMAC is **NOT** located on the same TVOE host as the failed NOAM, execute the following sections/procedures: |
|    |                                          | 1. **Installing TVOE on Rack Mount Server(s)** from reference [10]. |

| 11 | HP-Class Blade Failure: Configure blade server iLO, update firmware/BIOS settings | If the failed server is **NOT** an HP C-Class Blade, **skip to step 14.** |
|    |                                          | 1. Execute **Configure Blade Server iLO Password for Administrator Account** from reference [10]. |
|    |                                          | 2. Verify/Update Blade server firmware and BIOS settings by executing **Server Blades Installation Preparation** from reference [10] |

| 12 | HP-Class Blade Failure: Backups available | If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 14.** |
|    |                                          | This step assumes that TVOE backups are available. If backups are **NOT** available, **skip this step.** |
|    |                                          | 1. Install and configure TVOE on failed TVOE blade servers by executing **Install TVOE on Blade Servers** from reference [10]. |
|    |                                          | 2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on **ALL** failed TVOE Host blade servers. |

| 13 | HP-Class Blade Failure: Backups NOT available | If the failed server is **NOT** an OAM type HP C-Class Blade, **skip to step 14.** |
|    |                                          | This step assumes TVOE backups are **NOT** available. |
|    |                                          | Install and configure TVOE on failed TVOE blade servers by executing **Install TVOE on Blade Servers** from reference [10]. |
Procedure 5.  Recovery Scenario 5

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 14 | Execute fast deployment file for NOAMs | The backup fdconfig file used during the initial DSR installation is available on the PMAC, if a database backup was restored on the PMAC. If a backup fast deployment xml is NOT available, execute Configure NOAM Servers from reference [8]. If a backup fast deployment xml is already present on the PMAC, execute the following procedure:
1. Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade has been performed since initial installation).
2. Execute these commands:
   $ cd /usr/TKLC/smac/etc
   $ screen
   $ sudo fdconfig config --file=<Created_FD_File>.xml |
| 15 | DR-NOAM VIP GUI: Export the initial configuration | 1. Navigate to Configuration > Servers.
   2. From the GUI screen, select the failed NOAM server and click Export to generate the initial configuration data for that server. |
| 16 | DR-NOAM VIP GUI: Copy configuration file to failed NOAM server | 1. Obtain a terminal session to the DR-NOAM VIP, login as the admusr user.
2. Configure the failed NOAM server:
   $ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<Failed_NOAM_Hostname>.sh admusr@<Failed_NOAM_xmi_IP_address>:/var/tmp/TKLCConfigData.sh |
### Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 17. | **Recovered NOAM Server:** Verify configuration was called and reboot the server.  
   - Establish an SSH session to the Recovered NOAM server (Recovered_NOAM_xmi_IP_address)  
   - Login as the `admusr` user.  
   - The automatic configuration daemon looks for the file named `TKLCCfgData.sh` in the `/var/tmp` directory, implements the configuration in the file, and asks the user to reboot the server.  
   - Verify `awpushcfg` was called by checking the following file:
     ```
     $ sudo cat /var/TKLC/appw/logs/Process/install.log
     Verify this message displays:
     [SUCCESS] script completed successfully!
     ```
   - Now reboot the server:
     ```
     $ sudo init 6
     ```
   - Wait for the server to reboot. |
| 18. | **Recovered NOAM Server:** Configure networking for dedicated NetBackup interface (Optional)  
   - Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.  
     ```
     $ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP_Address> --netmask=<NO2_NetBackup_NetMask>
     ```
     ```
     $ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NO1_NetBackup_Network_ID> --netmask=<NO2_NetBackup_NetMask> --gateway=<NO2_NetBackup_Gateway_IP_Address>
     ```
| 19. | **Recovered NOAM Server:** Verify server health  
   - Execute this command on the failed NOAM server and make sure no errors are returned:
     ```
     $ sudo syscheck
     Running modules in class hardware...OK
     Running modules in class disk...OK
     Running modules in class net...OK
     Running modules in class system...OK
     Running modules in class proc...OK
     LOG LOCATION: /var/TKLC/log/syscheck/fail_log
     ```
| 20. | Repeat for additional 2nd failed NOAM  
   - Repeat steps 15-19 for the 2nd failed NOAM server. |
## Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
</table>
| 21 | Perform keyexchange between active NOAM and recovered NOAM servers:  
1. From a terminal window connection on the active NOAM as the `admusr` user, exchange SSH keys for `admusr` between the active NOAM and the recovered NOAM servers using the keyexchange utility, using the host names of the recovered NOAMs.  
2. When prompted for the password, enter the password for the `admusr` user of the recovered NOAM servers.  
   `$ keyexchange admusr@<Recovered_NOAM Hostname>` |
| 22 | NOAM VIP GUI: Set HA on the recovered NOAM servers  
1. Navigate to **Status & Manage** > **HA**.  
   ![Status & Manage Tree](image)  
   Set **HA Role** to **Active**  
2. Click **Edit**.  
3. For each NOAM server whose Max Allowed HA Role is set to **Standby**, set it to **Active**.  
   ![Status & Manage Tree](image)  
4. Click **OK**. |
| 23 | NOAM VIP GUI: Restart DSR application  
1. Navigate to **Status & Manage** > **Server**.  
   ![Status & Manage Tree](image)  
   Select each recovered NOAM server and click **Restart**. |
## Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th>No.</th>
<th>Task Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.</td>
<td><strong>Recovered NOAM Servers: Activate optional features</strong></td>
<td>Map-Diameter Interworking (MAP-IWF) and/or Policy and Charging Application (PCA) Only&lt;br&gt;Activate the features Map-Diameter Interworking (MAP-IWF) and Policy and Charging Application (PCA) as follows:&lt;br&gt;&lt;br&gt;<strong>For PCA:</strong>&lt;br&gt;Establish SSH sessions to the all the recovered NOAM servers and login as admusr. Refer [13] and execute PCA Activation on Standby NOAM Server on all recovered NOAM servers to re-activate PCA.&lt;br&gt;&lt;br&gt;<strong>For MAP-IWF:</strong>&lt;br&gt;Establish SSH session to the recovered active NOAM, login as admusr. Refer to [7] to activate Map-Diameter Interworking (MAP-IWF).&lt;br&gt;&lt;br&gt;<strong>Note:</strong> While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored:&lt;br&gt;iload#31000{S/W Fault}&lt;br&gt;&lt;br&gt;<strong>Note:</strong> If any of the MPs are failed and recovered, then restart these MP servers after activation of the feature.</td>
</tr>
</tbody>
</table>
| 25. | **DR-NOAM VIP: Copy key file to recovered NOAM 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.<br>1. Establish an SSH session to any of the active DR NOAM that is intact and operational. Login as admusr.<br>2. Check if existing key file on active DR NOAM server is valid:<br>$ cd /usr/TKLC/dpi/bin/<br>$ ./sharedKrevo-validate<br><br>**Note:** If errors are present, stop and contact My Oracle Support (MOS).<br>3. If key file is valid, copy key file from the active DR NOAM server to recovered NOAMs:<br>$./sharedKrevo -copyKey -destServer <First NOAM>  
$./sharedKrevo -copyKey -destServer <Second NOAM> |
| 26. | **Switch DR NOAM back to secondary** | Once the system have been recovered, refer to DSR/SDS 8.x NOAM Failover User's Guide [17]. |
| 27. | **Recovered Servers: Verify alarms** | 1. Navigate to Alarms & Events > View Active.<br>a. Alarms & Events<br>b. View Active<br>c. View History<br>d. View Trap Log<br><br>2. Verify the recovered servers are not contributing to any active alarms (Replication, Topology misconfiguration, database impairments, NTP, etc.) |
# Procedure 5.  Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM VIP GUI: Recover standby/spare SOAM and C-level servers</th>
<th>NOAM VIP: Verify all servers in topology are accessible (RADIUS Only)</th>
<th>NOAM VIP: Copy key file to all the servers in topology (RADIUS Only)</th>
<th>Recover IDIH</th>
</tr>
</thead>
</table>
| 28   | If necessary, refer to Procedure 3 to recover any standby or Spare SOAMs as well as any C-level servers. | 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. Login as admusr. 2. Check if all the servers in the Topology are accessible:  
   ```
   $ cd /usr/TKLC/dpi/bin/
   $ ./sharedKrevo -checkAccess
   ```  
   **Note:** If any of the servers are not accessible, stop and My Oracle Support (MOS). | 1. Establish an SSH session to the active NOAM, login as admusr. 2. Copy the key file to all the servers in the Topology:  
   ```
   $ ./sharedKrevo -synchronize
   $ ./sharedKrevo -updateData
   ```  
   **Note:** If errors are present, stop and contact My Oracle Support (MOS). | If IDIH was affected, refer to IDIH Disaster Recovery section to perform disaster recovery on IDIH. |

## 4.6  Recovery Scenario 6 (Database Recovery)

### 4.6.1  Recovery Scenario 6: Case 1

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

**Note:** During recovery, the corrupted database is replaced by the server runtime backup. Any configuration done after taking the backup is not available post recovery.
Procedure 6. Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></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)

This procedure performs recovery if database is corrupted in the system. Check off (\(\checkmark\)) 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.
**Procedure 6. Recovery Scenario 6 (Case 1)**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>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><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 <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Modifying HA attributes" /></td>
</tr>
<tr>
<td></td>
<td><strong>Hostname</strong></td>
</tr>
<tr>
<td></td>
<td>ZombieNOAM1</td>
</tr>
<tr>
<td></td>
<td>ZombieNOAM2</td>
</tr>
<tr>
<td></td>
<td>ZombieDRNOAM1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Set the Max Allowed HA Role option to <strong>OOS</strong> for the failed servers.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Ok Cancel" /></td>
</tr>
<tr>
<td>3.</td>
<td>Server in <strong>Question</strong>: Login</td>
</tr>
<tr>
<td></td>
<td>Establish an SSH session to the server in question. <strong>Login as admusr</strong>.</td>
</tr>
<tr>
<td>4.</td>
<td>Server in <strong>Question</strong>: Change runlevel to 3</td>
</tr>
<tr>
<td></td>
<td>Bring the system to runlevel 3.</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo init 3</code></td>
</tr>
<tr>
<td>5.</td>
<td>Server in <strong>Question</strong>: Recover system</td>
</tr>
<tr>
<td></td>
<td>Execute this command and follow the instructions appearing in the console prompt.</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo /usr/TKLC/appworks/sbin/backout_restore</code></td>
</tr>
<tr>
<td>6.</td>
<td>Server in <strong>Question</strong>: Change runlevel to 4</td>
</tr>
<tr>
<td></td>
<td>Bring the system back to runlevel 4.</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo init 6</code></td>
</tr>
</tbody>
</table>
Procedure 6. Recovery Scenario 6 (Case 1)

7. **Server in Question:** Verify the server
   Verify if the processes are up and running.
   
   $ sudo pm.getprocs

   Example output:
   ![Example output image]

8. **NOAM VIP GUI:** Set failed servers to active

   1. Navigate to **Status & Manage > HA**.
      ![Status & Manage menu]
      
      2. Click **Edit**.
      
      3. Select the failed server and set it to **Active**.
      
      4. Click **OK**.
## Procedure 6. Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP: Verify all servers in topology are accessible (RADIUS only)</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td>1. Establish an SSH session to the NOAM VIP and login as admusr.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Check if all the servers in the Topology are accessible:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$ cd /usr/TKLC/dpi/bin/</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$ ./sharedKrevo -checkAccess</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[admusr@NOAM-2 bin]$ ./sharedKrevo -checkAccess</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FIPS integrity verification test failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1450729797: [INFO] 'NOAM-1' is accessible.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FIPS integrity verification test failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1450729797: [INFO] 'NOAM-1' is accessible.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FIPS integrity verification test failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1450729797: [INFO] 'NOAM-1' is accessible.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FIPS integrity verification test failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1450729797: [INFO] 'NOAM-2' is accessible.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FIPS integrity verification test failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1450729798: [INFO] 'IPFK' is accessible.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FIPS integrity verification test failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1450729798: [INFO] 'IPFK' is accessible.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FIPS integrity verification test failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1450729798: [INFO] 'IPFK' is accessible.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FIPS integrity verification test failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1450729798: [INFO] 'IPFK' is accessible.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[admusr@NOAM-2 bin]$</td>
<td></td>
</tr>
</tbody>
</table>
## Procedure 6.  Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 10.  | **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
   
   [Output of command showing integrity verification test failed.]
   ```  
   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
   
   [Output of command showing integrity verification test failed.]
   ```  
   ```
   $ ./sharedKrevo -updateData
   
   [Output of command showing data updated on servers.]
   ```  
   **Note:** If any errors are present, stop and contact My Oracle Support (MOS). |

| 11.  | Backup and archive all the databases from the recovered system | Execute DSR Database Backup to back up the Configuration databases. |
### 4.6.2 Recovery Scenario 6: Case 2

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

#### Procedure 7. Recovery Scenario 6 (Case 2)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:</td>
</tr>
<tr>
<td></td>
<td>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</td>
</tr>
<tr>
<td>2.</td>
<td>Login as the guiadmin user:</td>
</tr>
</tbody>
</table>

---

[Oracle System Login]

```plaintext
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.
Procedure 7. Recovery Scenario 6 (Case 2)

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

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

   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>OOS</td>
<td>The maximum des</td>
</tr>
<tr>
<td>ZombieDRNOAM2</td>
<td>Active 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.**

   ![Image of HA attributes](image)

3. **Server in Question:** Login

   Establish an SSH session to the server in question. Login as **admusr.**

4. **Server in Question:** Stop httpd service

   Stop the httpd service.

   ```bash
   $ sudo bash -l
   $ service httpd stop
   ```

5. **Server in Question:** Take server out of service

   Take the server out of service.

   ```bash
   $ prod.clobber
   ```

6. **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)

### 7. **Server in Question:** Start httpd service

1. Start the httpd service.
   
   ```
   $ service httpd start
   ```

2. Exit out of root.
   
   ```
   $ exit
   ```

### 8. **NOAM VIP GUI:** Set failed servers to active

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

   ![Status & Manage HA diagram]

   2. Click **Edit** at the bottom of the screen.

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

   ![Modifying HA attributes]

   4. Click **OK**.

### 9. **NOAM VIP GUI:** Restart DSR application

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

   ![Status & Manage Server diagram]

   2. Select each recovered server and click **Restart**.

   ![Restart button]
## Procedure 7. Recovery Scenario 6 (Case 2)

### 10. **Server in Question: Verify the server state**

1. **Verify the processes are up and running:**
   
   ```
   $ sudo pm.getprocs
   ```
   
   **Example output:**
   ```
   A 3472 ohm  Up 12/21 13:16:25 1 cma
   A 5140 emplatalarm  Up 12/21 13:16:25 1 emplatalarm
   A 5143 cmserver  Up 12/21 13:16:25 1 cmserver -R 1.3.6.1.4.1.3
   A 5145 cmaop  Up 12/21 13:16:25 1 cmop
   A 9668 eclipseHelp  Up 12/21 13:16:29 1 eclipseHelp
   A 9146 idsrv  Up 12/21 13:16:25 1 idsrv -M10 -M204 -D40 -D82
   A 9146 idsmemlock  Up 12/21 13:16:26 1 idsmemlock -f
   A 9146 inetmerge  Up 12/21 13:16:25 1 inetmerge
   A 9146 irep  Up 12/21 13:16:25 1 irep
   A 9146 campagent  Up 12/21 13:16:25 1 campagent
   A 9146 pm.server  Up 12/21 13:16:25 1 pm.server
   A 9146 rscler  Up 12/21 13:16:25 1 rscler -r 6000
   A 9176 re-portmap  Up 12/21 13:16:25 1 re-portmap -c100
   A 9176 statclerk  Up 12/21 13:16:25 1 statclerk -a -0
   A 9176 vipper  Up 12/21 13:16:25 1 vipper
   A -1 astateinit  Done 12/21 13:16:36 1 astateinit
   A -1 auditTask  Done 12/21 13:16:36 1 auditTask
   A -1 auditTasks  Done 12/21 13:16:36 1 auditTasks
   A -1 guiexport  Done 12/21 13:16:25 1 guiexport
   A -1 mkrbook  Done 12/21 13:16:25 1 mkrbook
   [root@RWP-1 admusr]#
   ```

2. **Verify if replication channels are up and running:**
   
   ```
   $ sudo irepstat
   ```
   
   **Example output:**
   ```
   -- Policy 0 Antfstb [DbReplication] -------------------------------------------
   BC From SOAM-2 Active 0.50 *0.04%cpu 34B/s A-C2713.145
   CC From MP-2 Active 0.20 *0.01%cpu 53B/s A-C2713.145
   -- Policy 1001 DSR_SSLDB_Policy [] ------------------------------------------
   1 CC From MP-2 Active 0.20 *0.06%cpu 35B/s A-C2713.145
   ```

3. **Verify if merging channels are up and running:**
   
   ```
   $ sudo inetmstat
   ```
   
   **Example output:**
   ```
   nodeId InetMerge State dir dSeq dTime updTime info
   SOAM-1 Standby To 0 0.00 13:19:33
   SOAM-2 Active To 0 0.00 13:19:33
   ```

### 11. **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
   ```
Procedure 7. Recovery Scenario 6 (Case 2)

12. **NOAM VIP:** Copy key file to all the servers in topology (RADIUS Only)

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

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

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

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

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

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

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

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

    Execute DSR Database Backup to back up the Configuration databases.
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>Description</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 affected before the restoration and notify them that you will reset their password during this maintenance operation.</td>
</tr>
<tr>
<td>2.</td>
<td>After Restoration: Log into the NOAM VIP</td>
</tr>
<tr>
<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>
</tr>
<tr>
<td></td>
<td>2. Login as the guiadmin user:</td>
</tr>
<tr>
<td></td>
<td><strong>Oracle System Login</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Log In</strong></td>
</tr>
<tr>
<td></td>
<td>Enter your username and password to log in</td>
</tr>
<tr>
<td></td>
<td>Username: [ ]</td>
</tr>
<tr>
<td></td>
<td>Password: [ ]</td>
</tr>
<tr>
<td></td>
<td>[ ] Change password</td>
</tr>
<tr>
<td></td>
<td>Log In</td>
</tr>
</tbody>
</table>

If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.
Procedure 8. Keep Restored User

3. After Restoration: Reset user passwords

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to Administration &gt; Access Control &gt; Users.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the user.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>Change Password</strong>.</td>
</tr>
<tr>
<td>4.</td>
<td>Type a new password.</td>
</tr>
<tr>
<td>5.</td>
<td>Click <strong>Continue</strong>.</td>
</tr>
</tbody>
</table>

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

**Procedure 9. Remove the Restored User**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>After Restoration: Log into the NOAM VIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Perform this procedure to remove users restored by system restoration. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td>
</tr>
<tr>
<td>1.</td>
<td>Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:</td>
</tr>
<tr>
<td></td>
<td><code>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</code></td>
</tr>
<tr>
<td>2.</td>
<td>Login as the <code>guiadmin</code> 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 9. Remove the Restored User

2. **After Restoration:** Reset user passwords

<table>
<thead>
<tr>
<th>1. Navigate to Administration &gt; Access Control &gt; Users.</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Navigation Menu" /></td>
</tr>
<tr>
<td><img src="image" alt="Delete Action" /></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

Perform this procedure to remove users restored by system restoration. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Before Restoration: Notify affected users before restoration</th>
<th>Before Restoration: Log into the NOAM VIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.</td>
<td>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://&lt;Primary_NOAM_VIP_IP_Address&gt;</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>

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

3. Before Restoration: Record user settings

<table>
<thead>
<tr>
<th>1. Navigate to Administration &gt; Access Control &gt; Users.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Under each affected user, record the following:</td>
</tr>
<tr>
<td>• Username</td>
</tr>
<tr>
<td>• Account status</td>
</tr>
<tr>
<td>• Remote Auth</td>
</tr>
<tr>
<td>• Local Auth</td>
</tr>
<tr>
<td>• Concurrent Logins Allowed</td>
</tr>
<tr>
<td>• Inactivity Limit</td>
</tr>
<tr>
<td>• Comment</td>
</tr>
<tr>
<td>• Groups</td>
</tr>
</tbody>
</table>
Procedure 10. Restore an Archive That Does Not Contain a Current User

4. After Restoration: Login

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

   http://<Primary_NOAM_VIP_IP_Address>

2. Login as the guiadmin user:

   [Image of Oracle System Login]

   Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 5.0, 10.0, or 11.0 with support for JavaScript and cookies.

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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>After restoration: recreate affected user</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to Administration &gt; Access Control &gt; Users.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Click Insert.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Recreate the user using the data collected from step 3.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Click OK.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>After Restoration: Repeat for additional users</td>
</tr>
<tr>
<td></td>
<td>Repeat step 5 to recreate additional users.</td>
</tr>
</tbody>
</table>
Procedure 10. Restore an Archive That Does Not Contain a Current User

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.

   **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, refer to fresh installation section to re-create it.

Procedure 11. IDIH Disaster Recovery Preparation

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This procedure performs disaster recovery preparation steps for the IDIH. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td>
</tr>
</tbody>
</table>

1. **PMAC GUI:**
   - Login

   1. Open web browser and enter:
      ```
      http://<PMAC_Mgmt_Network_IP>
      ```
   2. Login as `pmacadmin` user:
## Procedure 11. IDIH Disaster Recovery Preparation

<table>
<thead>
<tr>
<th></th>
<th>PMAC GUI: Verify necessary IDIH images are available</th>
<th>1. Navigate to <strong>Software &gt; Manage Software Images.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>[Software] [Software Inventory] [Manage Software Images]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Verify the current IDIH TVOE, TPD, Oracle, Application and Mediation images are listed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> If the necessary software images are not available, follow the instructions from the <strong>Load Application and TPD ISO onto PMAC Server</strong> procedure and steps 1-4 of <strong>IDIH Configuration</strong> from [8] to acquire and transfer the images.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Oracle Guest: Establish an SSH session to the Oracle guest, login as admusr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Oracle Guest: Login</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Oracle Guest: Perform database health check</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Perform database health check:</td>
</tr>
</tbody>
</table>

```
$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i
```

**Example output:**

```
[admusr@thunderbolt-ora ]$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i
10:10:52: STARTING HEALTHCHECK PROCEDURE
10:10:52: date: 05-12-15, hostname: thunderbolt-ora
10:10:52: TPD VERSION: 7.0.1.0.0-86.20.0
10:10:52: 
10:10:52: Checking disk free space
10:10:52: No disk space issues found
10:10:52: Checking syscheck - this can take a while
10:10:58: No errors in syncheck modules
10:11:00: Checking Alert Manager alarmStatus
10:11:00: No alarms found
10:11:00: Checking statefiles
10:11:00: Statefiles do not exist
10:11:00: Checking runlevel
10:11:00: Runlevel is OK (N 4)
10:11:00: Checking upgrade log
10:11:00: Install logs are free of errors
10:11:00: Analyzing date
10:11:00: NTP daemon is running
10:11:00: Server is synchronized with ntp server
10:11:00: Checking NTP status
10:11:00: twc-host is integrated
10:11:00: Ntp settings is OK
10:11:00: Checking server entries in host file.
10:11:00: oracle is present in /etc/hosts
10:11:00: mediation is present in /etc/hosts
10:11:00: appserver is present in /etc/hosts
10:11:00: Ping server entries in host file.
10:11:00: Ping server oracle
10:11:00: Ping server mediation
10:11:00: Ping server appserver
10:11:00: Check oracle server
10:11:00: Oracle server and resources online
10:11:01: All tests passed!
10:11:01: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
[admusr@thunderbolt-ora ]$ 
```
### 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>PMAC GUI: Login</th>
<th>Remove existing application server</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>1. Open web browser and enter: <code>http://&lt;PMAC_Mgmt_Network_IP&gt;</code></td>
<td>1. Navigate to <strong>Main Menu &gt; VM Management</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Login as <code>pmacadmin</code> user:</td>
<td>2. Select the application guest.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Oracle System Login" /></td>
<td>3. Click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

- [ ] PMAC GUI: Login
- [ ] Remove existing application server

---

**Log In**
Enter your username and password to log in

- **Username:** [ ]
- **Password:** [ ]
- [ ] Change password

Log in

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Remove existing mediation server</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Main Menu &gt; VM Management</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Delete</strong>.</td>
</tr>
<tr>
<td></td>
<td>PMAC: Establish SSH session and login</td>
</tr>
<tr>
<td>4.</td>
<td>Establish an SSH session to the PMAC, login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td>5.</td>
<td>PMAC: Re-install the mediation and application servers</td>
</tr>
<tr>
<td></td>
<td>Execute this command (Enter your upgrade file):</td>
</tr>
</tbody>
</table>
|      | ```
|      | $ cd /var/TKLC/smac/guest-dropin
|      | $ screen
|      | $ sudo fdconfig config --file=<hostname-upgrade_xx-xx-xx>.xml
|      | **!!Warning!!** |
|      | If you run the fdconfig without **upgrade** in the XML filename, the database is destroyed and you lose all of the existing data. |
|      | **Note:** 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>6.</th>
<th>PMAC GUI: Monitor the configuration</th>
</tr>
</thead>
</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:~/KLL/smacc/guest-dropin]$ sudo fdconfig config --file=d-ray_04-21-15.xml
runConfig
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_20150511093944_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>
<th>1. Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server. Open the web browser and enter a URL of:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Login</td>
<td><a href="http://%3CPrimary_NOAM/SOAM_VIP_IP_Address%3E">http://&lt;Primary_NOAM/SOAM_VIP_IP_Address&gt;</a></td>
</tr>
</tbody>
</table>
| 2.     | guiadmin            | Login as the guiadmin user:  

![Oracle System Login](image)

Username: 
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.
Procedure 13. DSR Database Backup

1. Navigate to Status & Manage > Database.

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

2. Select the active NOAM server and click Backup.

3. Make sure that the Configuration checkbox is marked.

   **Database Backup**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server: ZombieNOAM1</td>
<td></td>
</tr>
</tbody>
</table>

   Select data for backup
   - Provisioning
   - Configuration

   Compression *
   - gzip
   - bzip2
   - none

   Archive Name *
   - Backup.dsr.ZombieNOAM1.Configuration.NETV

   Comment

   [Ok] [Cancel]

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Take a secured backup of key file (RADIUS only)</td>
</tr>
</tbody>
</table>

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

1. Log into ssh shell of active NOAM server as admusr.
2. Take a secure backup of updated key file RADIUS shared secret encryption key for disaster scenarios.
3. Encrypt the key file before backing up to secure customer setup:
   
   ```bash
   $ ./sharedKrevo -encr
   ```
4. Copy the encrypted key file to secure customer setup:
   
   ```bash
   $ sudo scp /var/TKLC/db/filemgmt/DpiKf.bin.encr user@<customer IP>:<path of customer setup>
   ```

**Note:** The operator must strictly control access to the backed up key file. If the operator needs to encrypt this key file further using operator specified encryption techniques, the operator is recommended to do so; however, the operator is responsible to decrypt this file using operator-specific decryption techniques and copy the resulting DpiKf.bin.encr file securely to the file management folder if the key file needs to be restored for disaster recovery. Once the key file is backed up to the operator-provided server and path, it is the responsibility of the operator to ensure access to the backed up key file is extremely selective and restricted.
Appendix B. Recover/Replace Failed 3rd Party Components (Switches, OAs)

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

Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F)

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

Prerequisites for this procedure are:
- A copy of the networking xml configuration files
- A copy of HP Misc Firmware DVD or ISO
- IP address and hostname of the failed switch
- Rack mount position of the failed switch

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

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

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`

   **Example output:**

   `/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso`  
   `1118514 1118514 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64`  
   `/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso`  
   `1118372 1118372 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64`  
   `/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso`
Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F)

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

   
   | cd /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64/upgrade/overlay/ |

   
   **Example:**
   
   cd /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64/upgrade/overlay/  

6. **Locate the DSR_NetConfig_Templates.zip file.**

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

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

   **Example:**
   
   $ unzip DSR_NetConfig_Templates.zip

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

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

   **Example:**
   
   $ cp <switch_xml_file> /usr/TKLC/smac/etc/switch/xml/
**Procedure 15. Recover a Failed Enclosure Switch (Cisco 3020)**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Recover Failed Enclosure Switch: Cisco 3020</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log into the PMAC using SSH as admusr.</td>
</tr>
<tr>
<td></td>
<td>Remove the old SSH key of the switch from the PMAC by executing this command from a PMAC command shell:</td>
</tr>
<tr>
<td></td>
<td><code>sudo ssh-keygen -R &lt;enclosure_switch_ip&gt;</code></td>
</tr>
<tr>
<td>2.</td>
<td>Refer to procedure Replace a failed 3020 switch (netConfig) to replace the failed enclosure switch from reference [2].</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>You need a copy of the HP Misc Firmware DVD or ISO and of the original networking xml files custom for this installation. These either be stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.</td>
</tr>
</tbody>
</table>

**Procedure 16. Recover a Failed Enclosure Switch (HP 6120XG , HP 6125XLG, HP 6125G)**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Recover Failed Enclosure Switch: HP 6120XG/6125XLG/6125G</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log into the PMAC using SSH as admusr.</td>
</tr>
<tr>
<td></td>
<td>Remove the old SSH key of the switch from the PMAC by executing this command from a PMAC command shell:</td>
</tr>
<tr>
<td></td>
<td><code>sudo ssh-keygen -R &lt;enclosure_switch_ip&gt;</code></td>
</tr>
<tr>
<td>2.</td>
<td>Refer to procedure Replace a failed HP 6120XG, 6125G, 6125XLG switch (netConfig) to replace the failed enclosure switch from reference [2].</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>You need a copy of the HP Misc Firmware DVD or ISO and of the original networking xml files custom for this installation. These either be stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Copy switch appropriate init file and use it for respective switch:</td>
</tr>
<tr>
<td>3.</td>
<td>Older platform init files may not work on platform 7.2 systems. Copy the</td>
</tr>
</tbody>
</table>
Procedure 16. Recover a Failed Enclosure Switch (HP 6120XG, HP 6125XLG, HP 6125G)

5. The templates can be found by the following method:

From the PMAC CLI:

```
df | grep -I DSR
```

Example output:

```
/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso
1118514 1118514 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64
/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso
1118372 1118372 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64
/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso
1117976 1117976 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64
```

6. 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-8.2.0.0.0_82.4.0-x86_64/upgrade/overlay/
```

7. Locate the DSR_NetConfig_Templates.zip file.

Example:

```
$ ll
```

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

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

Example:

```
$ unzip DSR_NetConfig_Templates.zip
```

9. Edit the desired file with site specific details. The existing file from original

```
**Procedure 16. Recover a Failed Enclosure Switch (HP 6120XG, HP 6125XLG, HP 6125G)**

<table>
<thead>
<tr>
<th>Deployment /usr/TKLC/smac/etc/switch/xml can be used as a reference.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10. Copy the new init file to the /usr/TKLC/smac/etc/switch/xml dir.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>$ cp &lt;switch_xml_file&gt; /usr/TKLC/smac/etc/switch/xml/</td>
</tr>
<tr>
<td><strong>Note:</strong> While restoring 6120XG switch, some features enabled on a 6120XG may not restore properly if they reference a port channel that does not currently exist on the switch ahead of the restore operation. Identify any port channels that need to be created on the switch according to the backup file and create them before restoring the configuration:</td>
</tr>
<tr>
<td>$ sudo /bin/cat &lt;switch_hostname&gt;-backup</td>
</tr>
<tr>
<td><strong>Example output:</strong></td>
</tr>
<tr>
<td>trunk &lt;int list&gt; Trk&lt;id&gt; LACP</td>
</tr>
<tr>
<td>trunk &lt;int list&gt; Trk&lt;id&gt; Trunk</td>
</tr>
<tr>
<td>11. If any port-channels are found, then for each portchannel identified by the above command, use the <code>netConfig setLinkAggregation</code> command to create it and the <code>netConfig showConfiguration</code> command to verify its configuration:</td>
</tr>
<tr>
<td>12. If an LACP port channel was found, add the port-channel with this command:</td>
</tr>
<tr>
<td>$ sudo /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY2 setLinkAggregation id=&lt;id&gt; addPort=tenGE&lt;int list&gt; mode=active</td>
</tr>
<tr>
<td>13. If a Trunk port-channel was found (as labeled after the Trk&lt;id&gt;), add the port-channel with this command:</td>
</tr>
<tr>
<td>$ sudo /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY2 setLinkAggregation id=&lt;id&gt; addPort=tenGE&lt;int list&gt; mode=static</td>
</tr>
<tr>
<td>14. Verify the port-channels were added to the running configuration:</td>
</tr>
<tr>
<td>$ sudo /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY2 showConfiguration</td>
</tr>
<tr>
<td>trunk &lt;int list&gt; Trk&lt;id&gt; LACP</td>
</tr>
<tr>
<td>trunk &lt;int list&gt; Trk&lt;id&gt; Trunk</td>
</tr>
<tr>
<td>15. For all switch types and configurations found, use netConfig to restore the configuration:</td>
</tr>
<tr>
<td>$ sudo /usr/TKLC/plat/bin/netConfig --device=&lt;switch_hostname&gt; restoreConfiguration service=ssh_service filename=&lt;switch_hostname&gt;-backup</td>
</tr>
<tr>
<td><strong>Note:</strong> This causes the switch to reboot. It takes approximately 120-180 seconds before connectivity is restored.</td>
</tr>
</tbody>
</table>
Procedure 17. Recover a Failed Enclosure OA

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Recover failed enclosure OA</td>
</tr>
</tbody>
</table>

Refer to procedure **Restore OA Configuration from Management Server** to replace a failed enclosure OA from reference [2].

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Active NOAM: login</td>
</tr>
</tbody>
</table>

Log into the active NOAM server using SSH as admusr.

| 1.     | 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.
Procedure 18. Inhibit A and B Level Replication on C-level Servers

<table>
<thead>
<tr>
<th></th>
<th>Active NOAM: Verify replication has been Inhibited</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled. Verify replication inhibition on MPs by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site, for example, Site SO_HPC03 is set as A B.</td>
</tr>
</tbody>
</table>

```
$ 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</td>
<td>A B</td>
<td>SO_HPC03</td>
</tr>
<tr>
<td>C2254.233</td>
<td>MP1</td>
<td>MP1</td>
<td>Active</td>
<td>A B</td>
<td>SO_HPC03</td>
</tr>
</tbody>
</table>
```

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

Procedure 19. Un-Inhibit A and B Level Replication on C-level Servers

<table>
<thead>
<tr>
<th></th>
<th>Un-Inhibit A and B Level Replication on C-level Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This procedure un-inhibits A and B level replication on all C-level servers of this site</td>
</tr>
<tr>
<td></td>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
</tr>
<tr>
<td></td>
<td>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Active NOAM:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Un-Inhibit replication on all C-level servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Execute this command:</td>
</tr>
</tbody>
</table>

```
$ 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.
Procedure 19. Un-Inhibit A and B Level Replication on C-level Servers

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Active NOAM: Verify replication has been Inhibited</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</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. The InhibitRepPlans field for all the MP servers for the selected site, for example, Site SO_HPC03 is set as A B.</td>
</tr>
</tbody>
</table>

```bash
$ sudo igt NodeInfo
```

Example output:
```
nodeId  nodeName  hostName  nodeCapability  inhibitRepPlans  siteId
excludeTables
A1386.099  NO1  NO1  Active                      NO_HPC03
B1754.109  SO1  SO1  Active                      SO_HPC03
C2254.131  MP2  MP2  Active  A B                  SO_HPC03
C2254.233  MP1  MP1  Active  A B                  SO_HPC03
```

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

Procedure 20. Inhibit A and B Level Replication on C-level Servers

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Active NOAM: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log into the active NOAM server using SSH as admusr.</td>
</tr>
</tbody>
</table>

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.
Procedure 20. Inhibit A and B Level Replication on C-level Servers

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Active NOAM: Inhibit replication on all C-level servers</td>
</tr>
<tr>
<td></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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Active NOAM: Verify replication has been inhibited</td>
</tr>
<tr>
<td></td>
<td>After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled. Verify replication inhibition on MPs by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO_SG is set as A B. Execute this command:</td>
</tr>
<tr>
<td></td>
<td>$ iqt NodeInfo</td>
</tr>
</tbody>
</table>

**Example output:**

```
nodeId  nodeName  hostName nodeCapability inhibitRepPlans  siteId excludeTables
A1386.099  NO1      NO1       Active                        NO_HPC03
B1754.109  SO1      SO1       Active                        SO_HPC03
C2254.131  MP2      MP2       Active  A B  SO_HPC03
C2254.233  MF1      MF1       Active  A B  SO_HPC03
```
**Appendix F. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost)**

**Procedure 21. Un-Inhibit A and B Level Replication on C-Level Servers**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
<th>Command Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Active NOAM: Login</td>
<td>Log into the active NOAM server using SSH as admusr.</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. 
/usr/TKLC/dsr/tools/InhibitReplication.sh --replication=allow --SO_SG_Name=<SOAM server group name> 
Alternatively to the above script, if the script is not in the specific path: 

```bash
```

**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 21. Un-Inhibit A and B Level Replication on C-Level Servers

3. Active NOAM: Verify replication has been Inhibited
   After executing above steps to un-inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.
   Verify replication inhibition on MPs by analyzing NodelInfo output.
   InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO_SG is set as A B.
   Execute this command:
   $ sudo iqt NodeInfo
   
   Example output:
   
<table>
<thead>
<tr>
<th>nodeId</th>
<th>nodeName</th>
<th>hostName</th>
<th>nodeCapability</th>
<th>inhibitRepPlans</th>
<th>siteId</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1386.099</td>
<td>NO1</td>
<td>NO1</td>
<td>Active</td>
<td>NO_HPC03</td>
<td></td>
</tr>
<tr>
<td>B1754.109</td>
<td>SO1</td>
<td>SO1</td>
<td>Active</td>
<td>SO_HPC03</td>
<td></td>
</tr>
<tr>
<td>C2254.131</td>
<td>MP2</td>
<td>MP2</td>
<td>Active</td>
<td>A B</td>
<td>SO_HPC03</td>
</tr>
<tr>
<td>C2254.233</td>
<td>MP1</td>
<td>MP1</td>
<td>Active</td>
<td>A B</td>
<td>SO_HPC03</td>
</tr>
</tbody>
</table>

Appendix G. Restore TVOE Configuration from Backup Media

Procedure 22. Restore TVOE Configuration from Backup Media

1. Install TVOE application
   - If the PMAC is NOT hosted on the failed rack mount server, execute IPM Servers Using PMAC Application from reference [10].
   - If the PMAC is hosted on the failed rack mount server, execute Installing TVOE on the Management Server from reference [10].

2. Establish network connectivity
   - If the PMAC is NOT hosted on the failed rack mount server, skip this step.
   - If the PMAC is hosted on the failed rack mount server, execute TVOE Network Configuration, steps 1-11, from reference [10].
   
   Note: The IP address configured on the TVOE must be one accessible through the network of the machine currently holding the TVOE Backup ISO image. This could be a NetBackup master server, a customer PC, etc.

3. Restore TVOE backup ISO image to the TVOE host (NetBackup)
   - If using NetBackup to restore the TVOE backup ISO image, then execute this step; otherwise, skip this step.
     1. Execute Application NetBackup Client Installation Procedures from reference [8].
     2. Interface with the NetBackup master server and initiate a restore of the TVOE backup ISO image.
   
   Note: Once restored, the ISO image is in /var/TKLC/bkp/ on the TVOE server.
Procedure 22. Restore TVOE Configuration from Backup Media

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></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/
```
where `<path_to_image>` is the path to the backup ISO image on the local system and `<TVOE_IP>` is the TVOE IP address.

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

**IPv4 Example:**
```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 [10], the Using WinSCP procedure, to copy the backup image to the customer system.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>TVOE Server: Login</td>
<td>Establish an SSH session to the TVOE server and login as <code>admsur</code>.</td>
</tr>
</tbody>
</table>
## Procedure 22. Restore TVOE Configuration from Backup Media

<table>
<thead>
<tr>
<th>6.</th>
<th>Restore TVOE backup ISO image</th>
</tr>
</thead>
</table>
| 1. | Restore the TVOE backup ISO by executing this command:  
   ```bash  
   $ sudo su - -c 'platcfg'  
   ``` |
| 2. | Navigate to **Maintenance > Backup and Restore > Restore Platform > Select Backup Media**. |
| 3. | Select the desired archive. |
| 4. | Click **OK**. |
| 5. | Click **Restore Backup Archive**. |
| 6. | Confirm restore. |
## Procedure 22. Restore TVOE Configuration from Backup Media

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Wait for the restore to complete.</td>
</tr>
<tr>
<td>2.</td>
<td><strong>Exit</strong> platcfg.</td>
</tr>
</tbody>
</table>

### Note:
This typically takes less than 5 minutes.

---

**TVOE Server:**  
Exit the Restore Backup Menu.

```
lu Backup and Restore Menu tqq
x       x
x Backup Platform(CD/DVD)  x
x Backup Platform(USB)     a x
x Restore Platform         a x
x Restore USB Archive      x
x Exit                     x
x x
mgqmgqmgqmgqmgmgmqmgmgqmgqmgqmgmgmgmqmgmgmgmgmgmgmgmgm
```

---

**Monitor TVOE backup process**

```
1qqu Restore Backup Menu tqq
x       x
x Select Backup Media    x
x View Table of Contents a x
x Change Restore Dir     a x
x Restore Backup Archive x
x Exit                   x
x x
mgqmgqmgqmgqmgmgmqmgmgqmgqmgqmgmgmgmqmgmgmgmgmgmgmgmgm
```

---

1. Wait for the restore to complete.

```
Restoring... This may take a while.
```

```
Please wait...
```

```
Restore completed successfully!
```

```
Press any key to continue...
```
Procedure 22. Restore TVOE Configuration from Backup Media

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

10. **TVOE Server:**
    Wait for restart to successfully complete
**Procedure 22. Restore TVOE Configuration from Backup Media**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| 11   | **TVOE Server:** Verify storage pools are active | 1. Login as **admusr**.  
2. Verify all storage pools are listed and are in the active state:  
```bash  
sudo virsh -c "qemu:///system" pool-list  
[admusr@5c10441-TVOE ~]$ sudo virsh -c "qemu:///system" pool-list  
Name     State  Autostart  
---------------------------  
vsguests   active   yes  
[admusr@5c10441-TVOE ~]$  
```

**Note:** If any storage pools are missing or inactive, contact My Oracle Support (MOS).

| 12   | **TVOE Server:** Enable HIDS (Optional) | **Note:** Enabling HIDS is optional. This step is skipped if HIDS is not required to be enabled.  
When enabling HIDS, update the baseline so the restored files are not reported as being tampered with. Execute these commands from the TVOE host remote console to enable HIDS and update the baseline:  
```bash  
$ /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 22. Restore TVOE Configuration from Backup Media

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.</td>
<td><strong>TVOE Server:</strong> Verify alarms</td>
</tr>
</tbody>
</table>
|      | 1. Verify alarms:  
|      | `$ sudo su - platcfg`  
|      | 2. Click **Diagnostics**. |
|      | 3. Click **Alarm Manager**. |
|      | 4. Click **Show Alarm Status**. |

If there are any failures, contact My Oracle Support (MOS).
## Appendix H. Restore PMAC from Backup

### Procedure 23. 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.

1. **Deploy the PMAC guest**
   - Execute **Install PMAC** from reference [10].

2. **PMAC: Login**
   - Establish an SSH session to the PMAC server and login as *admusr*.

3. **Restore PMAC Backup image to the PMAC host**
   - From the remote backup location, copy the backup file to the deployed PMAC. There are too many possible backup scenarios to cover them all here. This example is a simple *scp* from a redundant PMAC backup location. If using IPv6 addresses, the command requires shell escapes, for example, *admusr@[<ipV6addr>]:/<file>*

   **Note:** Execute the *scp* command from the recovered PMAC and the backup file is pulled/retrieved from the backup location.

   ```bash
   $ sudo /usr/bin/scp -p \
   admusr@<remoteserver>:/var/TKLC/smac/backup/*.pef \
   /var/TKLC/smac/backup/
   
   **Note:** It is important to copy the correct backup file to use in the restore. The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PMAC before the restoration of the data.

4. **PMAC: Verify no Alarms are present**
   - Verify no alarms are present.

   ```bash
   $ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus
   
   **Note:** The result eventually displays PMAC Restore successful.

5. **Restore the PMAC Data from Backup**
   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
      
      **Note:** The result eventually displays PMAC Restore successful.
Procedure 23. Restore PMAC from Backup Media

6. **PMAC GUI: Login**
   1. Open web browser and navigate to the PMAC GUI.
   2. Login as **PMACadmin** user:
      
      ![PMAC GUI Login](https://<pmac_network_ip>)

   **Oracle System Login**

   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.

   Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.

7. **PMAC GUI: Verify restore task completed**
   1. Navigate to **Task Monitoring**.
      
      ![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 23. Restore PMAC from Backup Media

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 8.  | **PMAC GUI:** Verify system inventory  
   - Navigate to **Hardware > System Inventory.**  
   - Verify previously provisioned enclosures are present. |
| 9.  | **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:  
     <pre>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.</pre> |
| 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 24. Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
<th>Action/Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Deploy the PMAC guest</td>
<td>Execute Install PMAC from reference [10].</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This procedure is for restoring from a NetBackup server, so specify the appropriate options when deploying PMAC for use with NetBackup.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>PMAC TVOE Host: Login</td>
<td>Establish an SSH session to the PMAC TVOE Host, login as admusr.</td>
</tr>
<tr>
<td>3.</td>
<td>PMAC TVOE Host: Log into PMAC guest console</td>
<td>1. On the TVOE host, execute this command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$sudo virsh list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This produces a listing of currently running virtual machines.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Find the VM name for your PMAC and note its ID number in the first column.</td>
</tr>
<tr>
<td>4.</td>
<td>Connect to console of the VM using the VM number obtained in step 3</td>
<td>On the TVOE host, execute this command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$sudo virsh console &lt;PMAC-VMID&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Where PMAC-VMID is the VM ID you obtained in step 3:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[admusr@Oahu-TVOE-1 ~]$ sudo virsh list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Id   Name                             State</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1      Oahu-PMAC                  running</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You are now connected to the PMAC guest console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you wish to return to the TVOE host, you can exit the session by pressing CTRL + ].</td>
</tr>
</tbody>
</table>

Note: This procedure provides steps to restore the PMAC application configuration from backup server. Prerequisite: TVOE management server has been restored. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.
### Procedure 24. Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus.</td>
<td>Execute these commands on the PMAC.</td>
<td></td>
</tr>
</tbody>
</table>

```bash
$ sudo /sbin/service iptables stop
iptables: Flushing firewall rules: [OK ]
iptables: Setting chains to policy ACCEPT: filter [OK ]
$ sudo /usr/TKLC/smrac/etc/services/netbackup start
Modified menu NBConfig
--
show
Set the following menus: NBConfig to visible=1
Modified menu NBInit
--
show
Set the following menus: NBInit to visible=1
Modified menu NBDeInit
--
show
Set the following menus: NBDeInit to visible=1
Modified menu NBInstall
--
show
Set the following menus: NBInstall to visible=1
Modified menu NBVerifyEnv
--
show
Set the following menus: NBVerifyEnv to visible=1
Modified menu NBVerify
--
show
Set the following menus: NBVerify to visible=1=
```
### Procedure 24. Restore PMAC from Backup Server

| 6. | **PMAC:** Verify the TPD platcfg backup menus are visible, then exit the TPD platcfg Utility |
|    | Verify the TPD platcfg backup menus are visible. |
|    | `$ sudo /bin/su – platcfg` |
|    | ![TPD platcfg Utility Main Menu](image) |
|    | **Note:** In the example image above of the TPD platcfg utility Main Menu the backup menu is identified as **NetBackup Configuration**. |
| 7. | **PMAC:** Verify the iptables rules are disabled on the PMAC guest |
|    | Verify the iptables rules are disabled on the PMAC guest. |
|    | `$ sudo /sbin/iptables -nL` |
|    | `INPUT (policy ACCEPT)` |
|    | `target prot opt source destination` |
|    | `CHAIN FORWARD (policy ACCEPT)` |
|    | `target prot opt source destination` |
|    | `CHAIN OUTPUT (policy ACCEPT)` |
|    | `target prot opt source destination` |
| 8. | **PMAC:** Install backup utility client software on the PMAC guest |
|    | **Note:** The **Initialize PMAC Application** and **Configure PMAC Application** prerequisites can be ignored. |
| 9. | Backup server: verify appropriate PMAC backup exists |
|    | This step is likely executed by customer IT personnel. |
|    | 1. Log into the backup server as the appropriate user using the user password. |
|    | 2. Execute the appropriate commands to verify the PMAC backup exists for the desired date. |
|    | **Note:** The actions and commands required to verify the PMAC backups exist and the commands required to perform backup and restore on the backup server are the responsibility of the site customer. |
|    | **Note:** It is important to select the correct backup file to use in the restore. The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PMAC before the restoration of the data. |
### Procedure 24. Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</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.  
      | **Note:** The result eventually displays PMAC Restore successful. |
| 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 24. Restore PMAC from Backup Server**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.</td>
<td><strong>PMAC GUI: Login</strong>&lt;br&gt;1. Open web browser and navigate to the PMAC GUI.&lt;br&gt;2. Login as <strong>PMACadmin</strong> user:</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Oracle System Login" /></td>
</tr>
<tr>
<td></td>
<td>Note: After the restore is complete, you should see <strong>Add Enclosure</strong> tasks start for all previously provisioning servers. These should be allowed to complete before continuing.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>14.</td>
<td><strong>PMAC GUI: Verify restore task completed</strong>&lt;br&gt;1. Navigate to <strong>Task Monitoring</strong>.&lt;br&gt;2. Verify the restore background task completed successfully.</td>
</tr>
</tbody>
</table>
Procedure 24. Restore PMAC from Backup Server

15. **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.

16. **PMAC:** Verify PMAC

   - **Perform a system health check on the PMAC.**

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

17. **PMAC:** Add ISO images to the PMAC

   - Re-add any needed ISO images to the PMAC by executing procedure **Load Application and TPD ISO onto PMAC Server** from reference [8].
Appendix I. Configure TVOE Hosts

Procedure 25. Configure TVOE

This procedure configures networking on TVOE hosts.

**Prerequisite:** Server has been IPM'ed with TVOE OS as described in [10].

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>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Determine bridge names and interfaces for XMI and IMI, and NetBackup (if used) networks</td>
</tr>
<tr>
<td>1.</td>
<td>Determine the bridge names and physical bridge interfaces to be used on the TVOE server for the NOAM XMI and IMI networks.</td>
</tr>
<tr>
<td>2.</td>
<td>Based on the site survey, determine if you are using VLAN tagging or not, what bonds are used, and also the actual Ethernet interfaces that make up those bonds.</td>
</tr>
<tr>
<td>3.</td>
<td>If the NetBackup bridge and interface were not previously configured on this server when PMAC was installed, determine those values as well.</td>
</tr>
<tr>
<td>4.</td>
<td>Fill in the appropriate values in the table below:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NOAM Guest Interface Name</th>
<th>TVOE Bridge Name</th>
<th>TVOE Bridge Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>xmi</td>
<td>xmi</td>
<td><strong>Interface Bond</strong> (for example, bond0, bond1, etc.): [xmi_bridge] &lt;TVOE_XMI_Bridge_Interface_Bond&gt; <strong>Interface Name</strong> (for example, bond0.3, bond1, bond0.100): [xmi_bridge] &lt;TVOE_XMI_Bridge_Interface&gt;</td>
</tr>
<tr>
<td>imi</td>
<td>imi</td>
<td><strong>Interface Bond</strong>: (for example, bond0, bond1, etc.): [imi_bridge] &lt;TVOE_IMI_Bridge_Interface_Bond&gt; <strong>Interface Name</strong>: (for example, bond0.4, bond1, bond0.100): [imi_bridge] &lt;TVOE_IMI_Bridge_Interface&gt;</td>
</tr>
<tr>
<td>NetBackup</td>
<td>NetBackup</td>
<td><strong>Interface Name</strong> (for example, eth11, eth04, eth03, etc.): [NetBackup_bridge] &lt;TVOE_NetBackup_Bridge_Interface&gt;</td>
</tr>
<tr>
<td>management</td>
<td>management</td>
<td><strong>Interface Name</strong> (for example, bond0.2, bond0.37, etc.): [management_bridge] &lt;TVOE_Mgmt_Bridge_Interface&gt;</td>
</tr>
</tbody>
</table>

| 2. | RMS Server: Login |
| Log in to the TVOE prompt of the RMS server as **admusr** using the iLO facility. |
### Procedure 25. Configure TVOE

**3. RMS Server:** Configure XMI bridge interface bond

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Verify the XMI bridge interface bond.</td>
</tr>
<tr>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/netAdm query --device=TVOE_XMI_Bridge_Interface_Bond</td>
</tr>
<tr>
<td></td>
<td>Protocol: none</td>
</tr>
<tr>
<td></td>
<td>On Boot: yes</td>
</tr>
<tr>
<td></td>
<td>Persistent: yes</td>
</tr>
<tr>
<td></td>
<td>Bonded Mode: active-backup</td>
</tr>
<tr>
<td></td>
<td>Enslaving: eth01 eth02</td>
</tr>
</tbody>
</table>

If the bond has already been configured, output, similar to what you see above, displays. If this is so, skip to the next step; otherwise, continue with this step.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Create bonding interface and associate subordinate interfaces with bond:</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The output below is for illustrative purposes only. The example output shows the control bridge configured.</td>
</tr>
<tr>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/netAdm add --device=TVOE_XMI_Bridge_Interface_Bond --onboot=yes --type=Bonding --mode=active-backup --miimon=100</td>
</tr>
<tr>
<td></td>
<td>Interface &lt;TVOE_XMI_Bridge_Bond&gt; added</td>
</tr>
<tr>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/netAdm set --device=TVOE_XMI_Bridge_Bond_Ethernet1 --type=Ethernet --master=TVOE_XMI_Bridge_Interface_Bond --slave=yes --onboot=yes</td>
</tr>
<tr>
<td></td>
<td>Interface &lt;TVOE_XMI_Bridge_Bond_Ethernet1&gt; updated</td>
</tr>
<tr>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/netAdm set --device=TVOE_XMI_Bridge_Bond_Ethernet2 --type=Ethernet --master=TVOE_XMI_Bridge_Interface_Bond --slave=yes --onboot=yes</td>
</tr>
<tr>
<td></td>
<td>Interface &lt;TVOE_XMI_Bridge_Bond_Ethernet2&gt; updated</td>
</tr>
<tr>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES --val=&lt;TVOE_XMI_Bridge_Interface_Bond&gt;,[bondX,bondX+1,...,bondN]</td>
</tr>
</tbody>
</table>

**Note:** All other existing bonds should be included in the **val** statement, for example, if TVOE_XMI_Bridge_Bond = bond1, val=bond0,bond1.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$ sudo syscheckAdm net ipbond -enable</td>
</tr>
</tbody>
</table>
## Procedure 25. Configure TVOE

4. **RMS Server:**
   - Create XMI bridge interface, if needed. (Only for VLAN tagging interfaces)
   - If you are using VLAN tagging for the XMI bridge interface, then you must create the VLAN interface first.

   ```bash
   $ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_XMI_Bridge_Interface> --onboot=yes
   Interface <TVOE_XMI_Bridge_Interface> created.
   ```

5. **RMS Server:**
   - Create XMI bridge
   - Now, create the XMI bridge:

   ```bash
   $ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=xmi --onboot=yes
   --bridgeInterfaces=<TVOE_XMI_Bridge_Interface>
   Interface <TVOE_XMI_Bridge_Interface> updated.
   Bridge xmi created.
   ```
Procedure 25. Configure TVOE

1. Verify the IMI bridge interface bond.

```
$ sudo /usr/TKLC/plat/bin/netAdm query
   --device=<TVOE_IMI_Bridge_Interface_Bond>
Protocol: none
On Boot: yes
Persistent: yes
Bonded Mode: active-backup
Enslaving: eth01 eth02
```

**Note:** The output below is for illustrative purposes only. The example output shows the control bridge configured.

If the bond has already been configured, output, similar to what you see above, displays. If this is so, skip to the next step; otherwise, continue with this step.

2. Create bonding interface and associate subordinate interfaces with bond:

```
$ sudo /usr/TKLC/plat/bin/netAdm add
   --device=<TVOE_IMI_Bridge_Interface_Bond>
   --onboot=yes
   --type=Bonding
   --mode=active-backup
   --miimon=100

Interface <TVOE_IMI_Bridge_Bond> added

$ sudo /usr/TKLC/plat/bin/netAdm set
   --device=<TVOE_IMI_Bridge_Bond_Ethernet1>
   --type=Ethernet
   --master=<TVOE_IMI_Bridge_Bond>
   --slave=yes
   --onboot=yes

Interface <TVOE_IMI_Bridge_Bond_Ethernet1> updated

$ sudo /usr/TKLC/plat/bin/netAdm set
   --device=<TVOE_IMI_Bridge_Bond_Ethernet2>
   --type=Ethernet
   --master=<TVOE_IMI_Bridge_Bond>
   --slave=yes
   --onboot=yes

Interface <TVOE_IMI_Bridge_Bond_Ethernet2> updated
```

3. Execute these 2 commands ONLY IF `<TVOE_XMI_Bridge_Bond>` is different from `<TVOE_IMI_Bridge_Bond>`.

```
$ sudo syscheckAdm net ipbond --set --var=DEVICES
   --val=<TVOE_XMI_Bridge_Interface_Bond>,
   <TVOE_IMI_Bridge_Interface_Bond>,[other bonds...]

$ sudo syscheckAdm net ipbond -enable
```

7. RMS Server: Create IMI bridge interface

If you are using VLAN tagging for the IMI bridge interface, then you must create the VLAN interface first.

```
$ sudo /usr/TKLC/plat/bin/netAdm add
   --device=<TVOE_IMI_Bridge_Interface>
   --onboot=yes

Interface <TVOE_IMI_Bridge_Interface> created.
```
## Procedure 25. Configure TVOE

### 8. RMS Server: Create IMI bridge

Create the IMI bridge:

```bash
$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=imi --onboot=yes
--bridgeInterfaces=<TVOE_IMI_Bridge_Interface>
Interface <TVOE_IMI_Bridge_Interface> updated.
Bridge imi created.
```

### 9. RMS Server iLO: Create management bridge and assign TVOE management IP

1. Execute this step only if the TVOE host is a rack mount server and is NOT the PMAC server.

   **Note:** The output below is for illustrative purposes only. The site information for this system determines the network interfaces (network devices, bonds, and bond enslaved devices) to configure.

2. If `<TVOE_Management_Bridge_Interface>`, or the bond it is based on (if using tagged interface), has not yet been created, then execute the next 3 commands; otherwise, skip to the example section:

   ```bash
   $ sudo /usr/TKLC/plat/bin/netAdm add
   --device=<TVOE_Mgmt_Bridge_Interface_Bond>
   --onboot=yes --type=Bonding --mode=active-backup
   --miimon=100
   Interface <TVOE_Management_Bridge.Interface> added
   
   $ sudo /usr/TKLC/plat/bin/netAdm set
   --device=<TVOE_Mgmt_Bridge_Bond_Interface1>
   --type=Ethernet --master=<TVOE_Mgmt_Bridge_Interface_Bond>
   --slave=yes --onboot=yes
   Interface <mgmt_ethernet_interface1> updated.
   
   $ sudo /usr/TKLC/plat/bin/netAdm set
   --device=<TVOE_Mgmt_Bridge_Bond_Interface2>
   --type=Ethernet --master=<TVOE_Mgmt_Bridge_Interface_Bond>
   --slave=yes --onboot=yes
   Interface <mgmt_ethernet_interface2> updated
   ```

   **EXAMPLE 1:** Create Management bridge using untagged interfaces

   ```bash
   $ sudo /usr/TKLC/plat/bin/netAdm add
   --type=Bridge
   --name=management --bootproto=none --onboot=yes
   --address=<TVOE_Mgmt_IP_Address>
   --netmask=<TVOE_Mgmt_Netmask/Prefix>
   --bridgeInterfaces=<TVOE_Mgmt_Bridge_Interface>
   ```

   **EXAMPLE 2:** Create Management bridge using tagged interfaces

   ```bash
   $ sudo /usr/TKLC/plat/bin/netAdm add
   --device=<TVOE_Management_Bridge_Interface>
   $ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge
   ```
### Procedure 25. Configure TVOE

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>10. RMS Server</strong></td>
<td><strong>iLO</strong>: Add default route</td>
</tr>
<tr>
<td></td>
<td>Add a default route using the xmi or management address (if configured).</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo /usr/TKLC/plat/bin/netAdm add --route=default --gateway=&lt;TVOE_Mgmt_gateway_IP_address&gt; --device=&lt;management or xmi&gt;</code></td>
</tr>
<tr>
<td></td>
<td>Route to management created.</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>11. RMS Server</strong></td>
<td><strong>iLO</strong>: Verify bridge creation status</td>
</tr>
<tr>
<td></td>
<td>Verify the XMI and IMI bridges have been created successfully.</td>
</tr>
<tr>
<td></td>
<td><code>$ brctl show</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example output:</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Bridge Output" /></td>
</tr>
<tr>
<td></td>
<td>- Verify <code>imi</code> and <code>xmi</code> are listed under the bridge name column.</td>
</tr>
<tr>
<td></td>
<td>- Verify <code>&lt;TVOE_XMI_Bridge_Interface&gt;</code> is listed under the interfaces column for <code>xmi</code>.</td>
</tr>
<tr>
<td></td>
<td>- Verify <code>&lt;TVOE_IMI_Bridge_Interface&gt;</code> is listed under the interfaces column for <code>imi</code>.</td>
</tr>
<tr>
<td></td>
<td>- Verify the <code>&lt;TVOE_Mgmt_Bridge_Interface&gt;</code> is listed under the interface column for <code>&lt;TVOE_Mgmt_Bridge_Interface&gt;</code></td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>12. RMS Server</strong></td>
<td><strong>iLO</strong>: Create NetBackup bridge (Optional)</td>
</tr>
<tr>
<td></td>
<td>Perform this command if you have a dedicated NetBackup interface within your NOAM guests (and if the NetBackup bridge was NOT configured when setting up the PMAC earlier).</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=NetBackup --onboot=yes --MTU=&lt;NetBackup_MTU_size&gt; --bridgeInterfaces=&lt;TVOE_NetBackup_Bridge_Interface&gt;</code></td>
</tr>
</tbody>
</table>
Procedure 25. Configure TVOE

13. **RMS Server iLO**: Set hostname

   $ sudo su – pltcfg

   1. Navigate to **Server Configuration > Hostname > Edit** and enter a new hostname for your server:

   ![Edit Hostname](image)

   2. Click **OK** and continue to click **Exit** until you are at the pltcfg main menu again.

   **Note**: Although the new hostname has been properly configured and committed at this point, it does not display on your command prompt unless you log out and log back in again.
### Procedure 25. Configure TVOE

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>From the platcfg main menu, navigate to <strong>Network Configuration &gt; SNMP Configuration &gt; NMS Configuration</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>Add a New NMS Server</strong>.</td>
</tr>
</tbody>
</table>
| 4.   | Enter the following NMS servers, clicking **OK** after each one and then selecting the **Add NMS** option again:  
  - Enter the Hostname/IP of the customer NMS server, for port enter 162, and for Community String enter the community string provided in the customer NAPD Document.  
  - Enter the IP of the NOAM VIP, for port enter 162, and for Community String enter the community string provided in the customer NAPD Document |
| 5.   | Click **Exit**. |
| 6.   | Click **Yes** when prompted to restart the Alarm Routing Service. |
| 7.   | Once Done, click **Exit** to quit to the platcfg main menu. |
Procedure 25. Configure TVOE

1. Select **Network Configuration**.

2. Select **NTP**.
3. Click **Edit**.

   - ntpserver1: Enter customer provided NTP server #1 IP address.
   - ntpserver2: Enter customer provided NTP server #2 IP address.
   - ntpserver3: Enter customer provided NTP server #3 IP address.

4. Click **OK**.
5. Click **Exit** to return to the platcfg menu.
### Procedure 25. Configure TVOE

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>16. RMS Server iLO: Configure timezone</td>
<td>$ sudo su - platcfg</td>
<td>1. Navigate to <strong>Server Configuration &gt; Time Zone</strong>.</td>
</tr>
</tbody>
</table>

1. Navigate to **Server Configuration > Time Zone**.

![Server Configuration Menu](image)

2. If the time zone displayed matches the time zone you desire, then you can continue to hit Exit until you are out of the platcfg program. If you want a different time zone, then proceed with this instruction.

3. **Click Edit**.

![Server Configuration Menu](image)

4. Select the desired time zone from the list and **click Enter**.

5. Continue clicking **Exit** until you are out of the platcfg program.

| 17. RMS Server iLO: Reboot server | Reboot the server. | $ sudo su - platcfg |

![Reboot Server](image)
Appendix J. Create NOAM/SOAM Virtual Machines

Procedure 26. Create NOAM Guest VMs

<table>
<thead>
<tr>
<th>STEP #</th>
<th>PMAC GUI: Login</th>
<th>1. Open web browser and enter:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>http://&lt;PMAC_Mgmt_Network_IP&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Login as <strong>pmacadmin</strong> user:</td>
</tr>
</tbody>
</table>

This procedure creates a DSR NOAM virtual machine (referred to as a **guest**) on a TVOE server blade or TVOE RMS. It is repeated for every NOAM server you want to install.

**Prerequisite:** TVOE has been installed and configured on the target blade server or RMS

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.
Procedure 26. Create NOAM Guest VMs

1. Navigate to **Main Menu > VM Management**.

2. **PMAC GUI**: Navigate to VM management of the target server blade

   1. Navigate to **Main Menu > VM Management**.

   2. Select the TVOE server blade or rack mounted server from the **VM Entities** listing on the left side of the screen. The selected server’s guest machine configuration displays in the remaining area of the window.

   View host on RMS pc5010439

<table>
<thead>
<tr>
<th>VM Info</th>
<th>Software</th>
<th>Network</th>
<th>Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Bridges</td>
<td>Storage Pools</td>
<td>Memory</td>
</tr>
</tbody>
</table>

   **Host Name**: 5010439-TVOE
   **Location**: RMS pc5010439

   **Guests**

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zombie_DSRDR_NOAM2</td>
<td>Running</td>
</tr>
<tr>
<td>Zombie_DSRNO_AM2</td>
<td>Running</td>
</tr>
</tbody>
</table>

3. Click **Create Guest**.
Procedure 26. Create NOAM Guest VMs

1. Click Import Profile.

2. From the ISO/Profile drop-down box, select the entry that matches depending on the hardware that your NOAM VM TVOE server is running on and your preference for NetBackup interfaces:

<table>
<thead>
<tr>
<th>NOAM VM TVOE Hardware Type(s)</th>
<th>Dedicated Netbackup Interface?</th>
<th>Navigate to Profile (Application ISO NAME)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP DL380 Gen 8 RMS</td>
<td>No</td>
<td>DSR_NOAMP_LARGE</td>
</tr>
<tr>
<td>HP BL460 Gen 9 RMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP BL460 Gen 8 Blade</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP BL460 Gen 9 Blade</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP DL380 Gen 8 RMS</td>
<td>Yes</td>
<td>DSR_NOAMP_LARGE_NBD</td>
</tr>
<tr>
<td>HP BL460 Gen 9 RMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP BL460 Gen 8 Blade</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP BL460 Gen 9 Blade</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Application_ISO_NAME is the name of the DSR Application ISO to be installed on this NOAM

3. Click Select Profile.
4. Click Create
### Procedure 26. Create NOAM Guest VMs

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td><strong>PMAC GUI</strong>: Wait for guest creation to complete</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Task Monitoring</strong> to monitor the progress of the guest creation task. A separate task displays for each guest creation you start.</td>
</tr>
<tr>
<td>2.</td>
<td>Wait or refresh the screen until you see the guest creation task has completed successfully.</td>
</tr>
<tr>
<td>5.</td>
<td><strong>PMAC GUI</strong>: Verify guest machine is running</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Main Menu &gt; VM Management</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the TVOE server blade on which the guest machine was just created.</td>
</tr>
<tr>
<td>3.</td>
<td>Look at the list of guests present on the blade and verify you see a guest that matches the name you configured and that its status is <strong>Running</strong>.</td>
</tr>
</tbody>
</table>

#### View guest Zombie_DSRNOAM2

<table>
<thead>
<tr>
<th>VM Info</th>
<th>Software</th>
<th>Network</th>
<th>Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Virtual Disks</td>
<td>Virtual NICs</td>
<td></td>
</tr>
</tbody>
</table>

- **Current Power State**: **Running**
- **Set Power State**: On
- **Guest Name (Required)**: Zombie_DSRNOAM2
- **Host**: RMS: pc5010439
- **Number of vCPUs**: 4
- **Memory (MBs)**: 6,144
- **VM UUID**: e9e22407-c289-4d2a-a1f6-6c7121905d40
- **Enable Virtual Watchdog**: ✓

4. VM creation for this guest is complete. Repeat from step 2 for any remaining NOAM VMs (for instance, the standby NOAM) that must be created.
### Procedure 27. Create SOAM Guest VMs

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. PMAC GUI: Login</td>
<td><strong>Prerequisite:</strong> TVOE has been installed and configured on the target blade server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td>
</tr>
</tbody>
</table>

1. Open web browser and enter:

   ![Login dialog](image)

   **Username:** [__]  
   **Password:** [__]

   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.

   http://<PMAC_Mgmt_Network_IP>

2. Login as `pmacadmin` user:
Procedure 27. Create SOAM Guest VMs

1. Navigate to Main Menu > VM Management.

2. Select the TVOE server blade or rack mounted server from the VM Entities listing on the left side of the screen. The selected server’s guest machine configuration displays in the remaining area of the window.

3. Click Create Guest.
## Procedure 27. Create SOAM Guest VMs

1. **Click Import Profile.**

   ![Import Profile](image)

   **Import Profile**
   - **ISO/Profile:** DSR-B.0.0.0.0_80.11.0-x86_64 => DSR_SOAM
   - **Num CPUs:** 4
   - **Memory (MBs):** 6144
   - **Virtual Disks:**
     - **Prim:** Yes, Size (MB): 107400
     - **NICS:**
       - **Bridge:** control
       - **TBD Dev:** control
   - **Pool:** vgguests
   - **TPD Dev:**

2. From the **ISO/Profile** drop-down box, select the entry that matches depending on the hardware that your SOAM VM TBOE server is running on and your preference for NetBackup interfaces.

<table>
<thead>
<tr>
<th>SOAM VM TBOE Hardware Type(s)</th>
<th>Dedicated Netbackup Interface?</th>
<th>Navigate to Profile (Application ISO NAME)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP BL460 Gen 8 Blade, HP BL460 Gen 9 Blade</td>
<td>No</td>
<td>DSR_SOAM</td>
</tr>
<tr>
<td>HP BL460 Gen 8 Blade, HP BL460 Gen 9 Blade</td>
<td>Yes</td>
<td>DSR_SOAM_NBD</td>
</tr>
</tbody>
</table>

   **Note:** Application ISO NAME is the name of the DSR Application ISO to be installed on this SOAM

3. **Click Select Profile.**

4. **Edit the name, if you want.** For instance: **DSR_SOAM_A** or **DSR_SOAM_B**. This is not the ultimate hostname. It is just an internal tag for the VM host manager.

5. **Click Create.**

4. **PMAC GUI:** Wait for guest creation to complete

   ![Create Guest](image)

   **Create Guest**
   - **RMS:** pc5016441
   - **Guest:** Zombie_DSR_SOAM1
   - **Guest creation completed (Zombie_DSR_SOAM1)**

   1. Navigate to **Task Monitoring** to monitor the progress of the guest creation task. A separate task displays for each guest creation you start.

   2. Wait or refresh the screen until you see that the guest creation task has completed successfully.
### Procedure 27. Create SOAM Guest VMs

<table>
<thead>
<tr>
<th></th>
<th>PMAC GUI: Verify guest machine is running</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to <strong>Main Menu &gt; VM Management</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the TVOE server blade on which the guest machine was just created.</td>
</tr>
<tr>
<td>3.</td>
<td>Look at the list of guests present on the blade and verify you see a guest that matches the name you configured and that its status is <strong>Running</strong>.</td>
</tr>
</tbody>
</table>

4. VM creation for this guest is complete. Repeat from Step 2 for any remaining NOAM VMs (for instance, the standby SOAM) that must be created.
Appendix K. SNMP Configuration

Procedure 28. 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.

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Note: This workaround step should be performed only in the following cases:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>If SNMP is not configured.</td>
</tr>
<tr>
<td></td>
<td>If SNMP is already configured and <strong>SNMPv3</strong> is selected as enabled version.</td>
</tr>
</tbody>
</table>

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

![Login Screen](http://<Primary_NOAM_VIP_IP_Address>)

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 28. Configure SNMP**

1. Navigate to Administration > Remote Servers > SNMP Trapping.

2. Select the Server Group tab for SNMP trap configuration:

3. Type the **IP address** or **hostname** of the Network Management Station (NMS) where you want to forward traps. This IP should be reachable from the NOAMP’s XMI network. If already configured SNMP with **SNMPv3** as enabled version, another server needs to be configured here.

4. Continue to fill in additional secondary, tertiary, etc., **Manager IPs** in the corresponding slots if desired.

5. Set the Enabled Versions as **SNMPv2c** and **SNMPv3**.

6. Check **Traps Enabled** checkboxes for the Manager servers being configured.

7. Type the **SNMP Community Name**.

8. Leave all other fields at their default values.

9. Click **OK**.
Procedure 28. Configure SNMP

3. PMAC GUI: Login

1. Open web browser and enter:

   http://<PMAC_Mgmt_Network_IP>

2. Login as guiadmin user:

   ![Oracle System Login](image)
Procedure 28. Configure SNMP

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to Administration &gt; Credentials &gt; SNMP Community String Update.</td>
</tr>
<tr>
<td>2.</td>
<td>Check the <strong>Use Site Specific Read/Write Community String</strong> checkbox.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Read Only</strong> or <strong>Read/Write</strong> Community String:</td>
</tr>
<tr>
<td></td>
<td>□ Read Only  □ Read/Write</td>
</tr>
<tr>
<td></td>
<td>Check this box if updating servers using the <strong>Site Specific</strong> SNMP Community String:</td>
</tr>
<tr>
<td></td>
<td>□ Use Site Specific Read/Write Community String</td>
</tr>
<tr>
<td></td>
<td>Community String: [Enter String]</td>
</tr>
<tr>
<td></td>
<td>Note: The Community String value can be 1 to 31 uppercase, lowercase, or numeric characters.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>Update Servers</strong>.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

**PMAC GUI:** Update the TVOE host SNMP community string
### Appendix L. Backup Directory

#### Procedure 29. Backup Directory

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command 1</th>
<th>Command 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>NOAM/SOA M VIP Console: Determine if backup directory exists</td>
<td>$ cd /var/TKLC/db/filemgmt/</td>
<td>$ ls -ltr</td>
</tr>
<tr>
<td></td>
<td>Execute this command on an active NOAM/SOAM server console (accessed using the VIP) and compare the output.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Look for the backup directory in the output.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Make sure the directory is already created with correct permission. The directory looks like this:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the directory is already there with correct permissions, then skip steps 2 and 3.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If directory does not have the correct permissions, then go to step 3.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>NOAM/SOA M VIP Console: Create backup directory</td>
<td>cd /var/TKLC/db/filemgmt/</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Go to the backup directory location.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create backup directory.</td>
<td>mkdir backup</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verify directory has been created.</td>
<td>ls -ltr</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var/TKLC/db/filemgmt/backup</td>
<td></td>
</tr>
</tbody>
</table>

*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 29. Backup Directory

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>ls -ltr /var/TKLC/db/filemgmt/backup</code></td>
<td>Verify directory has been created.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td><code>chmod 770 /var/TKLC/db/filemgmt/backup</code></td>
<td>Change permissions for the backup directory.</td>
</tr>
<tr>
<td>3.</td>
<td><code>sudo chown -R awadmin:awadm /var/TKLC/db/filemgmt/backup</code></td>
<td>Change ownership of backup directory.</td>
</tr>
<tr>
<td>4.</td>
<td><code>ls /var/TKLC/db/filemgmt/backup</code></td>
<td>Directory displays as follows:</td>
</tr>
</tbody>
</table>

```
drwxrwx--- 2 awadmin awadm        4096 Dec 22 02:15 backup
```

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td><code>cp BACKUPFILE /var/TKLC/db/filemgmt/backup</code></td>
<td>Copy the backup file to the backup directory.</td>
</tr>
<tr>
<td>2.</td>
<td><code>chmod 666 Backup.*</code></td>
<td>Change permissions of files in the backup directory.</td>
</tr>
<tr>
<td>3.</td>
<td><code>sudo chown -R awadmin:awadm Backup.*</code></td>
<td>Change ownership of files in the backup directory.</td>
</tr>
</tbody>
</table>

### Appendix M. 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.