Oracle Communications DSR Rack Mount Server 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 How to Use this Document ......................................................................................... 8  
   1.5 Optional Features ....................................................................................................... 8  

2. **General Description** ....................................................................................................... 9  
   2.1 Complete Server Outage (All Servers) ........................................................................ 10  
   2.2 Partial Server Outage with One NOAM Server Intact and Both SOAMs Failed .......... 10  
   2.3 Partial Server Outage with Both NOAM Servers Failed and One SOAM Server Intact...... 10  
   2.4 Partial Server Outage with NOAM and One SOAM Server Intact .............................. 11  
   2.5 2.5 Partial Server Outage with Both NOAMs Failed and DR-NOAM Available .......... 11  
   2.6 Partial Service Outage with Corrupt Database ......................................................... 11  

3. **Procedure Overview** ...................................................................................................... 11  
   3.1 Required Materials ..................................................................................................... 11  
   3.2 Disaster Recovery Strategy ....................................................................................... 12  

4. **Disaster Recovery Procedure** ........................................................................................ 14  
   4.1 Recovery Scenario 1 (Complete Server Outage) ......................................................... 14  
   4.2 Recovery Scenario 2 (Partial Server Outage with One NOAM Server Intact and ALL SOAMs Failed) ............................................................. 56  
   4.3 Recovery Scenario 3 (Partial Server Outage with All NOAM Servers Failed and One SOAM Server Intact) ...................................................... 91  
   4.4 Recovery Scenario 4 (Partial Server Outage with One NOAM Server and One SOAM Server Intact) ..................................................... 124  
   4.5 Recovery Scenario 5 (Both NOAM Servers Failed with DR-NOAM Available) .......... 148  
   4.6 Recovery Scenario 6 (Database Recovery) .................................................................. 153  
      4.6.1 Recovery Scenario 6: Case 1 .................................................................................. 153  
      4.6.2 Recovery Scenario 6: Case 2 ............................................................................... 159  

5. **Resolve User Credential Issues after Database Restore** .................................................. 164  
   5.1 Restore a Deleted User ............................................................................................... 164  
   5.2 Keep a Restored User ................................................................................................. 164  
   5.3 Remove a Restored User ............................................................................................ 166  
   5.4 Restore a Modified User ............................................................................................ 167  
   5.5 Restore an Archive that Does Not Contain a Current User ....................................... 167  

6. **IDIH Disaster Recovery** .................................................................................................. 172  

**Appendix A. DSR Database Backup** ................................................................................. 178
Appendix B. Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only) .......................................................................................................................... 181
Appendix C. Inhibit A and B Level Replication on C-level Servers ................................................................. 183
Appendix D. Un-Inhibit A and B Level Replication on C-level Servers ................................................................. 184
Appendix E. Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost) ............................................................................................................. 185
Appendix F. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost) ............................................................................................................. 187
Appendix G. Restore TVOE Configuration from Backup Media .............................................................................. 188
Appendix H. Restore PMAC from Backup .............................................................................................................. 196
Appendix I. Restore Provisioning Database ........................................................................................................ 205
Appendix J. Recover PDB Relay ........................................................................................................................ 208
Appendix K. SNMP Configuration ....................................................................................................................... 209
Appendix L. Backup Directory ........................................................................................................................... 212
Appendix M. My Oracle Support (MOS) ........................................................................................................... 213

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

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

List of Procedures
Procedure 1. Recovery Scenario 1 .................................................................................................................... 15
Procedure 2. Recovery Scenario 2 .................................................................................................................... 57
Procedure 3. Recovery Scenario 3 .................................................................................................................... 92
Procedure 4. Recovery Scenario 4 .................................................................................................................... 125
Procedure 5. Recovery Scenario 5 .................................................................................................................... 148
Procedure 6. Recovery Scenario 6 (Case 1) ...................................................................................................... 153
Procedure 7. Recovery Scenario 6 (Case 2) ...................................................................................................... 159
Procedure 8. Keep Restored User ................................................................................................................... 164
Procedure 9. Remove the Restored User ......................................................................................................... 166
Procedure 10. Restore an Archive That Does Not Contain a Current User ............................................. 168
Procedure 11. IDIH Disaster Recovery Preparation ................................................................................. 173
Procedure 12. IDIH Disaster Recovery (Re-Install Mediation and Application Servers) ....................... 175
Procedure 13. DSR Database Backup .................................................................................................. 178
Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F) (HP DL380 Gen 9 Only) .......................................................................................................................... 181
Procedure 15. Inhibit A and B Level Replication on C-level Servers .................................................... 183
Procedure 16. Un-Inhibit A and B Level Replication on C-level Servers .............................................. 184
Procedure 17. Inhibit A and B Level Replication on C-level Servers .................................................... 185
Procedure 18. Un-Inhibit A and B Level Replication on C-Level Servers ............................................ 187
Procedure 19. Restore TVOE Configuration from Backup Media ........................................................... 188
Procedure 20. Restore PMAC from Backup Media .................................................................................. 196
Procedure 21. Restore PMAC from Backup Server .............................................................................. 199
Procedure 22. Restore Provisioning Database......................................................................................... 205
Procedure 23. Recover PDB Relay ........................................................................................................ 208
Procedure 24. Configure SNMP ........................................................................................................... 209
Procedure 25. Backup Directory ............................................................................................................ 212
1. Introduction

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

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

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

1.1 References

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

1.2 Acronyms

An alphabetized list of acronyms used in the document.

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

### Terminology
An alphabetized list of terms used in the document.

**Table 2. Terminology**

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

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

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

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

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

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

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

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

Figure 1. Example Procedure Steps Used in This Document

1.5 Optional Features

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

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

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

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

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

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

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

### 2.1 Complete Server Outage (All Servers)

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

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

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

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

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

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

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

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

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

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

2.6 Partial Service Outage with Corrupt Database

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

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

3. Procedure Overview

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

3.1 Required Materials

The following items are needed for disaster recovery:

1. A hardcopy of this document and hardcopies of all documents in the reference list.
2. Hardcopy of all NAPD performed at the initial installation and network configuration of this customer’s site. If the NAPD cannot be found, escalate this issue within My Oracle Support (MOS) until the NAPD documents can be located.
3. DSR recent backup files: electronic backup file (preferred) or hardcopy of all DSR configuration and provisioning data.
5. The XML configuration files used to configure the Cisco 4948 aggregation switches, available on the PMAC Server (or PMAC backup).
6. The switch backup files taken after the switch is configured, available on the PMAC server (or PMAC backup).
7. The network element XML file used for the initial configuration.
8. Firmware files as provide by hardware vendor.
9. NetBackup files if they exist. This may require the assistance of the customer’s NetBackup administrator.
10. PMAC and TVOE backups (if available).
11. One (1) target release DSR media or a target-release ISO.
13. Three (3) target release iDIH Media or target-release ISOs.

15. Latest RADIUS shared secret encryption key file backup (DpiKf.bin.encr).

16. List of activated and enabled features.

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

### 3.2 Disaster Recovery Strategy

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

1. Evaluate failure conditions in the network and determine that normal operations cannot continue without disaster recovery procedures. This means the failure conditions in the network match one of the failure scenarios described in section 2.

2. Read and review the content in this document.

3. Gather required materials in section 3.1 Required Materials.

4. From the failure conditions, determine the Recovery Scenario and procedure to follow (using Figure 2 and Table 4. Recovery Scenarios).

5. Execute appropriate recovery procedures (listed in Table 4. Recovery Scenarios).
Figure 2. Determining Recovery Scenario
4. Disaster Recovery Procedure

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

**WARNING**

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

**Recovering Base Hardware:**

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

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

**WARNING**

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

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

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

4.1 Recovery Scenario 1 (Complete Server Outage)

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

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

- Recover base hardware and software for all rack mount servers
  - Recover the base hardware
  - Recover the virtual machines
  - Recover the software
- Recover **PMAC**
- Recover active **NOAM** guest
  - Recover the NOAM database
  - Reconfigure the application
- Recover standby **NOAM** guest
  - Reconfigure the application
- Recover query server (SDS only) guest
  - Reconfigure the application
- Recover all **SOAM** and MP/DP guest
  - Recover the SOAM database
  - Reconfigure the application
- Recover **IDIH**, if necessary
- Restart processes and re-enable provisioning and replication.

**Procedure 1. Recovery Scenario 1**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Gather required materials&lt;br&gt;Gather the documents and required materials listed in the Required Materials section.</td>
</tr>
<tr>
<td>2.</td>
<td>Create a backup directory, if needed&lt;br&gt;Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.</td>
</tr>
<tr>
<td>3.</td>
<td>Replace failed equipment&lt;br&gt;Work with the hardware vendor to replace the failed equipment.</td>
</tr>
<tr>
<td>4.</td>
<td>Recover <strong>PMAC</strong> and <strong>PMAC TVOE</strong> Host: Configure BIOS settings and update firmware&lt;br&gt;1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:&lt;br&gt;  - <strong>HP DL380 Gen8</strong>: Configure HP Gen 8 Server BIOS Settings&lt;br&gt;  - <strong>Oracle X5-2/Netra X5-2/X6-2/X7-2</strong>: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings&lt;br&gt;  - <strong>HP DL380 Gen9</strong>: Configure HP Gen9 Server BIOS Settings&lt;br&gt;  2. Verify and/or upgrade server firmware by executing the <strong>Upgrade Rack Mount Server Firmware</strong> procedure from reference [8].&lt;br&gt;Note: Determine VM placement and pinning by following:&lt;br&gt;  - Section 3.1, item 14; and&lt;br&gt;  - In reference [8], Appendix S VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1 Gbps NICs) and CPU Pinning in HP DL380 Gen 9 (Onboard 1 Gbps NICs) for Pinning Information on HP DL380 Gen 9.</td>
</tr>
</tbody>
</table>
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Details</th>
</tr>
</thead>
</table>
| 5.   | Recover PMAC, TVOE Hosts, and Switch | This step assumes TVOE and PMAC backups are available. If backups are NOT available, **skip this step**.  
1. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.  
2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup.  
3. Proceed to step 7. |
| 6.   | Recover PMAC, TVOE Hosts, and Switch | This step assumes TVOE and PMAC backups are NOT available. If the TVOE and PMAC have already been restored, **skip this step**.  
Execute these procedures from reference [8]:  
- Install and Configure TVOE on First RMS (PMAC Host)  
- Install PMAC  
- Initialize the PMAC Application |
| 7.   | Recover failed Cisco 4948 aggregation switches | Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 GEN 9, **skip this step**.  
Recover failed Cisco 4948 aggregation switches, if needed:  
1. Back up available configuration files. Refer to Appendix C Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only) to recover failed Cisco 4948 aggregation switches.  
2. Back up configuration files NOT available. Execute the **Configure Cisco 4948E-F Aggregation Switches (HP DL 380 Gen 8 Only)** section from reference [8]. |
| 8.   | Configure PMAC (no backup) | If PMAC backup was NOT restored in step 5, execute this step; otherwise, skip this step.  
Execute these procedures from reference [8]:  
- Configure PMAC Server (NetBackup Only)  
- Add RMS to the PMAC Inventory |
| 9.   | Install/Configure additional rack mount servers | 1. Execute the **Install TVOE on Additional Rack Mount Servers** procedure from reference [8].  
2. **If backups are available**, restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.  
**If backups are NOT available**, execute the **Configure TVOE on Additional Rack Mount Servers** procedure from reference [8]. |
| 10.  | Configure BIOS settings and update firmware on additional rack mount servers | 1. Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]:  
- **HP DL380 Gen8**: Configure HP Gen 8 Server BIOS Settings  
- **Oracle X5-2/Netra X5-2/X6-2/X7-2**: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings  
- **HP DL380 Gen9**: Configure HP Gen9 Server BIOS Settings  
2. Verify and/or upgrade server firmware by executing the **Upgrade Rack Mount Server Firmware** procedure from reference [8]. |
### Procedure 1. Recovery Scenario 1

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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
|   | • XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured)  
  |   | • XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured)  
  |   | • DSRNOAM1XMIIPADDRESS (if DSRNOAM1 is being configured)  
  |   | • DSRNOAM2XMIIPADDRESS (if DSRNOAM2 is being configured)  
  |   | • DSRDRNOAM1XMIIPADDRESS (if DSRDRNOAM1 is being configured)  
  |   | • DSRDRNOAM2XMIIPADDRESS (if DSRDRNOAM2 is being configured)  
  |   | • SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured)  
  |   | • SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured)  
  |   | • SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured)  
  |   | • SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured)  

**Notes:**

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

### WARNING

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

<table>
<thead>
<tr>
<th>17.</th>
<th><strong>PMAC:</strong> Copy the backed up fdc file to the RMS directory</th>
</tr>
</thead>
</table>
|     | Copy the fdconfig backup file to the RMS directory.  
  |     | $ sudo cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file>  
  |     | /usr/TKLC/smac/etc/RMS/  

Procedure 1. Recovery Scenario 1

18. **PMAC**: Execute the `config.sh` script

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

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

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

Example output:

```
Validating cfg file...
Successful validation of cfg file.
Added Cabinet 101 to Fast Deployment File.
Added Zombie_TVOE1 to Fast Deployment File.
Added Zombie_TV0E2 to Fast Deployment File.
Added xml (bond0.4) to Fast Deployment File.
Added ini (bond0.3) to Fast Deployment File.
Added rep (bond1.10) to Fast Deployment File.
Added xml (bond1.6) to Fast Deployment File.
Added xml (bond1.7) to Fast Deployment File.
Added xml (bond1.8) to Fast Deployment File.
Added xml (bond1.9) to Fast Deployment File.
Added xml (bond1.10) to Fast Deployment File.
Added xml (bond1.11) to Fast Deployment File.
Added xml (bond1.12) to Fast Deployment File.
Added xml (bond1.13) to Fast Deployment File.
Added xml (bond1.14) to Fast Deployment File.
Added xml (bond1.15) to Fast Deployment File.
Added xml (bond1.16) to Fast Deployment File.
Added xml (bond1.17) to Fast Deployment File.
Added xml (bond1.18) to Fast Deployment File.
Added xml (bond1.19) to Fast Deployment File.
Added xml (bond1.20) to Fast Deployment File.
Added xml (bond1.21) to Fast Deployment File.
Added xml (bond1.22) to Fast Deployment File.
```

Validating Fast Deployment File......

```
Configuration file validation successful.
```

```
SUCCESS: OPERATION SUCCESS!!
```

Procedure 1. Recovery Scenario 1

19. PMAC: Execute fast deployment

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

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

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

20. PMAC GUI: Monitor the configuration

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

2. Navigate to **Task Monitoring**.

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

3. Monitor the configuration to completion:

   ![Main Menu: Task Monitoring](image)

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

   ```
   [admusr@melbourne-pmac-1 fdconfig]$ sudo fdconfig dumpsteps --file=deploy_melbourne_20170329T202458_701b.fdcdb
   Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb"
   Here are the steps that were generated
   ------------------------ begin ------------------------
   Dump of DB steps:
   NUM PHS DLY INFRA ID SVRTYPE CMD ELEMENT
   1   1   0 pmac Fast_Deployment 0 Complete 300 0 Check PM&C is available
   2   1   0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet
   3   1   0 pmac Fast_Deployment 0 3 melbourne_RMS3 1 Skipped 900 0 Add Rms
   4   2   0 pmac Fast_Deployment 1
   ------------------------ end ------------------------
   ```

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

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>26.</td>
<td><strong>NOAM GUI</strong>: Login DSR only. If SDS, skip to step 31.</td>
</tr>
</tbody>
</table>

Log into the NOAM GUI as the `guiadmin` user.

![Oracle System Login](image)

**Welcome to the Oracle System Login.**

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

Unauthorized access is prohibited.

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

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

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27. NOAM GUI</td>
<td>Upload the backup database file. DSR only. If SDS, skip to step 31.</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to Status &amp; Manage &gt; Files.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the active NOAM server.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <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. <strong>Note:</strong> 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

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

1. Navigate to Status & Manage > Database.

2. Click Disable Provisioning.

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

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

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

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

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

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

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

| 30. | **Active NOAM:**
|     | Restore the database.
|     | DSR only. If SDS, skip to step 31.

1. From **Status & Manage > Database**.
2. Select the active NOAM server and click Restore.
3. Select the proper 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.dsrs.ZombieNOAM1.Configuration"**

- Force Restore?
  - **Force**
  - **Force restore**

**Note:** After the restore has started, the user is logged out of the XMI NO GUI since the restored topology is old data.
6. Go to step 37.
### Procedure 1. Recovery Scenario 1

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

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM VIP GUI: Login</th>
<th>Action</th>
</tr>
</thead>
</table>
| 37.  | Login               | 1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  
  \[
  \text{http://<Primary_NOAM_VIP_IP_Address>}
  \]  
  2. Login as the **guiadmin** user: |
|      |                     | ![Oracle System Login](image) |
| 38.  | Monitor and confirm database restore | 1. Wait for **5-10 minutes** for the system to stabilize with the new topology:  
  2. Monitor the Info tab for **Success**. This indicates the restore is complete and the system is stabilized.  
  Ignore these alarms for NOAM and MP servers until all the servers are configured:  
  - Alarms with Type Column as **REPL, COLL, HA** (with mate NOAM), **DB** (about Provisioning Manually Disabled).  
  **Notes:**  
  - Do not pay attention to alarms until all the servers in the system are completely restored.  
  - The Configuration and Maintenance information is in the same state it was when backed up during initial backup. |
Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>39.</td>
<td><strong>Active NOAM</strong>: Set failed servers to <strong>OOS</strong></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>- Network Elements</td>
</tr>
<tr>
<td></td>
<td>- Server</td>
</tr>
<tr>
<td></td>
<td>- HA</td>
</tr>
<tr>
<td></td>
<td>- Database</td>
</tr>
<tr>
<td></td>
<td>- KPIs</td>
</tr>
<tr>
<td></td>
<td>- Processes</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Set the Max Allowed HA Role option to <strong>OOS</strong> for the failed servers.</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></td>
<td><img src="image" alt="Ok Cancel" /></td>
</tr>
<tr>
<td>40.</td>
<td><strong>NOAM VIP GUI</strong>: Recover standby NOAM</td>
</tr>
<tr>
<td></td>
<td>Install the second NOAM server:</td>
</tr>
<tr>
<td></td>
<td><strong>DSR</strong>:</td>
</tr>
<tr>
<td></td>
<td>Execute the <strong>Configure the Second NOAM Server</strong> procedure, steps 1 and 3-6, from reference [8].</td>
</tr>
<tr>
<td></td>
<td><strong>SDS</strong>:</td>
</tr>
<tr>
<td></td>
<td>Execute the <strong>Configure the Second SDS NOAM Server</strong> procedure, steps 1 and 3-6, from reference [8].</td>
</tr>
<tr>
<td>41.</td>
<td>Install NetBackup client (optional)</td>
</tr>
<tr>
<td></td>
<td>If NetBackup is used, execute the <strong>Install NetBackup Client (Optional)</strong> procedure from reference [8].</td>
</tr>
</tbody>
</table>
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>42.</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>- Status &amp; Manage &gt; Network Elements &gt; Server &gt; HA &gt; Database &gt; KPIs &gt; Processes &gt; Tasks &gt; Files</td>
</tr>
<tr>
<td></td>
<td>- Click <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td>- Select the standby NOAM server and set it to <strong>Active</strong>.</td>
</tr>
<tr>
<td></td>
<td>- Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>43.</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>- Status &amp; Manage &gt; Network Elements &gt; Server &gt; HA &gt; Database &gt; KPIs &gt; Processes &gt; Tasks</td>
</tr>
<tr>
<td></td>
<td>- Select the recovered standby NOAM server and click <strong>Restart</strong>.</td>
</tr>
</tbody>
</table>

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

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

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

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

Repeat step 45. for the remote export server.
## Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>47.</td>
<td><strong>NOAM VIP GUI:</strong> Perform Keyexchange with export server</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Administration &gt; Remote Servers &gt; Data Export.</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Administration</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>General Options</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Access Control</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Software Management</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Remote Servers</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>LDAP Authentication</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>SNMP Trapping</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Data Export</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>DNS Configuration</strong></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>SSH Key Exchange.</strong></td>
</tr>
<tr>
<td></td>
<td>3. Type the <strong>Password</strong> and click <strong>OK.</strong></td>
</tr>
<tr>
<td>48.</td>
<td><strong>NOAM VIP GUI:</strong> Recover query servers. SDS only. If DSR, skip to step 51.</td>
</tr>
<tr>
<td></td>
<td>Execute the <strong>Configuring SDS Query Servers</strong> procedure, steps 1 and 4-7, from reference [8].</td>
</tr>
</tbody>
</table>
**Procedure 1. Recovery Scenario 1**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>49.</td>
<td><strong>SDS NOAM VIP GUI</strong>: Set HA on query server. SDS only. If DSR, skip to step 51.</td>
</tr>
</tbody>
</table>
|      | 1. Navigate to **Status & Manage > HA**.  
|      | - **Status & Manage**  
|      |   - **Network Elements**  
|      |   - **Server**  
|      |   - **HA**  
|      |   - **Database**  
|      |   - **KPIs**  
|      |   - **Processes**  
|      |   - **Tasks**  
|      |   - **Files**  
|      | 2. Click **Edit**.  
|      | 3. Select the query server and select **Observer**.  
|      | 4. Click **OK**.  
| 50.  | **SDS NOAM VIP GUI**: Restart SDS application. SDS only. If DSR, skip to step 51. |
|      | 1. Navigate to **Status & Manage > Server**.  
|      | - **Status & Manage**  
|      |   - **Network Elements**  
|      |   - **Server**  
|      |   - **HA**  
|      |   - **Database**  
|      |   - **KPIs**  
|      |   - **Processes**  
|      | 2. Select the recovered query server and click **Restart**.  
| 51.  | **NOAM VIP GUI**: Stop replication to the C-level servers of this site. DSR only. If SDS, skip to step next.  
|      |  | **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.  

---

*Page 33*
**Procedure 1. Recovery Scenario 1**

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM VIP GUI: Recover active SOAM server</th>
<th>Install the SOAM servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>52.</td>
<td>DSR:</td>
<td>Execute the <strong>Configure the SOAM Servers</strong> procedure, steps 1-3 and 5-9, from reference [8]. <strong>Note:</strong> If you are using NetBackup, also execute step 12.</td>
</tr>
<tr>
<td></td>
<td>SDS:</td>
<td>Execute the <strong>Configure the SDS DP SOAM Servers</strong> procedure, steps 1-3 and 5-8, from reference [8].</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM VIP GUI: Set HA on the SOAM server</th>
<th>1. Navigate to <strong>Status &amp; Manage &gt; HA</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>53.</td>
<td></td>
<td>Status &amp; Manage &gt; HA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network Elements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KPIs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Files</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Active</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The n° of servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zombie SOAM1</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Active</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zombie SOAM2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Standby</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spare</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Observer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The n° of servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM VIP GUI: Restart DSR application</th>
<th>1. Navigate to <strong>Status &amp; Manage &gt; Server</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>54.</td>
<td></td>
<td>Status &amp; Manage &gt; Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network Elements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KPIs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Files</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Restart</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Restart</strong></td>
</tr>
</tbody>
</table>
Procedure 1. Recovery Scenario 1

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

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

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>56.</td>
<td><strong>Recovered SOAM GUI</strong>: Login. DSR only. If SDS, skip to step 60.</td>
</tr>
<tr>
<td>1.</td>
<td>Establish a GUI session on the recovered SOAM server.</td>
</tr>
</tbody>
</table>
| 2.   | Open the web browser and enter a URL of:  

   http://<Recovered_SOAM_IP_Address>  

| 3.   | Login as the **guiadmin** user: |

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>57.</td>
<td><strong>Recovered SOAM GUI</strong>: Verify the archive contents and database compatibility. DSR only. If SDS, skip to step 60.</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 27. of this procedure.</td>
</tr>
<tr>
<td>4.</td>
<td>Verify the output window matches the screen below.</td>
</tr>
<tr>
<td></td>
<td><strong>Database Archive Compare</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Database Compare" /></td>
</tr>
<tr>
<td></td>
<td><strong>The selected database came from ZombieSOAM1 on 1</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Archive Contents</strong></td>
</tr>
<tr>
<td></td>
<td>Configuration data</td>
</tr>
<tr>
<td></td>
<td><strong>Database Compatibility</strong></td>
</tr>
<tr>
<td></td>
<td>The databases are compatible.</td>
</tr>
</tbody>
</table>

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

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

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

- **Topology Compatibility**

  THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>58.</td>
<td><strong>Recovered SOAM GUI:</strong> Restore the database. DSR only. If SDS, skip to step 60.</td>
</tr>
<tr>
<td>1.</td>
<td>Select the <strong>Active SOAM</strong> server and click <strong>Restore</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the backup provisioning and configuration file.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
| 4.   | If the Node Type Compatibility error displays, it is expected. If no other errors display, mark the **Force** checkbox and click **OK** to proceed with the DB restore. **Notes:**
- After the restore has started, the user is logged out of XMI SOAM GUI since the restored topology is old data.
- If the spare SOAM is in another network and is unreachable, the database restore cannot be done. **Workaround:** If the spare SOAM is unreachable and ping (from recovered SOAM server to spare SOAM server) hangs (as evidenced by `ps -ef | grep ping` showing the same ping process and its child for more than 10 seconds), then kill the hung ping processes and the restore proceeds. |
| 59.  | **Recovered SOAM GUI:** Monitor and confirm database restoral. DSR only. If SDS, skip to step 60. |
|      | Wait for **5-10 minutes** for the system to stabilize with the new topology: Monitor the Info tab for **Success**. This indicates the restore is complete and the system is stabilized. **Notes:**
- Do not pay attention to alarms until all the servers in the system are completely restored.  
- The Configuration and Maintenance information is in the same state it was when backed up during initial backup. |
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1.   | establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  
|      | http://<Primary_NOAM_VIP_IP_Address> |
| 2.   | Login as the `guiadmin` user:  
|      | ![Oracle System Login](image) |
| 60.  | **NOAM VIP GUI:**  
|      | Login |
| 61.  | **NOAM VIP GUI:**  
|      | Recover the remaining SOAM servers (standby, spare) |

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

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

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

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

**NOAM VIP GUI**: Set HA on SOAM server

- [ ] 62.
Procedure 1. Recovery Scenario 1

63. **NOAM VIP GUI:**

Start replication on working C-level servers.

DSR only. If SDS, skip to next step.

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

- **If the spare SOAM is also present in the site and lost**, execute Appendix F Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost).
- **If the spare SOAM is NOT deployed in the site**, execute Appendix D Un-Inhibit A and B Level Replication on C-level Servers.

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

2. If the **Repl Status** is set to **Inhibited**, click **Allow Replication** using this order; otherwise, if none of the servers are inhibited, skip this step and continue with the next step:

   - Active NOAM Server
   - Standby NOAM Server
   - Active SOAM Server
   - Standby SOAM Server
   - Spare SOAM Server (if applicable) — Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only
   - Active DR NOAM Server
   - Standby DR NOAM Server
   - MP/IPFE Servers (if MPs are configured as active/standby, start with the active MP; otherwise, the order of the MPs does not matter)
   - SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only

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

<table>
<thead>
<tr>
<th>OAM Repl Status</th>
<th>SIG Repl Status</th>
<th>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>
## Procedure 1. Recovery Scenario 1

### 64. 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 standby NOAM server and click **Restart**.

### 65. NOAM VIP GUI: Perform Keyexchange 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 the **Task Name** and click **Key Exchange**.

   ![Key Exchange Task](image)

3. Type the **Password** and click **OK**.

   ![Password Entry](image)
**Procedure 1. Recovery Scenario 1**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 66.  | **Activate PCA feature.**  
      | DSR only  
      | **Note:** If you have PCA installed in the system being recovered, re-activate PCA by executing the **PCA Activation on Entire Network** procedure on the recovered NOAM server from [7].  
      |      |
| 67.  | **NOAM VIP GUI:**  
      | Recover the C-level server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs  
      | **Note:** If not all SOAM sites are recovered at this point, then repeat the activation for each “new” SOAM site that comes online.  
      |      |
| 68.  | **NOAM VIP GUI:**  
      | Set HA on all C-level servers  
      | **DSR:**  
      | Execute the **Configure the MP Servers** procedure, steps 1 and 9-13, from reference [8].  
      | **Note:** Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.  
      | SDS (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only):  
      | Execute the **Configure the SDS DP Servers** procedure, steps 1 and 5-8, from reference [8].  
      | Repeat this step for any remaining failed MP servers.  
      |      |

1. Navigate to **Status & Manage -> HA**.  
2. Click **Edit**.  
3. For each recovered C-Level with a Max Allowed HA Role set to **OOS**, set it to **Active**.  
4. Click **OK**.
**Procedure 1. Recovery Scenario 1**

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

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

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

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

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

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

1. Navigate to Status & Manage > Database.

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

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

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

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 72.  | **Active NOAM:** Activate optional features. DSR only. If SDS, then skip to next step.  
|      | Establish an SSH session to the active NOAM and login as admusr.  
|      | **Note for PCA Feature Activation:**  
|      | If you have PCA installed in the system being recovered, re-activate the PCA by executing the **PCA Activation on Entire Server** procedure on the recovered NOAM server from [6].  
|      | **Notes:**  
|      | • If not all SOAM sites are recovered at this point, then repeat the activation for each “new” SOAM site that comes online.  
|      | • If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature.  
|      | Refer to section 1.5 Optional Features to activate any features that were previously activated. |
| 73.  | **NOAM VIP GUI:** Fetch and store the database report for the newly restored data and save it  
|      | 1. Navigate to **Status & Manage > Database.**  
|      | ![Status & Manage](image)  
|      | 2. Select the active NOAM server and click **Report.**  
|      | The following screen displays:  
|      | **Main Menu: Status & Manage -> Database [Report]**  
|      | ![Database Status Report](image)  
|      | 3. Click **Save** and save the report to your local machine. |
## Procedure 1. Recovery Scenario 1

| 74 | Active NOAM: Verify replication between servers | 1. Log into the active NOAM as admusr using SSH terminal.  
2. Execute this command: |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<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 & Manager > Database**.

   ![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; 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;IP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM2</td>
<td>Network OAM&amp;IP</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM2</td>
<td>System OAM</td>
<td>N/A</td>
</tr>
<tr>
<td>ZombieNOIAM</td>
<td>ZombieNOIAM1</td>
<td>Network OAM&amp;IP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOIAM</td>
<td>ZombieSOIAM1</td>
<td>System OAM</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOIAM</td>
<td>ZombieDRNOIAM1</td>
<td>Network OAM&amp;IP</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOI</td>
<td>ZombieSOI1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOI</td>
<td>ZombieSOI2</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOI</td>
<td>ZombieSOI3</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOI</td>
<td>ZombieSOI4</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOI</td>
<td>ZombieSOI5</td>
<td>MP</td>
<td>Active</td>
</tr>
</tbody>
</table>
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th><strong>76. NOAM VIP GUI:</strong></th>
<th><strong>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.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload the backed up RADIUS key file (RADIUS only). DSR only. If SDS, skip to the next step.</td>
<td>Navigate to <strong>Status &amp; Manage &gt; Files.</strong></td>
</tr>
<tr>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Files.</strong></td>
<td>2. Select the active NOAM server tab. Click <strong>Upload</strong> and select the <strong>RADIUS shared secret encryption key</strong> file backed up after initial installation and provisioning or after key revocation execution.</td>
</tr>
<tr>
<td>2. Select the active NOAM server tab. Click <strong>Upload</strong> and select the <strong>RADIUS shared secret encryption key</strong> file backed up after initial installation and provisioning or after key revocation execution.</td>
<td>3. Click <strong>Browse.</strong></td>
</tr>
<tr>
<td>3. Click <strong>Browse.</strong></td>
<td>4. Locate the <strong>DpiKf.bin.encr</strong> file.</td>
</tr>
<tr>
<td>4. Locate the <strong>DpiKf.bin.encr</strong> file.</td>
<td>5. Click <strong>Upload.</strong></td>
</tr>
<tr>
<td>5. Click <strong>Upload.</strong></td>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
<td><strong>Note:</strong> This file should be deleted from the operator's local servers as soon as key file is uploaded to the active NOAM server.</td>
</tr>
</tbody>
</table>
Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>NOAM VIP</th>
<th>Copy and distribute RADIUS key file on active NOAM (RADIUS only) — Part 1</th>
</tr>
</thead>
<tbody>
<tr>
<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>
<td></td>
</tr>
<tr>
<td>1. Log into the active NOAM VIP as <code>admusr</code> user using SSH terminal.</td>
<td></td>
</tr>
<tr>
<td>2. Copy the key file:</td>
<td></td>
</tr>
<tr>
<td><code>$ cd /usr/TKLC/dpi/bin</code></td>
<td></td>
</tr>
<tr>
<td><code>$ ./sharedKrevo -decr</code></td>
<td></td>
</tr>
<tr>
<td><code>$ sudo rm /var/TKLC/db/filemgmt/&lt;backed up key file name&gt;</code></td>
<td></td>
</tr>
<tr>
<td>3. Make sure all servers in the topology are accessible.</td>
<td></td>
</tr>
<tr>
<td><code>$ ./sharedKrevo -checkAccess</code></td>
<td></td>
</tr>
</tbody>
</table>

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

78. **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.
[1450723211]: [INFO] Key file on Active NOAM and MD-1 are same.
[1450723211]: [INFO] NO NEED to sync key file to MD-1.
```

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

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

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

![Status and Manage](image)

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>ZombieORNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieORNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
</tbody>
</table>
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th></th>
<th>NOAM GUI: Enable provisioning</th>
</tr>
</thead>
</table>
| 80. | 1. Navigate to Status & Manage > Database.  
   |   - Status & Manage  
   |   - Network Elements  
   |   - Server  
   |   - HA  
   |   - Database  
   |   - KPIs  
   |   - Processes  
   |   - Tasks  
   |   - Files  
   |   2. Click **Enable Provisioning**.  
   |   ![Enable Provisioning](image)  
   |   ![Report](image)  
   |   ![Inhibit/](image)  
   |   3. Click **OK**. |

<table>
<thead>
<tr>
<th></th>
<th>SOAM GUI: Enable site provisioning. DSR only. If SDS, then skip to step 91.</th>
</tr>
</thead>
</table>
| 81. | 1. Navigate to Status & Manage > Database.  
   |   - Status & Manage  
   |   - Network Elements  
   |   - Server  
   |   - HA  
   |   - Database  
   |   - KPIs  
   |   - Processes  
   |   - Tasks  
   |   - Files  
   |   2. Click **Enable Site Provisioning**.  
   |   ![Enable Site Provisioning](image)  
   |   ![Report](image)  
   |   ![Inhibit/](image)  
   |   3. Click **OK**. |

<table>
<thead>
<tr>
<th></th>
<th>SOAM VIP GUI: Verify the local node information. DSR only. If SDS, then skip to step 91.</th>
</tr>
</thead>
</table>
| 82. | 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 1. Recovery Scenario 1

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **86.** | **SOAM VIP GUI:** Enable connections, if needed.  
DSR only. If SDS, then skip to step 91. |
| 1. | Navigate to **Diameter > Maintenance > Connections**. |
| 2. | Select each connection and click **Enable**. Alternatively, enable all the connections by clicking **EnableAll**.  
| 3. | Verify the Operational State is **Available**.  
**Note:** If a disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution |
| **87.** | **SOAM VIP GUI:** Enable optional features.  
DSR only. If SDS, then skip to step 91. |
| 1. | Navigate to **Diameter > Maintenance > Applications**. |
| 2. | Select the optional feature application configured in step 72. |
| 3. | Click **Enable**. |
| **88.** | **SOAM VIP GUI:** Re-enable transports, if needed.  
DSR only. If SDS, then skip to step 91. |
| 1. | Navigate to **Transport Manager > Maintenance > Transport**. |
| 2. | Select each transport and click **Enable**. |
| 3. | Verify the Operational Status for each transport is **Up**. |
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>89.</td>
<td><strong>SOAM VIP GUI:</strong> Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 91.</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to SS7/Sigtran &gt; Maintenance &gt; Local SCCP Users.</td>
</tr>
<tr>
<td></td>
<td>- SS7/Sigtran</td>
</tr>
<tr>
<td></td>
<td>- Configuration</td>
</tr>
<tr>
<td></td>
<td>- Maintenance</td>
</tr>
<tr>
<td></td>
<td>- Local SCCP Users</td>
</tr>
<tr>
<td></td>
<td>- Remote Signaling Points</td>
</tr>
<tr>
<td></td>
<td>- Remote MTP3 Users</td>
</tr>
<tr>
<td></td>
<td>- Linksets</td>
</tr>
<tr>
<td></td>
<td>- Links</td>
</tr>
<tr>
<td>2.</td>
<td>Click the Enable button corresponding to MAPIWF Application Name.</td>
</tr>
<tr>
<td></td>
<td><img src="Enable_Disable" alt="Enable Disable" /></td>
</tr>
<tr>
<td>3.</td>
<td>Verify the SSN Status is Enabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>90.</td>
<td><strong>SOAM VIP GUI:</strong> Re-enable links, if needed. DSR only. If SDS, then skip to step 91.</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to SS7/Sigtran &gt; Maintenance &gt; Links.</td>
</tr>
<tr>
<td></td>
<td>- SS7/Sigtran</td>
</tr>
<tr>
<td></td>
<td>- Configuration</td>
</tr>
<tr>
<td></td>
<td>- Maintenance</td>
</tr>
<tr>
<td></td>
<td>- Local SCCP Users</td>
</tr>
<tr>
<td></td>
<td>- Remote Signaling Points</td>
</tr>
<tr>
<td></td>
<td>- Remote MTP3 Users</td>
</tr>
<tr>
<td></td>
<td>- Linksets</td>
</tr>
<tr>
<td></td>
<td>- Links</td>
</tr>
<tr>
<td>2.</td>
<td>Click Enable for each link.</td>
</tr>
<tr>
<td></td>
<td><img src="Enable_Disable" alt="Enable Disable" /></td>
</tr>
<tr>
<td>3.</td>
<td>Verify the Operational Status for each link is Up.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>91.</td>
<td><strong>SOAM VIP GUI:</strong> Examine all alarms</td>
</tr>
<tr>
<td>1.</td>
<td>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>2.</td>
<td>Examine all active alarms and refer to the on-line help on how to address them.</td>
</tr>
<tr>
<td></td>
<td>If needed, contact My Oracle Support (MOS).</td>
</tr>
</tbody>
</table>
Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
</table>
| 92. NOAM 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). |
| 93. Restore GUI usernames and passwords | If applicable, execute the section 5 Resolve User Credential Issues after Database Restore procedure to recover the user and group information restored. |
| 94. Back up and archive all the databases from the recovered system | Execute the DSR Database Backup procedure to back up the configuration databases. |
| 95. Recover IDIH, if configured | If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH. |
| 96. SNMP workaround | Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases:  
   1. If SNMP is not configured in DSR/SDS.  
   2. If SNMP is already configured and SNMPv3 is selected as enabled version. |

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

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

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

**Procedure 2. Recovery Scenario 2**

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

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</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)

---

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

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

### 7. Recover PMAC and PMAC TVOE Host: Backups available

If PMAC is located on the failed rack mount server(s), execute this step; otherwise, skip to step 11.
This step assumes TVOE and PMAC backups are available. If backups are NOT available, skip this step.
1. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.
2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup.
3. Proceed to step 11.

### 8. Recover PMAC and PMAC TVOE Host: Backups not available

This step assumes TVOE and PMAC backups are NOT available, if the TVOE and PMAC have already been restored, **skip this step**.
1. Execute these procedures from reference [8]:
   - Install and Configure TVOE on First RMS (PMAC Host)
   - Install PMAC
   - Initialize the PMAC Application
2. Proceed to next step.

### 9. Configure PMAC: No Backup

If PMAC backup was NOT restored in step 7., execute this step; otherwise, skip this step.
Execute these procedures from reference [8]:
- Configure PMAC Server (NetBackup Only)
- Add RMS to the PMAC Inventory

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

This step assumes TVOE backups are available on any additional rack mount servers; otherwise, skip this step.
Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on additional rack mount servers.

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

If TVOE backups were NOT performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step.
1. Execute these procedures from reference [8]:
   - Install TVOE on Additional Rack Mount Servers
   - Configure TVOE on Additional Rack Mount Servers
2. Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]:
   - **HP DL380 Gen8**: Configure HP Gen 8 Server BIOS Settings
   - **Oracle X5-2/Netra X5-2/X6-2/X7-2**: Configure Oracle X5-2/Netra X5-2/X6-2/X7-2 Server BIOS Settings
   - **HP DL380 Gen9**: Configure HP Gen9 Server BIOS Settings
### Procedure 2. Recovery Scenario 2

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

- `sdsIso` (if SDS VMs are being configured)
- `NETWORK_xmi` (if DSR/SDS NOAM/DRNOAMs are being configured)
- `XMIGATEWAY` (if DSR/SDS NOAM/DRNOAMs are being configured)
- `XMISUBNETMASK` (if DSR/SDS NOAM/DRNOAMs are being configured)
- `DSRNOAM1XObjectIPADDRESS` (if DSRNOAM1 is being configured)
- `DSRNOAM2XObjectIPADDRESS` (if DSRNOAM2 is being configured)
- `DSRDRNOAM1XObjectIPADDRESS` (if DSRDRNOAM1 is being configured)
- `DSRDRNOAM2XObjectIPADDRESS` (if DSRDRNOAM2 is being configured)
- `SDSNOAM1XObjectIPADDRESS` (if SDSNOAM1 is being configured)
- `SDSNOAM2XObjectIPADDRESS` (if SDSNOAM2 is being configured)
- `SDSDRNOAM1XObjectIPADDRESS` (if SDSDRNOAM1 is being configured)
- `SDSDRNOAM2XObjectIPADDRESS` (if SDSDRNOAM2 is being configured)

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

**WARNING**

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

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

<table>
<thead>
<tr>
<th>19.</th>
<th><strong>PMAC:</strong> Execute the config.sh script</th>
</tr>
</thead>
</table>

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

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

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

**Example output:**

```
[sdmasc@1019441PMAC RMS]$ sudo ./config.sh rms.cfg
Validating cfg file...
  Successful validation of cfg file.
  Added Cabinet 101 to Fast Deployment File.
  Added Zombie_TV0E1 to Fast Deployment File.
  Added Zombie_TV0E2 to Fast Deployment File.
  Added xml(bond0.4) to Fast Deployment File.
  Added imi(bond0.3) to Fast Deployment File.
  Added rep(bond1.10) to Fast Deployment File.
  Added xsl1(bond1.6) to Fast Deployment File.
  Added xsl2(bond1.7) to Fast Deployment File.
  Added xsl3(bond1.8) to Fast Deployment File.
  Added xsl4(bond1.9) to Fast Deployment File.
  Added xsl5(bond1.10) to Fast Deployment File.
  Added xsl6(bond1.12) to Fast Deployment File.
  Added xsl7(bond1.13) to Fast Deployment File.
  Added xsl8(bond1.14) to Fast Deployment File.
  Added xsl9(bond1.15) to Fast Deployment File.
  Added xsl10(bond1.16) to Fast Deployment File.
  Added xsl11(bond1.17) to Fast Deployment File.
  Added xsl12(bond1.19) to Fast Deployment File.
  Added xsl13(bond1.19) to Fast Deployment File.
  Added xsl14(bond1.20) to Fast Deployment File.
  Added xsl15(bond1.21) to Fast Deployment File.
  Added xsl16(bond1.22) to Fast Deployment File.
  Added Zombie_DSRK0A0M1 to Fast Deployment File.
  Added Zombie_DSRK0A0M2 to Fast Deployment File.
  Added Zombie_DSRRK0A0M1 to Fast Deployment File.
  Added Zombie_DSRRK0A0M2 to Fast Deployment File.
  Added Zombie_SDK0A0M1 to Fast Deployment File.
  Added Zombie_SDK0A0M2 to Fast Deployment File.
  Added Zombie_SDSR0A0M1 to Fast Deployment File.
  Added Zombie_SDSR0A0M2 to Fast Deployment File.
  Added Zombie_SDSS0A0M1 to Fast Deployment File.
  Added Zombie_SDSS0A0M2 to Fast Deployment File.
  Added Zombie_DSFR0A0M1 to Fast Deployment File.
  Added Zombie_DSFR0A0M2 to Fast Deployment File.
  Added Zombie_DSFR1A0M1 to Fast Deployment File.
  Added Zombie_DSFR1A0M2 to Fast Deployment File.
  Added Zombie_DSFR1PP0M1 to Fast Deployment File.
  Added Zombie_DSFR1PP0M2 to Fast Deployment File.
  Added Zombie_SDSSF0V1 to Fast Deployment File.
  Added Zombie_SDSSF0V2 to Fast Deployment File.

Validating Fast Deployment File.......

Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml"
Configuration file validation successful.
Validation complete
Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml
SUCCESS: OPERATION SUCCESS!!
```

Procedure 2. Recovery Scenario 2

20. **PMAC**: Execute fast deployment

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

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

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

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

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

![Status and Manage]
- Task Monitoring
- Help
- Legal Notices
- Logout

3. Monitor the configuration to completion:

![Main Menu: Task Monitoring]

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

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

1 1 0 pmac Fast_Deployment 0 21 0 Complete 300 0 Check PM&C is available
2 1 0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet
3 1 0 pmac Fast_Deployment 0 3 melbourne_RMS3 1 Skipped 900 0 Add Rms
4 2 0 pmac Fast_Deployment 1
```

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td><strong>PMAC</strong>: Repeat for each rack mount server configuration file</td>
</tr>
<tr>
<td></td>
<td>Repeat steps 14. - 21. for each rack mount server/configuration file, if required.</td>
</tr>
<tr>
<td>23.</td>
<td><strong>PMAC</strong>: Back up FDC file</td>
</tr>
<tr>
<td></td>
<td>1. Copy the updated fdc file to the fdc backup directory:</td>
</tr>
<tr>
<td></td>
<td>```bash</td>
</tr>
<tr>
<td></td>
<td>$ sudo cp /usr/TKLC/smac/etc/RMS/&lt;fdc_file&gt; /usr/TKLC/smac/etc/fdc/</td>
</tr>
<tr>
<td></td>
<td>2. Change permissions:</td>
</tr>
<tr>
<td></td>
<td>```bash</td>
</tr>
<tr>
<td></td>
<td>$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/&lt;fdc_file&gt;</td>
</tr>
<tr>
<td>24.</td>
<td>Perform CPU pinning</td>
</tr>
<tr>
<td></td>
<td>Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only) procedure from reference [8].</td>
</tr>
<tr>
<td>25.</td>
<td><strong>NOAM GUI</strong>: Login</td>
</tr>
<tr>
<td></td>
<td>If the failed server is not OAM, then skip to step 47.</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>```bash</td>
</tr>
<tr>
<td></td>
<td>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</td>
</tr>
<tr>
<td></td>
<td>2. Login as the <code>guiadmin</code> user:</td>
</tr>
</tbody>
</table>

![Oracle System Login](image)
### Procedure 2. Recovery Scenario 2

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

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI:</th>
<th></th>
</tr>
</thead>
</table>
| 29 | Restart DSR application | 1. Navigate to **Status & Manage > Server**.  
   | |   |  
   | |   | ![Status & Manage](image)  
   | |   |   - Network Elements  
   | |   |   - Server  
   | |   |   - HA  
   | |   |   - Database  
   | |   |   - KPIs  
   | |   |   - Processes  
   | |   |   - Tasks  
   | |   |   - Files  
   | |   |  
   | | 2. Select the recovered standby NOAM server and click **Restart**.  
   | |   | ![Restart](image)  
   | |   | ![Reboot](image)  
| 30 | Recover query servers.  
   | | SDS only. If DSR, skip to step 33. | Execute the **Configuring SDS Query Servers** procedure, steps 1 and 4-7, from reference [8].
| 31 | SDS NOAM VIP GUI: Set HA on query server.  
   | | SDS only. If DSR, skip to step 33. | 1. Navigate to **Status & Manage > HA**.  
   | | | ![Status & Manage](image)  
   | | |   - Network Elements  
   | | |   - Server  
   | | |   - HA  
   | | |   - Database  
   | | |   - KPIs  
   | | |   - Processes  
   | | |   - Tasks  
   | | |   - Files  
   | | 2. Click **Edit**.  
   | | 3. Select the query server and select **Observer**.  
   | | 4. Click **OK**.  


### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>32.</td>
<td><strong>SDS NOAM VIP GUI:</strong> Restart SDS application. If SDS only, skip to step 33.</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Status &amp; Manage &gt; Server.</strong></td>
</tr>
</tbody>
</table>
|     | - Status & Manage  
|     |   - Network Elements  
|     |   - Server  
|     |   - HA  
|     |   - Database  
|     |   - KPIs  
|     |   - Processes  
|     | Select the recovered query server and click **Restart.** |

**!!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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>33.</td>
<td><strong>NOAM VIP GUI:</strong> Stop replication to the C-level servers of this site. If SDS, skip to step next step.</td>
</tr>
<tr>
<td></td>
<td><strong>!!Warning!!</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>34.</td>
<td><strong>NOAM VIP GUI:</strong> Recover active SOAM server</td>
</tr>
<tr>
<td></td>
<td>Install the SOAM servers.</td>
</tr>
</tbody>
</table>
|     | **DSR:**  
|     | Execute the **Configure the SOAM Servers** procedure, steps 1-3 and 5-9, from reference [8].  
|     | **Note:** If you are using NetBackup, also execute step 12.  
|     | **SDS:**  
|     | Execute the **Configure the SDS DP SOAM Servers** procedure, steps 1-3 and 5-8, from reference [8]. |
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Set HA on the SOAM server</th>
<th>NOAM VIP GUI: Restart DSR application</th>
</tr>
</thead>
</table>
| 35. | **1.** Navigate to **Status & Manage > HA.**

- Navigate to **Status & Manage > HA.**
- Click **Edit.**
- Select the SOA M server and set it to **Active.**
- Click **OK.**

| 36. | **1.** Navigate to **Status & Manage > Server.**

- Navigate to **Status & Manage > Server.**
- Select the recovered SOAM server and click **Restart.**

- Select the recovered SOAM server and click **Restart.** |
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 37.  | **NOAM VIP GUI:** Upload the backup SOAM database file.  
DSR only. If SDS, skip to step 42. |
| 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. |
| 3.   | Click **Browse** and locate the backup file. |
| 4.   | Mark the **This is a backup file** checkbox. |
| 5.   | Click **Open**. |
| 6.   | Click **Upload**. |

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>38.</td>
<td>Recovered SOAM GUI: Login. DSR only. If SDS, skip to step 42.</td>
</tr>
<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: <code>&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]

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

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

Copyright © 2010, 2016 Oracle and/or its affiliates. All rights reserved.
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>39.</td>
<td><strong>Recovered SOAM GUI:</strong> Verify the archive contents and database compatibility. DSR only. If SDS, skip to step 42.</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 27 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: 2
Archive: backup/Backup.DSR.Zom
```

**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** and continue to **next step** in this procedure.
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 40. | **Recovered SOAM GUI:**  
  Restore the database.  
  DSR only. If SDS, skip to step 42.  
  1. Select the Active SOAM server and click **Restore**.  
  2. Select the backup provisioning and configuration file.  
  ![Database Compare](image)  
  Archive: `backup/Backup.dsr.Z`  
  3. Click **OK**.  
  ![Database Restore Confirm](image)  
  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.  
  **Notes:**  
  - After the restore has started, the user is logged out of XMI SOAM GUI since the restored topology is old data.  
  - If the spare SOAM is in another network and is unreachable, the database restore cannot be done.  
  **Workaround:** If the spare SOAM is unreachable and ping (from recovered SOAM server to spare SOAM server) hangs (as evidenced by `ps -ef | grep ping` showing the same ping process and its child for more than 10 seconds), then kill the hung ping processes and the restore proceeds. |
| 41. | **Recovered SOAM GUI:**  
  Monitor and confirm database restoration.  
  DSR only. If SDS, skip to step 42.  
  Wait for **5-10 minutes** for the system to stabilize with the new topology:  
  Monitor the Info tab for **Success**. This indicates the restore is complete and the system is stabilized.  
  **Notes:**  
  - Do not pay attention to alarms until all the servers in the system are completely restored.  
  - The Configuration and Maintenance information is in the same state it was when backed up during initial backup. |
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>42.</th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

#### Oracle System Login

```
Log In
Enter your username and password to log in
Username: [ ]
Password: [ ]
[ ] Change password
Log In
```

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

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.</td>
<td><strong>NOAM VIP GUI:</strong> Start replication on the recovered SOAMs, if replication is inhibited. <strong>Un-Inhibit (start) replication to the recovered SOAM servers.</strong></td>
</tr>
<tr>
<td>45.</td>
<td><strong>NOAM VIP GUI:</strong> Set HA on the recovered standby SOAM server. <strong>Navigate to Status &amp; Manage &gt; Database.</strong> <strong>Set HA on the recovered standby SOAM server.</strong></td>
</tr>
<tr>
<td>5.</td>
<td>Navigate to <strong>Status &amp; Manage &gt; Database.</strong> <strong>Click Allow Replication on the recovered SOAM servers.</strong> <strong>Verify the replication on all SOAMs servers is allowed. This can be done by checking Repl status column of respective server</strong></td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Status &amp; Manage &gt; HA.</strong> <strong>Click Edit at the bottom of the screen</strong></td>
</tr>
<tr>
<td>2.</td>
<td><strong>Select the recovered standby SOAM server and set it to Active.</strong></td>
</tr>
<tr>
<td>3.</td>
<td><strong>Click OK.</strong></td>
</tr>
</tbody>
</table>
## Procedure 2. Recovery Scenario 2

| 46. | **NOAM VIP GUI:**
|     | Restart DSR application

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

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

| 47. | NOAM VIP GUI: | Start replication on working C-level servers. DSR only. If SDS, skip to next step. |
| Un-Inhibit (start) replication to the working C-level Servers which belongs to the same site as of the failed SOAM servers. |
| **If the spare SOAM is also present in the site and lost**, execute Appendix F Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost). |
| **If the spare SOAM is NOT deployed in the site**, execute Appendix D Un-Inhibit A and B Level Replication on C-level Servers. |

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

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

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

<table>
<thead>
<tr>
<th>OAM Repl Status</th>
<th>SIG Repl Status</th>
<th>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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>48.</td>
<td><strong>Activate PCA</strong>&lt;br&gt;DSR only</td>
<td>If you have PCA installed in the system being recovered, re-activate PCA by executing the <strong>PCA Activation on Entire Network</strong> procedure on the recovered standby NOAM server from [7].</td>
</tr>
</tbody>
</table>
| 49.  | **NOAM VIP GUI: Recover the C-level server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs)**<br>DSR: Execute the **Configure the MP Servers** procedure, steps 1 and 9-13, from reference [8].<br>Note: Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.<br>**SDS (Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only):**<br>Execute the **Configure the SDS DP Servers** procedure, steps 1 and 5-8, from reference [8].
Repeat this step for any remaining failed MP servers. |
| 50.  | **NOAM VIP GUI: Set HA on all C-level servers**<br>1. Navigate to **Status & Manage -> HA**.<br>2. Click **Edit**.<br>3. For each recovered C-Level with a Max Allowed HA Role set to **OOS**, set it to **Active**.<br>4. Click **OK**. |
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>51.</th>
<th>NOAM VIP GUI: Restart DSR application on the recovered C-level servers</th>
<th>1. Navigate to Status &amp; Manage &gt; Server.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Status &amp; Manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network Elements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KPIs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Processes</td>
</tr>
<tr>
<td></td>
<td>2. Select the recovered C-level servers and click Restart.</td>
<td></td>
</tr>
</tbody>
</table>
Procedure 2. Recovery Scenario 2

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

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

1. Navigate to Status & Manage > Database.

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

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

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

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

1. Establish an SSH session to the active NOAM and login as admusr.
2. Perform a keyexchange from the active NOAM to each recovered server:

   $ keyexchange admusr@<Recovered Server Hostname>

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

| 54. Active NOAM: Activate optional features. DSR only. If SDS, then skip to next step. | Establish an SSH session to the active NOAM and login as admusr. **Note for PCA Feature Activation:** If you have PCA installed in the system being recovered, re-activate the PCA by executing the **PCA Activation on Stand By 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 [6]. **Notes:**
- If not all SOAM sites are recovered at this point, then repeat the activation for each “new” SOAM site that comes online.
- If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature.

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

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

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

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]**

   ![Database Report](image)

   - From: Active Network OAM&P on host ZombieNOAM1
   - Report Version: 8.0.0.0.0.0-60.9.0
   - 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%: 558M used of 7.0G total, 6.0G available
   - Memory Utilization: 0.0%: used of total, 0M available

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

56. **Active NOAM**
   Verify replication between servers

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

   ```
   $ sudo irepstat -m
   ```

Example output:

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

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

1. Navigate to **Status & Manager > Database.**
   - **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; 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>NA</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM1</td>
<td>System OAM</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM</td>
<td>ZombieDRNOAM2</td>
<td>Network OAM&amp;P</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieISPMP2</td>
<td>MP</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSS7MP2</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSS7MP1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieIPFE1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieIPFE2</td>
<td>MP</td>
<td>Active</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Hostname</th>
<th>OAM HA Role</th>
<th>Application HA Role</th>
<th>Max Allowed HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Standby</td>
</tr>
</tbody>
</table>
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>59.</td>
<td><strong>SOAM GUI:</strong> Enable site provisioning. DSR only. If SDS, skip to step 69.</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Database.</strong>&lt;br&gt; Status &amp; Manage&lt;br&gt; - Network Elements&lt;br&gt; - Server&lt;br&gt; - HA&lt;br&gt; - Database&lt;br&gt; - KPIs&lt;br&gt; - Processes&lt;br&gt; - Tasks&lt;br&gt; - Files&lt;br&gt; 2. Click <strong>Enable Site Provisioning.</strong>&lt;br&gt; 3. A confirmation window displays. Click <strong>OK</strong> to enable provisioning.</td>
</tr>
<tr>
<td>60.</td>
<td><strong>SOAM VIP GUI:</strong> Verify local node information. DSR only. If SDS, skip to step 69.</td>
</tr>
</tbody>
</table>
|      | 1. Navigate to **Diameter > Configuration > Local Node.**
|      | 2. Verify all the local nodes are shown. |
| 61.  | **SOAM VIP GUI:** Verify the peer node information. DSR only. If SDS, then skip to step 69. |
|      | 1. Navigate to **Diameter > Configuration > Peer Node.**
|      | 2. Verify all the peer nodes are shown. |
### Procedure 2. Recovery Scenario 2

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

65. **SOAM VIP GUI:**
    Enable optional features.
    DSR only. If SDS, then skip to step 69.
    1. Navigate to **Diameter > Maintenance > Applications**.
    2. Select the optional feature application configured in step 72.
    3. Click **Enable**.

66. **SOAM VIP GUI:**
    Re-enable transports, if needed.
    DSR only. If SDS, then skip to step 69.
    1. Navigate to **Transport Manager > Maintenance > Transport**.
    2. Select each transport and click **Enable**.
    3. Verify the Operational Status for each transport is **Up**.

67. **SOAM VIP GUI:**
    Re-enable MAPIWF application, if needed.
    DSR only. If SDS, then skip to step 69.
    1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.
    2. Click the **Enable** button corresponding to MAPIWF Application Name.
    3. Verify the SSN Status is **Enabled**.
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>68.</td>
<td><strong>SOAM VIP GUI:</strong></td>
<td>Re-enable links, if needed. DSR only. If SDS, then skip to step 69.</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>SS7/Sigtran &gt; Maintenance &gt; Links.</strong></td>
<td>![Diagram of SOAM VIP GUI]</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Enable</strong> for each link.</td>
<td>![Enable/Disable buttons]</td>
</tr>
<tr>
<td>2.</td>
<td>Verify the Operational Status for each link is <strong>Up.</strong></td>
<td></td>
</tr>
<tr>
<td>69.</td>
<td><strong>SOAM VIP GUI:</strong></td>
<td>Examine all alarms</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Alarms &amp; Events &gt; View Active.</strong></td>
<td>![Diagram of SOAM VIP GUI]</td>
</tr>
<tr>
<td>2.</td>
<td>Examine all active alarms and refer to the on-line help on how to address them.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If needed, contact My Oracle Support (MOS).</td>
<td></td>
</tr>
<tr>
<td>70.</td>
<td><strong>NOAM VIP GUI:</strong></td>
<td>Examine all alarms</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Alarms &amp; Events &gt; View Active.</strong></td>
<td>![Diagram of NOAM VIP GUI]</td>
</tr>
<tr>
<td>2.</td>
<td>Examine all active alarms and refer to the on-line help on how to address them.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If needed, contact My Oracle Support (MOS).</td>
<td></td>
</tr>
</tbody>
</table>
## Procedure 2. Recovery Scenario 2

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

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

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

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

Example output:

```bash
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
```

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

Example output:
**Procedure 2. Recovery Scenario 2**

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>73.</td>
<td>Back up and archive all the databases from the recovered system</td>
</tr>
<tr>
<td>74.</td>
<td>Recover IDIH</td>
</tr>
</tbody>
</table>

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

- Execute Appendix A DSR Database Backup to back up the Configuration databases.
- If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.

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

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

- Recover **Active NOAM** server by recovering base hardware, software, and the database
  - Recover the base hardware
  - Recover the software
  - Recover the database
- Recover **NOAM servers** by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover **Query Server** (if needed) by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover any failed **SOAM and MP/DP servers** by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
Database is already intact at one SOAM server and does not require restoration at the other SOAM and MP/DP servers.

- Recover IDIH if necessary

**Procedure 3. Recovery Scenario 3**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Gather required materials</td>
</tr>
<tr>
<td>2.</td>
<td>Create a backup directory, if needed</td>
</tr>
<tr>
<td>3.</td>
<td>Replace failed equipment</td>
</tr>
</tbody>
</table>
| 4.     | Recover PMAC and PMAC TVOE Host: Configure BIOS settings and update firmware | 1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:
   - HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings
   - HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings
   2. Verify and/or upgrade server firmware by executing the Upgrade Rack Mount Server Firmware procedure from reference [8]. |
| 5.     | PMAC, TVOE Hosts, and Switch Recovery: Backups available | This step assumes TVOE and PMAC backups are available. If backups are NOT available, skip this step.
   1. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.
   2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup.
   3. Proceed to step 7. |
| 6.     | PMAC, TVOE Hosts, and Switch Recovery: Backups NOT available | This step assumes TVOE and PMAC backups are NOT available. If the TVOE and PMAC have already been restored, skip this step.
   1. Execute the Install and Configure TVOE on First RMS (PMAC Host) procedure from reference [8].
   2. Execute the Install PMAC procedure from reference [8].
   3. Execute the Initialize the PMAC Application section from reference [8]. |
### Procedure 3. Recovery Scenario 3

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

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC:</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 13.  | PMAC: | Determine if the fdconfig file exists from the initial deployment | 1. Type:  
```
[admusr@melbourne-pmac-1 ~]$ ll /usr/TKLC/smac/etc/fdc/
```
2. Examine the results and verify if the `rms config file <hostname>.cfg` exists.  

**Note:** There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS. |
| 14.  | Create fdconfig backup file, if it does not already exist | Execute this step ONLY if the fdconfig backup file does NOT exist.  
1. Create the needed file(s) by executing the *Virtual Machine/Network Fast Deployment* section from reference [8].  

**WARNING**  
It is very important to ensure the file(s) created only affects the TVOE server(s) and the guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.  
2. Skip to step 23. if this step was executed. |
| 15.  | PMAC: | Load ISOs into PMAC, if not done already | If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the *Virtual Machine/Network Fast Deployment* section from reference [8]. |
| 16.  | PMAC: | Edit/Update configuration file | Edit the fdconfig file to include only the required/failed servers.  

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

The following items are mandatory:  
- `siteName`  
- `tpdIso`  
- `dsrIso` (if DSR VMs are being configured)  
- `sdsIso` (if SDS VMs are being configured)  
- `NETWORK_xmi` (if DSR/SDS NOAM/DRNOAMs are being configured)  
- `XMIGATEWAY` (if DSR/SDS NOAM/DRNOAMs are being configured)  
- `XMISUBNETMASK` (if DSR/SDS NOAM/DRNOAMs are being configured)  
- `DSRNOAM1XMIPADDRESS` (if DSRNOAM1 is being configured)  
- `DSRNOAM2XMIPADDRESS` (if DSRNOAM2 is being configured)  
- `DSRDRNOAM1XMIPADDRESS` (if DSRDRNOAM1 is being configured)  
- `DSRDRNOAM2XMIPADDRESS` (if DSRDRNOAM2 is being configured) |
### Procedure 3. Recovery Scenario 3

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
|   | • SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured)  
   | • SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured)  
   | • SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured)  
   | • SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured)  

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

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

<table>
<thead>
<tr>
<th>17.</th>
<th><strong>PMAC:</strong> Copy the backed up fdc file to the RMS directory</th>
</tr>
</thead>
</table>

Copy the fdconfig backup file to the RMS directory.  

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.</td>
<td><strong>PMAC:</strong> Execute the <code>config.sh</code> script</td>
</tr>
</tbody>
</table>

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

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

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

Example output:

```
[admasc@b010641 PMAC RMS]$ sudo ./config.sh rms.cfg
Validating cfg file...
Successful validation of cfg file.
Added Cabinet 101 to Fast Deployment File.
Added Zombie_TVOE1 to Fast Deployment File.
Added Zombie_TVOE2 to Fast Deployment File.
Added xml(bond0.4) to Fast Deployment File.
Added imi(bond0.3) to Fast Deployment File.
Added rep(bond1.10) to Fast Deployment File.
Added xsl1(bond1.6) to Fast Deployment File.
Added xsl2(bond1.7) to Fast Deployment File.
Added xsl3(bond1.8) to Fast Deployment File.
Added xsl4(bond1.9) to Fast Deployment File.
Added xsl5(bond1.10) to Fast Deployment File.
Added xsl6(bond1.11) to Fast Deployment File.
Added xsl7(bond1.12) to Fast Deployment File.
Added xsl8(bond1.13) to Fast Deployment File.
Added xsl9(bond1.14) to Fast Deployment File.
Added xsl10(bond1.15) to Fast Deployment File.
Added xsl11(bond1.16) to Fast Deployment File.
Added xsl12(bond1.17) to Fast Deployment File.
Added xsl13(bond1.18) to Fast Deployment File.
Added xsl14(bond1.19) to Fast Deployment File.
Added xsl15(bond1.20) to Fast Deployment File.
Added xsl16(bond1.21) to Fast Deployment File.
Added Zombie_DSROAM1 to Fast Deployment File.
Added Zombie_DSROAM2 to Fast Deployment File.
Added Zombie_DSROAM3 to Fast Deployment File.
Added Zombie_DSROAM4 to Fast Deployment File.
Added Zombie_DSROAM5 to Fast Deployment File.
Added Zombie_DSROAM6 to Fast Deployment File.
Adding Fast Deployment File......
Validation configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml"
Configuration file validation successful.
Validation complete
Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml
SUCCESS: OPERATION SUCCESS!!
[admasc@b010641 PMAC RMS]$ 
```
Procedure 3. Recovery Scenario 3

19. **PMAC**: Execute fast deployment

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

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

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

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

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

   ![Status and Manage](image)

   ![Task Monitoring](image)

   ![Help](image)

   ![Legal Notices](image)

   ![Logout](image)

   3. Monitor the configuration to completion:

   ![Main Menu: Task Monitoring](image)

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

   ```
   [admusr@melbourne-pmac-1 fdconfig]$ sudo fdconfig dumpsteps --file=deploy_melbourne_20170329T202458_701b.fdcdb
   Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb"
   Here are the steps that were generated
   ------------------------ begin ------------------------
   Dump of DB steps:
   NUM PHS DLY INFRA ID SVRTYPE CMD ELEMENT PRE STATE TO BGTS COMMAND TEXT
   ---------------------------------------------------------------------------------------------------------------------
   1 1 0 pmac Fast_Deployment 0 21 0 Complete 300 0 Check PM&C is available
   2 1 0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet
   3 1 0 pmac Fast_Deployment 0 3 melbourne_RMS3 1 Skipped 900 0 Add Rms
   4 2 0 pmac Fast_Deployment 1
   ```

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>21.</td>
<td>PMAC: Repeat for each rack mount server configuration file</td>
<td>Repeat steps 13.-20. for each rack mount server/configuration file, if required.</td>
</tr>
</tbody>
</table>
| 22.  | PMAC: Back up FDC file | 1. Copy the updated fdc file to the fdc backup directory:  
\[
\text{\$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file>}
\text{/usr/TKLC/smac/etc/fdc/}
\]  
2. Change permissions:  
\[
\text{\$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/<fdc_file>}
\] |
| 23.  | Perform CPU pinning | Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only) procedure from reference [8]. |
| 24.  | Obtain latest database backup and network configuration data | 1. Obtain the most recent database backup file from external backup sources (for example, file servers) or tape backup sources.  
2. Obtain most recent RADIUS shared secret encryption key from the DpiKf.bin.encr file on external backup sources (only when the RADIUS key revocation MOP has been executed on the system).  
3. From required materials list in the Required Materials section, use the site survey documents and Network Element report (if available) to determine network configuration data. |
| 25.  | Execute DSR installation procedure for the first NOAM | Verify the networking data for network elements.  
**Notes**  
- Use the backup copy of network configuration data and site surveys from step 2.  
- SDS disaster recovery actions can and should be worked simultaneously to allow faster recovery of the complete solution (that is, stale DB on DP servers do not receive updates until SDS-SOAM servers are recovered). The following steps accommodate both DSR and SDS disaster recovery steps.  
**Important:** While creating the first NOAMs in this step, it is important that the server hostname is the same as one of the NOAM hostnames used prior to the disaster.  
DSR:  
1. Configure the first NOAM server by executing the **Configure First NOAM NE and Server** procedure from reference [8].  
2. Configure the NOAM server group by executing the **Configure the NOAM Server Group** procedure from reference [8].  
SDS:  
3. Configure the first SDS NOAM server by executing **Configure First SDS NOAM NE and Server** procedure from reference [8].  
4. Configure the SDS NOAM server group by executing the **Configure the SDS NOAM Server Group** procedure from reference [8].  
5. Skip to step 31. |
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th></th>
<th>NOAM GUI:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Login</td>
</tr>
<tr>
<td></td>
<td>DSR only. If SDS, skip to step 31. If the failed server is not OAM, then skip to step 37.</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)

   Welcome to the Oracle System Login.

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

   Unauthorized access is prohibited.

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

   Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.
Procedure 3. Recovery Scenario 3

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

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

   - **Status & Manage**
     - **Files**

2. Select the active NOAM server.

   - **Main Menu: Status & Manage -> Files**

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

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

5. Click **Open.**

6. Mark the **This is a backup file** checkbox.

7. Click **Upload.**

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

28. **NOAM GUI:**

   - Disable provisioning. DSR only. If SDS, skip to step 31.

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

2. Click **Disable Provisioning.**

3. Click **OK** to disable Provisioning.

   Disable provisioning.
   Are you sure?

   - **OK**
   - **Cancel**
**Procedure 3. Recovery Scenario 3**

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

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

![Database Archive Compare](image)

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

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

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

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

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

3. Select the proper 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**

Neutral 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.

6. Go to step 37.
### Procedure 3. Recovery Scenario 3

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>37.</td>
<td><strong>NOAM VIP GUI: Login</strong></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 <strong>guiadmin</strong> user:</td>
</tr>
</tbody>
</table>

![Oracle System Login](image_url)

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

Unauthorized access is prohibited.

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>38.</td>
<td><strong>NOAM VIP GUI: Monitor and confirm database restore</strong></td>
</tr>
<tr>
<td></td>
<td>1. Wait for <strong>5-10 minutes</strong> for the system to stabilize with the new topology:</td>
</tr>
<tr>
<td></td>
<td>2. Monitor the Info tab for <strong>Success</strong>. This indicates the restore is complete and the system is stabilized.</td>
</tr>
<tr>
<td></td>
<td>Ignore these alarms for NOAM and MP servers until all the servers are configured:</td>
</tr>
<tr>
<td></td>
<td>- Alarms with Type Column as <strong>REPL, COLL, HA</strong> (with mate NOAM), <strong>DB</strong> (about Provisioning Manually Disabled).</td>
</tr>
<tr>
<td></td>
<td><strong>Notes:</strong></td>
</tr>
<tr>
<td></td>
<td>- Do not pay attention to alarms until all the servers in the system are completely restored.</td>
</tr>
<tr>
<td></td>
<td>- The Configuration and Maintenance information is in the same state it was when backed up during initial backup.</td>
</tr>
</tbody>
</table>
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>39.</td>
<td><strong>Active NOAM:</strong> Set failed servers to OOS</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. Set the Max Allowed HA Role option to <strong>OOS</strong> for the failed servers.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>40.</td>
<td><strong>NOAM VIP GUI:</strong> Recover standby NOAM</td>
</tr>
<tr>
<td></td>
<td>Install the second NOAM server:</td>
</tr>
<tr>
<td></td>
<td><strong>DSR:</strong></td>
</tr>
<tr>
<td></td>
<td>Execute the <strong>Configure the Second NOAM Server</strong> procedure, steps 1, 3-6, from reference [8].</td>
</tr>
<tr>
<td></td>
<td><strong>SDS:</strong></td>
</tr>
<tr>
<td></td>
<td>Execute the <strong>Configure the Second SDS NOAM Server</strong> procedure, steps 1, 3-6, from reference [8].</td>
</tr>
<tr>
<td>41.</td>
<td><strong>Install NetBackup client (optional)</strong></td>
</tr>
<tr>
<td></td>
<td>If NetBackup is used, execute the <strong>Install NetBackup Client (Optional)</strong> procedure from reference [8].</td>
</tr>
</tbody>
</table>
Procedure 3. Recovery Scenario 3

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

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

   ![Diagram](image)

2. Click **Edit.**

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

4. Click **OK.**

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

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

   ![Diagram](image)

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

<table>
<thead>
<tr>
<th></th>
<th>Active NOAM: Correct the recognized authority table</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.</td>
<td>Establish an SSH session to the active NOAM and login as <code>admusr</code>.</td>
</tr>
<tr>
<td></td>
<td>Execute this command:</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo top.setPrimary</code></td>
</tr>
<tr>
<td></td>
<td><code>- Using my cluster: A1789</code></td>
</tr>
<tr>
<td></td>
<td><code>- Updating A1789.022: &lt;DSR_NOAM_B_hostname&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>- Updating A1789.144: &lt;DSR_NOAM_A_hostname&gt;</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Perform Keyexchange with remote import server. SDS only. If DSR, skip to step 47.</th>
</tr>
</thead>
<tbody>
<tr>
<td>45.</td>
<td>Navigate to SDS &gt; Configuration &gt; Options.</td>
</tr>
<tr>
<td></td>
<td>Unmark the <strong>Remote Import Enabled</strong> checkbox.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Navigate to SDS &gt; Configuration &gt; Options again to clear the banner.</td>
</tr>
<tr>
<td></td>
<td>Enter the <strong>Remote Import Password</strong>.</td>
</tr>
<tr>
<td></td>
<td>Enter the <strong>Remote Import Password</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Navigate to SDS &gt; Configuration &gt; Options again to clear the banner.</td>
</tr>
<tr>
<td></td>
<td>Mark the <strong>Remote Import Enabled</strong> checkbox.</td>
</tr>
</tbody>
</table>
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>NOAM VIP GUI:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>46.</td>
<td>Repeat for remote export server. SDS only. If DSR, skip to step 47.</td>
<td>Repeat step 45. for the remote export server.</td>
</tr>
</tbody>
</table>
| 47.  | Perform Keyexchange with export server | **1.** Navigate to *Administration > Remote Servers > Data Export.*  
   - **2.** Click *SSH Key Exchange.*  
   - **3.** Type the *Password* and click *OK.*  
   - **4.** Execute the *Configuring SDS Query Servers* procedure, steps 1, 4-7, from reference [8]. |
| 48.  | Recover query servers. SDS only. If DSR, skip to step 51. | |

**Image:**
- Diagram showing navigation through NOAM VIP GUI and SSH Key Exchange.
## Procedure 3. Recovery Scenario 3

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

52. NOAM VIP GUI: Set HA on SOAM server
   1. Navigate to Status & Manage > HA.
   2. Click Edit.
   3. Select the SOAM server and set it to Active.

<table>
<thead>
<tr>
<th>ZombieSOAM1</th>
<th>Active</th>
<th>The rr</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieSOAM2</td>
<td>Standby Spare Observer OOS</td>
<td>The rr</td>
</tr>
</tbody>
</table>

4. Click OK.

53. NOAM VIP GUI: Set HA on the SOAM server
   1. Navigate to Status & Manage > HA.
   2. Click Edit.
   3. Select the SOAM server and set it to Active.

<table>
<thead>
<tr>
<th>ZombieSOAM1</th>
<th>Active</th>
<th>The rr</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieSOAM2</td>
<td>Standby Spare Observer OOS</td>
<td>The rr</td>
</tr>
</tbody>
</table>

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

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

57. **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**.

58. **NOAM VIP GUI: Restart DSR application on recovered C-level servers**

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

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

1. Establish an SSH session to the active NOAM, login as **admusr**.
2. Perform a keyexchange from the active NOAM to each recovered server:
   
   ```bash
   $ keyexchange admusr@<Recovered Server Hostname>
   ```
   
   **Note:** If an export server is configured, perform this step.
**Procedure 3. Recovery Scenario 3**

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

<table>
<thead>
<tr>
<th>61.</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.**

   ![Status & Manage]

   The following screen displays:

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

   ![Database Status Report]

   - From: Active Network ONH6P on host ZombieNOAM1
   - Report Version: 5.6.0.0.0-30.9.0
   - User: quadmin

   ---

   **General**

   - Hostname: ZombieNOAM1
   - Database Birthday: 2016-07-11 11:21:59 EDT
   - AppWorks Database Version: 6.0
   - Application Database Version:

   ---

   **Capacities and Utilization**

   - Disk Utilization: 8.4% used of 7.0G total, 6.0G available
   - Memory Utilization: 0.0% used of total, 0K available

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

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

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

   ```
   $ sudo irepstat -m
   ```

**Example output:**

```- Policy 0 ActStb [DbReplication] ---------------

Oahu-DAMP-1 -- Active
   BC From Oahu-SOAM-2 Active 0 0.50 ^0.15%cpu 25B/s A=me
   CC To Oahu-DAMP-2 Active 0 0.10 0.14%cpu 25B/s A=me

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

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

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

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

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

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

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

irepstat ( 40 lines) (h)elp (m)erged
```
Procedure 3. Recovery Scenario 3

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

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

   ![Status & Manage](image)

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

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

<table>
<thead>
<tr>
<th>Network Element</th>
<th>Server</th>
<th>Role</th>
<th>OAM Max HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieDRNNOAM</td>
<td>ZombieDRNNOAM1</td>
<td>Network OAM&amp;MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM</td>
<td>ZombieNOAM2</td>
<td>Network OAM&amp;MP</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;MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSOAM1</td>
<td>System OAM</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNNOAM</td>
<td>ZombieDRNNOAM2</td>
<td>Network OAM&amp;MP</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieDMP2</td>
<td>MP</td>
<td>Standby</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSS7MP2</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieSS7MP1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieIPFE1</td>
<td>MP</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM</td>
<td>ZombieIPFE2</td>
<td>MP</td>
<td>Active</td>
</tr>
</tbody>
</table>

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

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

   ![Status & Manage](image)

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

2. Select the row for all of the servers.

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

<table>
<thead>
<tr>
<th>Hostname</th>
<th>OAM HA Role</th>
<th>Application HA Role</th>
<th>Max Allowed HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Standby</td>
</tr>
</tbody>
</table>
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 65.  | NOAM GUI: Enable provisioning | **NOAM GUI:** Enable provisioning  
1. Navigate to **Status & Manage > Database.**  
   - **Status & Manage**  
     - **Network Elements**  
     - **Server**  
     - **HA**  
     - **Database**  
     - **KPIs**  
     - **Processes**  
     - **Tasks**  
     - **Files**  
   2. Click **Enable Provisioning.**  
   3. Click **OK.** |
| 66.  | SOAM GUI: Enable site provisioning | **SOAM GUI:** Enable site provisioning.  
   **DSR** only. If **SDS,** then skip to step 75.  
1. Navigate to **Status & Manage > Database.**  
   2. Click **Enable Site Provisioning.**  
   3. Click **OK.** |
| 67.  | SOAM VIP GUI: Verify the peer node information | **SOAM VIP GUI:** Verify the peer node information.  
   **DSR** only. If **SDS,** then skip to step 75.  
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>Task Description</th>
</tr>
</thead>
</table>
| **68.** | **SOAM VIP GUI:** Verify the connections information.  
DSR only. If SDS, then skip to step 75. |
| **1.** | Navigate to **Diameter > Configuration > Connections.** |
| |  
| | **Diameter**  
| | **Configuration**  
| | **Capacity Summary**  
| | **Connection Capacity Dash**  
| | **Application Ids**  
| | **CEX Parameters**  
| | **Command Codes**  
| | **Configuration Sets**  
| | **Local Nodes**  
| | **Peer Nodes**  
| | **Peer Node Groups**  
| | **Connections**  
| |  
| | **2.** Verify all the connections are shown. |
| **69.** | **MP Servers:** Disable SCTP Auth Flag (DSR only).  
DSR only. If SDS, then skip to step 75.  
For SCTP connections without DTLS enabled, refer to the **Enable/Disable DTLS (SCTP Diameter Connections Only)** section in reference [8]. |
| | Execute this procedure on all failed MP servers. |
| **70.** | **SOAM VIP GUI:** Enable connections, if needed.  
DSR only. If SDS, then skip to step 75. |
| **1.** | Navigate to **Diameter > Maintenance > Connections.** |
| |  
| | **Maintenance**  
| | **Route Lists**  
| | **Route Groups**  
| | **Peer Nodes**  
| | **Connections**  
| |  
| | **2.** Select each connection and click **Enable.** Alternatively, enable all the connections by clicking **EnableAll.** |
| |  
| | **3.** Verify the Operational State is **Available.**  
**Note:** If a disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution.
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>SOAM VIP GUI: Enable optional features. DSR only. If SDS, then skip to step 75.</th>
<th>SOAM VIP GUI: Re-enable transports, if needed. DSR only. If SDS, then skip to step 75.</th>
<th>SOAM VIP GUI: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 75.</th>
</tr>
</thead>
<tbody>
<tr>
<td>71.</td>
<td>1. Navigate to <strong>Diameter &gt; Maintenance &gt; Applications</strong>. &lt;br&gt;   - Maintenance &lt;br&gt;   - Route Lists &lt;br&gt;   - Route Groups &lt;br&gt;   - Peer Nodes &lt;br&gt;   - Connections &lt;br&gt;   - Egress Throttle Groups &lt;br&gt;   - Applications &lt;br&gt;   2. Select the optional feature application configured in step 60. &lt;br&gt;   3. Click <strong>Enable</strong>. &lt;br&gt;     ![Enable, Disable] &lt;br&gt;     □ Pause updates</td>
<td>1. Navigate to <strong>Transport Manager &gt; Maintenance &gt; Transport</strong>. &lt;br&gt;   - Transport Manager &lt;br&gt;   - Configuration &lt;br&gt;   - Maintenance &lt;br&gt;     - Transport &lt;br&gt;   2. Select each transport and click <strong>Enable</strong>. &lt;br&gt;     ![Enable, Disable, Block]</td>
<td>1. Navigate to <strong>SS7/Sigtran &gt; Maintenance &gt; Local SCCP Users</strong>. &lt;br&gt;   - SS7/Sigtran &lt;br&gt;   - Configuration &lt;br&gt;   - Maintenance &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 &lt;br&gt;   2. Click the <strong>Enable</strong> button corresponding to MAPIWF Application Name. &lt;br&gt;     ![Enable, Disable]</td>
</tr>
<tr>
<td>72.</td>
<td>1. Navigate to <strong>Diameter &gt; Maintenance &gt; Applications</strong>. &lt;br&gt;   - Maintenance &lt;br&gt;   - Route Lists &lt;br&gt;   - Route Groups &lt;br&gt;   - Peer Nodes &lt;br&gt;   - Connections &lt;br&gt;   - Egress Throttle Groups &lt;br&gt;   - Applications &lt;br&gt;   2. Select the optional feature application configured in step 60. &lt;br&gt;   3. Click <strong>Enable</strong>. &lt;br&gt;     ![Enable, Disable] &lt;br&gt;     □ Pause updates</td>
<td>1. Navigate to <strong>Transport Manager &gt; Maintenance &gt; Transport</strong>. &lt;br&gt;   - Transport Manager &lt;br&gt;   - Configuration &lt;br&gt;   - Maintenance &lt;br&gt;     - Transport &lt;br&gt;   2. Select each transport and click <strong>Enable</strong>. &lt;br&gt;     ![Enable, Disable, Block]</td>
<td>2. Verify the Operational Status for each transport is <strong>Up</strong>.</td>
</tr>
<tr>
<td>73.</td>
<td>1. Navigate to <strong>Diameter &gt; Maintenance &gt; Applications</strong>. &lt;br&gt;   - Maintenance &lt;br&gt;   - Route Lists &lt;br&gt;   - Route Groups &lt;br&gt;   - Peer Nodes &lt;br&gt;   - Connections &lt;br&gt;   - Egress Throttle Groups &lt;br&gt;   - Applications &lt;br&gt;   2. Select the optional feature application configured in step 60. &lt;br&gt;   3. Click <strong>Enable</strong>. &lt;br&gt;     ![Enable, Disable] &lt;br&gt;     □ Pause updates</td>
<td>1. Navigate to <strong>Transport Manager &gt; Maintenance &gt; Transport</strong>. &lt;br&gt;   - Transport Manager &lt;br&gt;   - Configuration &lt;br&gt;   - Maintenance &lt;br&gt;     - Transport &lt;br&gt;   2. Select each transport and click <strong>Enable</strong>. &lt;br&gt;     ![Enable, Disable, Block]</td>
<td>3. Verify the SSN Status is <strong>Enabled</strong>.</td>
</tr>
</tbody>
</table>
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>74.</td>
<td><strong>SOAM VIP GUI:</strong> Re-enable links, if needed. DSR only. If SDS, then skip to step 75.</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to SS7/Sigtran &gt; Maintenance &gt; Links.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Enable</strong> for each link.</td>
</tr>
<tr>
<td>3.</td>
<td>Verify the Operational Status for each link is <strong>Up</strong>.</td>
</tr>
<tr>
<td>75.</td>
<td><strong>NOAM VIP:</strong> Verify all servers in topology are accessible (RADIUS only)</td>
</tr>
<tr>
<td>1.</td>
<td>Establish an SSH session to the NOAM VIP and login as admusr.</td>
</tr>
<tr>
<td>2.</td>
<td>Check if all the servers in the topology are accessible:</td>
</tr>
<tr>
<td><strong>Example output:</strong></td>
<td></td>
</tr>
</tbody>
</table>

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

**Note:** If any server is not accessible, stop and contact My Oracle Support (MOS).
Procedure 3. Recovery Scenario 3

| 76. SOAM VIP: Copy key file to all the servers in topology (RADIUS only) | If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.  
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).  
2. Login as admusr.  
3. Check if the existing key file on active SOAM server is valid:  
   
   ```
   $ cd /usr/TKLC/dpi/bin/
   $ ./sharedKrevo --validate
   ```  
   **Note:** If output of above command shows that existing key file is not valid, contact My Oracle Support (MOS).  
4. Establish an SSH session to the active NOAM, login as admusr.  
5. Copy the key file to active NOAM:  
   
   ```
   $ cd /usr/TKLC/dpi/bin/
   $ ./sharedKrevo --copyKey --destServer <Active NOAM server name>
   ``` |
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th></th>
<th><strong>NOAM VIP:</strong> Copy key file to all the servers in topology (RADIUS only)</th>
</tr>
</thead>
</table>
| 77. | 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:**  
   | ![Example output](image1)  
   | $ ./sharedKrevo -updateData  
   | **Example output:**  
   | ![Example output](image2)  

<table>
<thead>
<tr>
<th></th>
<th><strong>SOAM VIP GUI:</strong> Examine all alarms</th>
</tr>
</thead>
</table>
| 78. | 1. Navigate to Alarms & Events &gt; View Active.  
   | ![Alarms & Events](image3)  
   | 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>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>79.</td>
<td>NOAM VIP GUI: Examine all alarms</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to Alarms &amp; Events &gt; View Active.</td>
</tr>
<tr>
<td></td>
<td>- 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. If needed, contact My Oracle Support (MOS).</td>
</tr>
<tr>
<td>80.</td>
<td>Back up and archive all the databases from the recovered system</td>
</tr>
<tr>
<td></td>
<td>Execute the DSR Database Backup procedure to back up the configuration databases.</td>
</tr>
<tr>
<td>81.</td>
<td>Recover IDIH, if configured</td>
</tr>
<tr>
<td></td>
<td>If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.</td>
</tr>
<tr>
<td>82.</td>
<td>SNMP workaround</td>
</tr>
<tr>
<td></td>
<td>Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases:</td>
</tr>
<tr>
<td></td>
<td>1. If SNMP is not configured in DSR/SDS.</td>
</tr>
<tr>
<td></td>
<td>2. If SNMP is already configured and SNMPv3 is selected as enabled version.</td>
</tr>
</tbody>
</table>

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

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

- Recover standby NOAM server by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover Query Server (if needed) by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
- Recover Standby SOAM server by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
- Recover MP/DP C-level servers by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
- Recover IDIH if necessary

### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Workarounds</td>
<td>This procedure performs recovery if at least one NOAM server is intact and available and 1 SOAM server is intact and available. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td>
</tr>
<tr>
<td>2. Gather required materials</td>
<td>Gather the documents and required materials listed in Required Materials.</td>
</tr>
<tr>
<td>3. Replace failed equipment</td>
<td>Work with the hardware vendor to replace the failed equipment.</td>
</tr>
</tbody>
</table>
| 4. 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)
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td><strong>Active NOAM</strong>: Set failed servers to OOS</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><strong>Network Elements</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Server</strong></td>
</tr>
<tr>
<td></td>
<td><strong>HA</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Database</strong></td>
</tr>
<tr>
<td></td>
<td><strong>KPIs</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Processes</strong></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Set the Max Allowed HA Role option to <strong>OOS</strong> for the failed servers.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>6</td>
<td><strong>Recover PMAC and PMAC TVOE Host</strong>: Configure BIOS settings and update firmware</td>
</tr>
<tr>
<td></td>
<td>1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:</td>
</tr>
<tr>
<td></td>
<td>- <strong>HP DL380 Gen8</strong>: Configure HP Gen 8 Server BIOS Settings</td>
</tr>
<tr>
<td></td>
<td>- <strong>Oracle X5-2/Netra X5-2/X6-2/X7-2</strong>: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings</td>
</tr>
<tr>
<td></td>
<td>- <strong>HP DL380 Gen9</strong>: Configure HP Gen9 Server BIOS Settings</td>
</tr>
<tr>
<td></td>
<td>2. Verify and/or upgrade server firmware by executing the <strong>Upgrade Rack Mount Server Firmware</strong> procedure from reference [8].</td>
</tr>
</tbody>
</table>
**Procedure 4. Recovery Scenario 4**

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

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

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

Copy the fdconfig backup file to the RMS directory.

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

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

### WARNING

Ensure the file(s) created only affect the TVOE server(s) and guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 18   | **PMAC:** Execute the `config.sh` script | Execute `config.sh` against the modified backup config file. *Note:* If the below command is executed on multiple `cfg` files, it overwrites the existing `xml` file. Rename the `xml` file before running the command again.  

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

**Example output:**

```
Validating cfg file...  
Successful validation of cfg file.  
Added Cabinet 101 to Fast Deployment File.  
Added Zombie_TV0EZ1 to Fast Deployment File.  
Added Zombie_TV0EZ2 to Fast Deployment File.  
Added xml (bond0.4) to Fast Deployment File.  
Added ini (bond0.3) to Fast Deployment File.  
Added rep (bond1.10) to Fast Deployment File.  
Added xml (bond1.6) to Fast Deployment File.  
Added xml (bond1.7) to Fast Deployment File.  
Added xml (bond1.8) to Fast Deployment File.  
Added xml (bond1.9) to Fast Deployment File.  
Added xml (bond1.11) to Fast Deployment File.  
Added xml (bond1.12) to Fast Deployment File.  
Added xml (bond1.13) to Fast Deployment File.  
Added xml (bond1.14) to Fast Deployment File.  
Added xml (bond1.15) to Fast Deployment File.  
Added xml (bond1.16) to Fast Deployment File.  
Added xml (bond1.17) to Fast Deployment File.  
Added xml (bond1.18) to Fast Deployment File.  
Added xml (bond1.19) to Fast Deployment File.  
Added xml (bond1.20) to Fast Deployment File.  
Added xml (bond1.21) to Fast Deployment File.  
Added xml (bond1.22) to Fast Deployment File.  
Added Zombie_DSRRVan1 to Fast Deployment File.  
Added Zombie_DSRRVan2 to Fast Deployment File.  
Added Zombie_DSRRVanAM1 to Fast Deployment File.  
Added Zombie_DSRRVanAM2 to Fast Deployment File.  
Validating Fast Deployment File......  
Validation configuration file: "Zombie_DSRR_Fast_Deployment_06-15-16.xml"  
Configuration file validation successful.  
Validation complete  
```
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command/Action</th>
</tr>
</thead>
</table>
| 19.  | **PMAC**: Execute fast deployment | With the file generated from the config.sh script, execute the following command to start fast deployment:  

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command/Action</th>
</tr>
</thead>
</table>
| 20.  | **PMAC GUI**: Monitor the configuration | 1. If not already done, establish a GUI session on the PMAC server.  
2. Navigate to **Task Monitoring**.  
   
   ![Task Monitoring](image)  
   
   **Note:** If a failure occurs with fdconfig, logs can be accessed in `/var/TKLC/log/fdconfig/fdconfig.log` file.  
   
   ```bash
   [admusr@melbourne-pmac-1 fdconfig]$ sudo fdconfig dumpsteps --file=deploy_melbourne_20170329T202458_701b.fdcdb
   Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb"
   Here are the steps that were generated
   ------------------------------ begin ------------------------------
   Dump of DB steps:
   NUM PHS DLY INFRA ID SVRTYPE CMD ELEMENT PRE STATE TO BGTS COMMAND TEXT
   ------------------------------
   1 1 0 pmac Fast_Deployment 0 21 0 Complete 300 0 Check PM&C is available
   2 1 0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet
   3 1 0 pmac Fast_Deployment 0 3 melbourne RMS3 1 Skipped 900 0 Add Rms
   4 2 0 pmac Fast_Deployment 1
   4. Restart the fdconfig after a failure has occurred and has been resolved:  

```bash
$ sudo fdconfig restart --file=deploy_melbourne_20170329T202458_701b.fdcdb
```
## Procedure 4. Recovery Scenario 4

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

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

25. **NOAM VIP GUI:** Recover standby NOAM, if needed

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

26. **Install NetBackup client (optional)**

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

27. **NOAM VIP GUI:** Set HA on standby NOAM

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>28.</td>
<td>NOAM VIP GUI:</td>
<td><strong>Restart DSR application</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Server</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the recovered standby NOAM server and click <strong>Restart</strong>.</td>
</tr>
<tr>
<td>29.</td>
<td>Active NOAM:</td>
<td><strong>Correct the recognized authority table</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Establish an SSH session to the active NOAM and login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Execute this command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ sudo top.setPrimary</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>Using my cluster: A1789</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>New Primary Timestamp: 11/09/15 20:21:43.418</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>Updating A1789.022: &lt;DSR_NOAM_B_hostname&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>Updating A1789.144: &lt;DSR_NOAM_A_hostname&gt;</code></td>
</tr>
<tr>
<td>30.</td>
<td>NOAM VIP GUI:</td>
<td><strong>Recover query servers.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SDS only. If DSR, skip to step 33.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Execute the <strong>Configuring SDS Query Servers</strong> procedure, steps 1 and 4-7, from reference [8].</td>
</tr>
</tbody>
</table>
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 31. | **SDS NOAM VIP GUI:** Set HA on query server.  
     SDS only. If DSR, skip to step 33. |
| 1.  | Navigate to **Status & Manage > HA.** |
| 2.  | Click **Edit.** |
| 3.  | Select the query server and select **Observer.** |
| 4.  | Click **OK.** |
| 32. | **SDS NOAM VIP GUI:** Restart SDS application.  
     SDS only. If DSR, skip to step 33. |
| 1.  | Navigate to **Status & Manage > Server.** |
| 2.  | Select the recovered query server and click **Restart.** |
| 33. | **NOAM VIP GUI:** Recover the SOAM servers *(Standby, Spare — Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only)*  
     **DSR:** Execute the **Configure the SOAM Servers** procedure, steps 1-3 and 5-9, from reference [8].  
     **Note:** If you are using NetBackup, also execute step 12.  
     **SDS:** Execute the **Configure the SDS DP SOAM Servers** procedure, steps 1-3 and 5-8, from reference [8]. |
### Procedure 4. Recovery Scenario 4

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

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

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

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

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

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

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

2. Click **Edit.**

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

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

<table>
<thead>
<tr>
<th>39.</th>
<th><strong>NOAM VIP GUI:</strong> Restart DSR application on recovered C-level servers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Server.</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Status &amp; Manage</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Network Elements</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Server</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>HA</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Database</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>KPIs</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Processes</strong></td>
</tr>
<tr>
<td></td>
<td>2. Select the recovered C-level servers and click <strong>Restart.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>40.</th>
<th><strong>Active NOAM:</strong> Perform keyexchange between the active-NOAM and recovered servers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Establish an SSH session to the active NOAM, login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Perform a keyexchange from the active NOAM to each recovered server:</td>
</tr>
</tbody>
</table>
|     |   ```
|     | $ keyexchange admusr@<Recovered Server Hostname>
|     | ```
|     | **Note:** If an export server is configured, perform this step.                   |

<table>
<thead>
<tr>
<th>41.</th>
<th><strong>Active NOAM:</strong> Activate optional features. DSR only. If SDS, then skip step 43.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Establish an SSH session to the active NOAM and login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note for PCA Feature Activation:</strong></td>
</tr>
<tr>
<td></td>
<td>If you have PCA installed in the system being recovered, re-activate the PCA</td>
</tr>
<tr>
<td></td>
<td>by executing the <strong>PCA Activation on Active NOAM Server</strong> procedure on</td>
</tr>
<tr>
<td></td>
<td>recovered active NOAM server and the <strong>PCA Activation on Standby SOAM Server</strong></td>
</tr>
<tr>
<td></td>
<td>procedure on the recovered standby SOAM server from [6].</td>
</tr>
<tr>
<td></td>
<td><strong>Notes:</strong></td>
</tr>
<tr>
<td></td>
<td>- If not all SOAM sites are recovered at this point, then repeat the activation</td>
</tr>
<tr>
<td></td>
<td>for each “new” SOAM site that comes online.</td>
</tr>
<tr>
<td></td>
<td>- If any of the MPs have failed and recovered, then restart these MP</td>
</tr>
<tr>
<td></td>
<td>servers after activation of the feature.</td>
</tr>
<tr>
<td></td>
<td>Refer to section 1.5 Optional Features to activate any features that were</td>
</tr>
<tr>
<td></td>
<td>previously activated.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> While running the activation script, the following error message (and</td>
</tr>
<tr>
<td></td>
<td>corresponding messages) output may display. This can safely be</td>
</tr>
<tr>
<td></td>
<td>ignored:</td>
</tr>
</tbody>
</table>
|     |   ```
|     | iload#31000{S/W Fault}
|     | ```

<table>
<thead>
<tr>
<th>42.</th>
<th><strong>MP Servers:</strong> Disable SCTP Auth Flag (DSR only). DSR only. If SDS, then skip step 43.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For SCTP connections without DTLS enabled, refer to the <strong>Enable/Disable DTLS (SCTP Diameter Connections Only)</strong> section in reference [8].</td>
</tr>
<tr>
<td></td>
<td>Execute this procedure on all failed MP servers.</td>
</tr>
</tbody>
</table>
Procedure 4. Recovery Scenario 4

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

1. Navigate to Status & Manage > Database.

2. Select the active NOAM server and click Report.

The following screen displays:

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

```
<table>
<thead>
<tr>
<th>Database Status Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Active Network OAM5P on host ZombieNOAM1</td>
</tr>
<tr>
<td>Report Version: 8.0.0.0.0-80.9.0</td>
</tr>
<tr>
<td>User: guiadmin</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname: ZombieNOAM1</td>
</tr>
<tr>
<td>Database Birthday: 2016-07-11 11:21:50 EDT</td>
</tr>
<tr>
<td>Applications Database Version: 6.0</td>
</tr>
<tr>
<td>Application Database Version:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Capacities and Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Utilization: 5.4%: 555M used of 7.0G total, 6.0G available</td>
</tr>
<tr>
<td>Memory Utilization: 0.0%: used of total, 0K available</td>
</tr>
</tbody>
</table>
```

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

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

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

**Example output:**

```
-- Policy 0 ActStb [DbReplication] --------------------------
Oahu-DAMP-1 -- Active
  BC From Oahu-SOAM-2 Active 0.50 0.15%cpu 25B/s A=me
  CC To Oahu-DAMP-2 Active 0.10 0.14%cpu 25B/s A=me
Oahu-DAMP-2 -- Stby
  BC From Oahu-SOAM-2 Active 0.50 0.11%cpu 31B/s A=C3642.212
  CC From Oahu-DAMP-1 Active 0.10 0.14 1.16%cpu 31B/s
                     A=C3642.212
Oahu-IPFE-1 -- Active
  BC From Oahu-SOAM-2 Active 0.50 0.03%cpu 24B/s A=C3642.212
Oahu-IPFE-2 -- Active
  BC From Oahu-SOAM-2 Active 0.50 0.03%cpu 28B/s A=C3642.212
Oahu-NOAM-1 -- Stby
  AA From Oahu-NOAM-2 Active 0.25 0.03%cpu 23B/s
Oahu-NOAM-2 -- Active
  AA To Oahu-NOAM-1 Active 0.25 1%R 0.04%cpu 61B/s
  AB To Oahu-SOAM-2 Active 0.50 1%R 0.05%cpu 75B/s
Oahu-SOAM-1 -- Stby
  BB From Oahu-SOAM-2 Active 0.50 0.03%cpu 27B/s
Oahu-SOAM-2 -- Active
  AB From Oahu-NOAM-2 Active 0.50 0.03%cpu 24B/s
  BB To Oahu-SOAM-1 Active 0.50 1%R 0.04%cpu 32B/s
  BC To Oahu-IPFE-1 Active 0.50 1%R 0.04%cpu 21B/s
  BC To Oahu-SS7MP-2 Active 0.50 1%R 0.04%cpu 21B/s
irepstat (40 lines) (h)elp (m)erged
```
Procedure 4. Recovery Scenario 4

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

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

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

2. Verify the OAM Max HA Role as shown.

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

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

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

2. Select the row for all of the servers.

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

<table>
<thead>
<tr>
<th>Hostname</th>
<th>OAM HA Role</th>
<th>Application HA Role</th>
<th>Max Allowed HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieDRNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZombieSOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Standby</td>
</tr>
<tr>
<td>Procedure 4. Recovery Scenario 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>47. <strong>SOAM VIP GUI:</strong> Verify the local node information. DSR only. If SDS, then skip to step 56.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Navigate to <strong>Diameter &gt; Configuration &gt; Local Node</strong>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Configuration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Capacity Summary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Connection Capacity Dash</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Application Ids</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- CEX Parameters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Command Codes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Configuration Sets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Local Nodes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Verify all the local nodes are shown.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>48. <strong>SOAM VIP GUI:</strong> Verify the peer node information. DSR only. If SDS, then skip to step 56.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Navigate to <strong>Diameter &gt; Configuration &gt; Peer Node</strong>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Configuration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Capacity Summary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Connection Capacity Dash</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Application Ids</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- CEX Parameters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Command Codes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Configuration Sets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Local Nodes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Peer Nodes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Verify all the peer nodes are shown.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>49. <strong>SOAM VIP GUI:</strong> Verify the connections information. DSR only. If SDS, then skip to step 56.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Navigate to <strong>Diameter &gt; Configuration &gt; Connections</strong>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Configuration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Capacity Summary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Connection Capacity Dash</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Application Ids</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- CEX Parameters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Command Codes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Configuration Sets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Local Nodes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Peer Nodes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Peer Node Groups</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Connections</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Verify all the connections are shown.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>50.</td>
<td><strong>SOAM VIP GUI:</strong> Enable connections, if needed. DSR only. If SDS, then skip to step 56.</td>
</tr>
</tbody>
</table>
| 1. | Navigate to **Diameter > Maintenance > Connections.**  
   ![Connections](image)  
   1. Select each connection and click **Enable**. Alternatively, enable all the connections by clicking **EnableAll**.  
   ![EnableAll](image) ![Disable](image)  
   3. Verify the Operational State is **Available**.  
      **Note:** If a disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution. |
| 51. | **SOAM VIP GUI:** Enable optional features. DSR only. If SDS, then skip to step 56. |
| 1. | Navigate to **Diameter > Maintenance > Applications.**  
   ![Applications](image)  
   2. Select the optional feature application configured in step 72.  
   3. Click **Enable**.  
   ![Enable](image) ![Disable](image) ![Pause updates](image) |
| 52. | **SOAM VIP GUI:** Re-enable transports, if needed. DSR only. If SDS, then skip to step 56. |
| 1. | Navigate to **Transport Manager > Maintenance > Transport.**  
   ![Transport Manager](image)  
   2. Select each transport and click **Enable**.  
   ![Enable](image) ![Disable](image) ![Block](image)  
   3. Verify the Operational Status for each transport is **Up**. |
## Procedure 4. Recovery Scenario 4

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SOAM VIP GUI:</strong></td>
<td><strong>Re-enable MAPIWF application, if needed.</strong></td>
<td><strong>DSR only. If SDS, then skip to step 56.</strong></td>
</tr>
<tr>
<td><strong>53.</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users.**

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

2. Click the **Enable** button corresponding to MAPIWF Application Name.

![Enable Disable buttons](image)

3. Verify the SSN Status is **Enabled.**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SOAM VIP GUI:</strong></td>
<td><strong>Re-enable links, if needed.</strong></td>
<td><strong>DSR only. If SDS, then skip to step 56.</strong></td>
</tr>
<tr>
<td><strong>54.</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Navigate to **SS7/Sigtran > Maintenance > Links.**

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

2. Click **Enable** for each link.

![Enable Disable buttons](image)

3. Verify the Operational Status for each link is **Up.**
### Procedure 4. Recovery Scenario 4

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

1. **Validate Key File**

   ```bash
   $ cd /usr/TKLC/dpi/bin/
   $ ./sharedKrevo -validate
   
   Example output:
   ```
   ```bash
   [admusr@NOAM-2 bin]$ ./sharedKrevo -validate
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   1450723458: [INFO] Key file for 'NOAM-1' is valid
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   1450723460: [INFO] Key file for 'NOAM-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}$
   
   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 Servers**

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

   Example output:
   ```bash
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   1450722736: [INFO] Synched key to IPFE.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   1450722736: [INFO] Synched key to MP-2.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   1450722736: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   1450722736: [INFO] Synched key to MP-1.
   {admusr@NOAM-2 bin}$
   ```

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

   Example output:
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>58.</td>
<td><strong>SOAM VIP GUI:</strong> 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>- <strong>View Active</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>View History</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>View Trap Log</strong></td>
</tr>
<tr>
<td></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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>59.</td>
<td><strong>NOAM VIP GUI:</strong> 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>- <strong>View Active</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>View History</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>View Trap Log</strong></td>
</tr>
<tr>
<td></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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>60.</td>
<td><strong>Restart oampAgent, if needed</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If <strong>10012: The responder for a monitored table failed to respond to a table change</strong> alarm displays, the oampAgent needs to be restarted.</td>
</tr>
<tr>
<td></td>
<td>1. Establish an SSH session to each server that has the alarm.</td>
</tr>
<tr>
<td></td>
<td>2. Login admusr</td>
</tr>
<tr>
<td></td>
<td>3. Execute the following 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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>61.</td>
<td><strong>Back up and archive all the databases from the recovered system</strong></td>
</tr>
<tr>
<td></td>
<td>Execute the <strong>DSR Database Backup</strong> procedure to back up the configuration databases.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>62.</td>
<td><strong>Recover IDIH</strong></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>
</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
- Recover IDIH if necessary

Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step #</th>
<th>Workarounds</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>2.</td>
<td>Gather required materials</td>
<td>Gather the documents and required materials listed in Required Materials.</td>
</tr>
</tbody>
</table>

1. Workarounds
   - 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.
**Procedure 5. Recovery Scenario 5**

| 4. | Recover failed SOAMs | If ALL SOAM servers have failed, execute Procedure 2.  
If ALL NOAM servers have failed, execute:  
1. Procedure 4, steps 4. through 14.  
2. Perform keyexchange between the newly active NOAM and the recovered NOAM PMAC.  
   From a terminal window connection on the active NOAM as the *admusr* user, exchange SSH keys for *admusr* between the active NOAM and the recovered NOAM's PMAC server using the keyexchange utility, using the management IP address for the PMAC server.  
   When asked for the password, enter the password for the *admusr* user of the PMAC server.  
   
   ```
   $ keyexchange admusr@<Recovered_Servers_PMAC_IP Address>
   ```  
   **Note:** If keyexchange fails, edit `/home/admusr/.ssh/known_hosts` and remove blank lines. Retry the keyexchange commands.

| 5. | Perform keyexchange between active NOAM and recovered NOAMs | Perform a keyexchange between the newly active NOAM and the recovered NOAM servers:  
8. 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.  
9. When prompted for the password, enter the password for the *admusr* user of the recovered NOAM servers.  
   
   ```
   $ keyexchange admusr@<Recovered_NOAM Hostname>
   ```  

3. Use the PMAC GUI to determine the control network IP address of the recovered VMs.  
4. Navigate to Software Inventory.  
5. Perform a keyexchange between the recovered PMAC and the recovered guests:  
   From a terminal window connection on the recovered PMAC as the *admusr* user, exchange SSH keys for *admusr* between the PMAC and the recovered VM guests using the keyexchange utility, using the control network IP addresses for the VM guests.  
   When asked for the password, enter the password for the *admusr* user of the VM guest.  
   
   ```
   $ keyexchange admusr@<Recovered_VM_control_IP Address>
   ```  
   **Note:** If keyexchange fails, edit `/home/admusr/.ssh/known_hosts` and remove blank lines. Retry the keyexchange commands.

6. Procedure 4, steps 15. through 19. for each NOAM.
### Procedure 5. Recovery Scenario 5

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

```
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. |
| 8.   | **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
   ```

   **Note:** If output of above command shows that existing key file is not valid, contact My Oracle Support (MOS).  
2. Copy the key file from active DR NOAM to recovered NOAMs.

   ```
   $ ./sharedKrevo -copyKey -destServer <First NOAM server>
   $ ./sharedKrevo -copyKey -destServer <Second NOAM server>
   ```
## Procedure 5. Recovery Scenario 5

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 9. | **Primary NOAM**: Modify DSR OAM process | 1. Establish an SSH session to the primary NOAM, login as `admusr`.<br>2. Retrieve the cluster ID of the recovered NOAM:<br>$ sudo iqt -fClusterID TopologyMapping where "NodeID='<DR_NOAM_Host_Name>'"  
Server_ID NodeID ClusterID  
   1 Oahu-DSR-NOAM-2 A1055<br>3. Execute this command to start the DSR OAM process on the recovered NOAM:<br>$ echo "<clusterID>|DSROAM_Proc|Yes" | iload -ha -xun -fcluster -fresource -foptional HaClusterResourceCfg|
| 10. | Switch DR NOAM back to secondary | Once the system has been recovered, refer to [13] DSR/SDS 8.2 NOAM Failover User's Guide. |
## Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11. NOAM VIP:</td>
<td>Verify all servers in topology are accessible (RADIUS only). DSF only. If SDS, then skip to the next step.</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. Establish an SSH session to the NOAM VIP and login as `admusr`.
2. Check if all the servers in the topology are accessible:

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

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

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

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

   **Example output:**

   ```
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   14S0722753: [INFO] Synced key to DPX
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   14S0722756: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   14S0722758: [INFO] Synced key to MP-1
   [admusr@NOAM-2 ~]$ 
   ```

   **Example output:**

   ```
   [admusr@NOAM-1 ~]$ ./sharedKrevo -updateData
   14S0024519: [INFO] Updating data on server 'NOAM-1'
   14S0024519: [INFO] Data updated to 'NOAM-1'
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   14S0024520: [INFO] Updating data on server 'NOAM-2'
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   14S0024522: [INFO] 1 rows updated on 'NOAM-2'
   14S0024522: [INFO] Data updated to 'NOAM-2'
   ```

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

12. **Recovered Servers:**
    - Verify alarms

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

2. Verify the recovered servers are not contributing to any active alarms (Replication, Topology misconfiguration, database impairments, NTP, etc.)

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

4.6 Recovery Scenario 6 (Database Recovery)

4.6.1 Recovery Scenario 6: Case 1

For a partial outage with:
- Server having a corrupted database
- Replication channel from parent is inhibited because of upgrade activity; or
- Server is in a different release 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

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

Procedure 6. Recovery Scenario 6 (Case 1)

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

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

![Oracle System Login](image)
### Procedure 6. Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | Navigate to **Status & Manage > HA**. ![Status & Manage HA tree](image1.png)  
  1. Select **Edit**.  
  ![Modifying HA attributes](image2.png)  
  3. Set the Max Allowed HA Role option to **OOS** for the failed servers.  
  4. Click **OK**.  
| 2.   | **Server in Question**: Login. Establish an SSH session to the server in question. Login as **admusr**. |
| 3.   | **Server in Question**: Bring the system to runlevel 3.  
  `$ sudo init 3` |
| 4.   | **Server in Question**: Recover system. Execute this command and follow the instructions appearing in the console prompt.  
  `$ sudo /usr/TKLC/appworks/sbin/backout_restore` |
| 5.   | **Server in Question**: Change runlevel to 4.  
  `$ sudo init 6` |
### Procedure 6. Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 8.   | **Server in Question:** Verify the server
|      | **Verify if the processes are up and running.**
|      | `$ sudo pm.getprocs` |
|      | **Example output:** |
|      | ![Example output screenshot](image) |

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 9.   | **NOAM VIP GUI:** Set failed servers to active
|      | **Navigate to Status & Manage > HA.**
|      | ![Status & Manage diagram](image) |
|      | **Click Edit.** |
|      | **Select the failed server and set it to Active.** |
|      | ![Modifying HA attributes screenshot](image) |
|      | **Click OK.** |
Procedure 6. Recovery Scenario 6 (Case 1)

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 10. | **NOAM VIP:** Verify all servers in topology are accessible (RADIUS only) | If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.

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

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

   ```
   $ cd /usr/TKLC/dpi/bin/
   $ ./sharedKrevo -checkAccess
   [admusr@NOAM-2 bin]$ ./sharedKrevo -checkAccess
   FIPS integrity verification test failed.
   1450723797: [INFO] 'NOAM-1' is accessible.
   FIPS integrity verification test failed.
   1450723797: [INFO] 'SOAM-1' is accessible.
   FIPS integrity verification test failed.
   1450723797: [INFO] 'SOAM-2' is accessible.
   FIPS integrity verification test failed.
   1450723797: [INFO] 'IPFE' is accessible.
   FIPS integrity verification test failed.
   1450723797: [INFO] 'MP-2' is accessible.
   FIPS integrity verification test failed.
   1450723797: [INFO] 'MP-1' is accessible.
   [admusr@NOAM-2 bin]$ 
   ```

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

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

   ```
   [admusr@NOAM-2 bin]$ ./sharedKrevo -validate
   [admusr@NOAM-2 bin]$ ./sharedKrevo -validate
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   1450723843: [INFO] Key file for 'NOAM-1' is valid
   1450723843: [INFO] Key file for 'NOAM-2' is valid
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   1450723843: [INFO] Key file for 'SOAM-1' is valid
   1450723843: [INFO] Key file for 'SOAM-2' is valid
   FIPS integrity verification test failed.
   FIPS integrity verification test failed.
   1450723843: [INFO] Key file for 'IPFE' is valid
   1450723843: [INFO] Key file for 'MP-2' is valid
   1450723843: [INFO] Key file for 'MP-1' is valid
   [admusr@NOAM-2 bin]$ 
   ```

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

<table>
<thead>
<tr>
<th></th>
<th>2. Copy the key file to all the servers in the Topology:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$ ./sharedKrevo –synchronize</td>
</tr>
<tr>
<td></td>
<td>$ ./sharedKrevo –updateData</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Command Output" /></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th>12. Backup and archive all the databases from the recovered system</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Execute DSR Database Backup to back up the Configuration databases.</td>
</tr>
</tbody>
</table>
### 4.6.2 Recovery Scenario 6: Case 2

For a partial outage with:

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

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

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

**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 7. Recovery Scenario 6 (Case 2)

| 3. | **NOAM VIP GUI:** Set failed servers to OOS |
| 4. | **Server in Question:** Login |
| 5. | **Server in Question:** Stop httpd service |
| 6. | **Server in Question:** Take server out of service |
| 7. | **Server in Question:** Take server to DbUp state and start the application |

1. **Navigate to Status & Manage > HA.**
   - ![Diagram showing Status & Manage menu with options like Network Elements, Server, HA, Database, KPIs, and Processes]
   - 2. **Click Edit.**

   **Modifying HA attributes**
   - | Hostname | Max Allowed HA Role | Description |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ZombieNOAM1</td>
<td>Active</td>
<td>The maximum det</td>
</tr>
<tr>
<td>ZombieNOAM2</td>
<td>OOS</td>
<td>The maximum det</td>
</tr>
<tr>
<td>ZombieDRNOAM1</td>
<td>Standby</td>
<td>The maximum det</td>
</tr>
<tr>
<td>ZombieDRNOAM1</td>
<td>Spare Observer</td>
<td>The maximum det</td>
</tr>
</tbody>
</table>

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

4. **Click OK.**

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

6. **Server in Question:** Take server out of service
   - Take the server out of service.
   - `$ prod.clobber`

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 8. **Server in Question:** Start httpd service | 1. Start the httpd service.  
   
   ```bash
   $ service httpd start
   ```  
   2. Exit out of root.  
   
   ```bash
   $ exit
   ``` |
| 9. **NOAM VIP GUI:** Set failed servers to active | 1. Navigate to **Status & Manage > HA.**  
   2. Click **Edit** at the bottom of the screen.  
   3. Select the failed server and set it to **Active.**  
   4. Click **OK.** |
| 10. **NOAM VIP GUI:** Restart DSR application | 1. Navigate to **Status & Manage > Server.**  
   2. Select each recovered server and click **Restart.** |
Procedure 7. Recovery Scenario 6 (Case 2)

11. **Server in Question:** Verify the server state

1. Verify the processes are up and running:

   ```
   $ sudo pm.getprocs
   ```

   **Example output:**

   ```
   A ipl3554-cpx126 Up 12/21 19:16:25 i pl3554
   A ipl3554-cpx127 Up 12/21 19:16:25 i pl3554
   A ipl3554-cpx128 Up 12/21 19:16:25 i pl3554
   ```

2. Verify if replication channels are up and running:

   ```
   $ sudo irepstat
   ```

   **Example output:**

   ```
   Policy: 0 Activated [DbReplication] ---------------------------------------
   BC From MP3 Active 0.50 0.02%cpu 358/s A=T2173.145
   CC From MP3 Active 0.50 0.02%cpu 358/s A=T2173.145
   ```

3. Verify if merging channels are up and running:

   ```
   $ sudo inetmstat
   ```

   **Example output:**

   ```
   nodeID InetMerge State dir dSeq dTime updTime info
   SOA-1 Standby To 0 0.00 15:19:33
   SOA-2 Active To 0 0.00 15:19:33
   ```

12. **NOAM VIP:** Verify all servers in topology are accessible (RADIUS Only).

    DSR only. If SDS, skip to step 14.

    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)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>13.</strong></td>
<td><strong>NOAM VIP:</strong> Copy key file to all the servers in topology (RADIUS Only)</td>
</tr>
<tr>
<td></td>
<td>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</td>
</tr>
<tr>
<td>1.</td>
<td>Check if existing key file on active NOAM (the NOAM which is intact and was not recovered) server is valid:</td>
</tr>
</tbody>
</table>
| | ```
| 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 |
| ``` |
| **14.** | Backup and archive all the databases from the recovered system |
| | Execute DSR Database Backup to back up the Configuration databases. |

**Note:** If any errors are present, stop and contact My Oracle Support (MOS).
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>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Before Restoration: Notify affected users before restoration</td>
<td>Contact each user affected before the restoration and notify them that you will reset their password during this maintenance operation.</td>
</tr>
</tbody>
</table>
| 2.     | After Restoration: Log into the NOAM VIP | 1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: 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 8. Keep Restored User

1. Navigate to Administration > Access Control > Users.

2. Select the user.

3. Click Change Password.

4. Type a new password.

5. Click Continue.

**NOTE:** The password must be between 8 and 16 characters.

The password must also contain 3 of these 4 types of characters:

- numeric
- lowercase alpha
- uppercase alpha
- special character (!@#$%^&*?)

Enter the old password once, new password twice for **guiadmin**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Old Password</td>
<td></td>
</tr>
<tr>
<td>New Password</td>
<td></td>
</tr>
<tr>
<td>Retype New Password</td>
<td></td>
</tr>
<tr>
<td>Force password change on next login</td>
<td>Yes/No</td>
</tr>
</tbody>
</table>

Click **Continue**
# 5.3 Remove a Restored User

## Procedure 9. Remove the Restored 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.

### After Restoration: Log into the NOAM VIP

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

![Oracle System Login](image)
Procedure 9. Remove the Restored User

<table>
<thead>
<tr>
<th>2.</th>
<th>After Restoration: Reset user passwords</th>
</tr>
</thead>
</table>

1. Navigate to Administration > Access Control > Users.

2. Select the user.
3. Click Delete.
4. Click OK to confirm.

5.4 Restore a Modified User

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

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

Before Restoration:
Verify you have access to a user with administrator permissions that is not affected.
Contact each user affected and notify them that you will reset their password during this maintenance operation.

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

5.5 Restore an Archive that Does Not Contain a Current User

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

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

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

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

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

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

   ![Oracle System Login](image-url)
### Procedure 10. Restore an Archive That Does Not Contain a Current User

#### Before Restoration: Record user settings

1. Navigate to **Administration > Access Control > Users.**

   - **Main Menu**
     - **Administration**
       - **General Options**
       - **Access Control**
         - **Users**
         - **Groups**
         - **Sessions**
         - **Certificate Management**
         - **Authorized IPs**
         - **SFTP Users**

2. Under each affected user, record the following:
   - Username
   - Account status
   - Remote Auth
   - Local Auth
   - Concurrent Logins Allowed
   - Inactivity Limit
   - Comment
   - Groups
## Procedure 10. Restore an Archive That Does Not Contain a Current User

<table>
<thead>
<tr>
<th>4. After Restoration: Login</th>
</tr>
</thead>
<tbody>
<tr>
<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>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</td>
</tr>
<tr>
<td>2. Login as the <strong>guiadmin</strong> user:</td>
</tr>
</tbody>
</table>

![Oracle System Login](image-url)
Procedure 10. Restore an Archive That Does Not Contain a Current User

5. **After restoration:** recreate affected user

1. **Navigate to Administration > Access Control > Users.**

   - **Main Menu**
     - **Administration**
       - **General Options**
         - **Access Control**
           - **Users**
             - **Groups**
               - **Sessions**
                 - **Certificate Management**
                   - **Authorized IPs**
                     - **SFTP Users**

2. **Click Insert.**

   ![Insert Button]

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

   **Adding new user**

   - **Username**: admin
   - **Group**: admin
   - **Authentication Options**
     - Allow Local Authentication
   - **Access Options**
     - Allow GUI Access
     - Allow MMI Access
   - **Access Allowed**
     - Account Enabled
   - **Maximum Concurrent Logins**: 0
   - **Session Inactivity Limit**: 120
   - **Comment**:

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

6. **After Restoration:**
   - Repeat for additional users

7. **After Restoration:**
   - Repeat step 5 to recreate additional users.

### 6. IDIH Disaster Recovery

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

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

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

### Disaster Recovery Scenarios

<table>
<thead>
<tr>
<th>Disaster Recovery Scenario</th>
<th>fdconfig file to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server containing Oracle database server</td>
<td>Install fdconfig xml</td>
</tr>
<tr>
<td>Server containing Application Server</td>
<td>Upgrade/Disaster Recovery xml</td>
</tr>
<tr>
<td>Server containing Mediation Server</td>
<td>Upgrade/Disaster Recovery xml</td>
</tr>
</tbody>
</table>
Procedure 11. IDIH Disaster Recovery Preparation

<table>
<thead>
<tr>
<th>STEP #</th>
<th>PMAC GUI: Login</th>
</tr>
</thead>
</table>
| 1.     | Open web browser and enter:  
        | http://<PMAC_Mgmt_Network_IP>  
        | Login as pmacadmin user: |

1. **PMAC GUI**: Login

   1. Open web browser and enter:
      
      `http://<PMAC_Mgmt_Network_IP>`

   2. Login as `pmacadmin` user:

      ![Oracle System Login](image)

      Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 10.0, or 11.0 with support for JavaScript and cookies.

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

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

2. **PMAC GUI**: Verify necessary IDIH images are available

   1. Navigate to **Software** > **Manage Software Images**.

      ![Software Tree](image)

      2. Verify the current IDIH TVOE, TPD, Oracle, Application and Mediation images are listed.

      3. Verify these values match the name in the `<software> </software>` section in the `hostname-upgrade_xx-xx-xx.xml` file.

      **Note:** If the necessary software images are not available, follow the instructions from the **Load Application and TPD ISO onto PMAC Server** procedure and steps 1-4 of **IDIH Configuration** from [8] to acquire and transfer the images.
<table>
<thead>
<tr>
<th>Procedure 11. IDIH Disaster Recovery Preparation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3.</strong></td>
</tr>
<tr>
<td><strong>4.</strong></td>
</tr>
</tbody>
</table>

Example output:
```bash
(admusr@thunderbolt-oracle ~) $ 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-oracle
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 sysexec - this can take a while
10:10:58: No errors in sysexec modules
10:10:58: Checking Alarm 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: ttcp-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
10:11:01: Oracle server and resources online
10:11:01: All tests passed!
10:11:01: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
(admusr@thunderbolt-oracle ~)$  
```
## 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>
</table>
| 1.     | Open web browser and enter:  

http://<PMAC_Mgmt_Network_IP>

2. Login as pmacadmin user: |

![Oracle System Login](image)

1. Navigate to **Main Menu > VM Management**.
   - Software
     - Software Inventory
     - Manage Software Images
     - VM Management
   2. Select the application guest.
   3. Click **Delete**.
### Procedure 12. IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

<table>
<thead>
<tr>
<th></th>
<th>Remove existing mediation server</th>
<th>1. Navigate to <strong>Main Menu &gt; VM Management.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2. <strong>Software Inventory</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. <strong>Manage Software Images</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. <strong>VM Management</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>E</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>88964</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>-</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>01</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>-</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>-</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>-</strong></td>
</tr>
<tr>
<td></td>
<td>2. Select the Mediation guest.</td>
<td><strong>-</strong></td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Delete</strong>.</td>
<td><strong>-</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>PMAC: Establish SSH session and login</th>
<th>Establish an SSH session to the PMAC, login as <strong>admusr</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>PMAC</strong>: Establish SSH session and login</td>
<td><strong>PMAC</strong>: Re-install the mediation and application servers</td>
</tr>
<tr>
<td></td>
<td><strong>PMAC</strong>: Establish SSH session and login</td>
<td>Execute this command (Enter your upgrade file):</td>
</tr>
<tr>
<td></td>
<td><strong>PMAC</strong>: Establish SSH session and login</td>
<td><code>$ cd /var/TKLC/smac/guest-dropin</code></td>
</tr>
<tr>
<td></td>
<td><strong>PMAC</strong>: Establish SSH session and login</td>
<td><code>$ screen</code></td>
</tr>
<tr>
<td></td>
<td><strong>PMAC</strong>: Establish SSH session and login</td>
<td><code>$ sudo fdconfig config --file=&lt;hostname-upgrade_xx-xx-xx&gt;.xml</code></td>
</tr>
</tbody>
</table>

---

**Warning**

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

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

<table>
<thead>
<tr>
<th></th>
<th>PMAC GUI: Monitor the configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td><img src="image1.png" alt="Image" /></td>
</tr>
</tbody>
</table>

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

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

3. Monitor the IDIH configuration to completion.
   Alternatively, you can monitor the fdconfig status through the command line after executing the fdconfig command:

Example:

```
admusr@bertie:~/VAR/KL episodes/fdconfigxml/run_config
```

```
Request to start a new configuration
Running d-ray-04-21-15.xml configuration
Configuration file processing complete

Created a deployment database file: deploy_d-ray_20150511093944_630c.fdcdb
Preparing to run the configuration steps
FM4C 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>Description</th>
</tr>
</thead>
</table>
| 1. ☐ NOAM/SOAM VIP: Login | 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:

```
http://<Primary_NOAM/SOAM_VIP_IP_Address>
```

2. Login as the guadmin user:

![Oracle System Login](image-url)

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.
Procedure 13. DSR Database Backup

1. Navigate to **Status & Manage > Database**.
   - Select **Database**
   - Select **Configuration**

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

3. Make sure that the **Configuration** checkbox is marked.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>NOAM/SOAM VIP: Verify the backup file existence</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Status &amp; Manage &gt; Files</strong>.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Screenshot of Status &amp; Manage &gt; Files" /></td>
</tr>
<tr>
<td>2.</td>
<td>Select the active NOAM or SOAM tab.</td>
</tr>
<tr>
<td>3.</td>
<td>The files on this server display. Verify the existence of the backup file.</td>
</tr>
<tr>
<td>4.</td>
<td>NOAM/SOAM VIP: Download the file to a local machine</td>
</tr>
<tr>
<td>1.</td>
<td>From the previous step, select the backup file.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Download</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Click <strong>OK</strong> to confirm the download.</td>
</tr>
<tr>
<td>5.</td>
<td>Upload the image to secure location</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>Backup active SOAM</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 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 using user `admusr`.

2. Take 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:

   ```
   $ ./sharedKrevo -encr
   ```

4. Copy the encrypted key file to secure customer setup:

   ```
   $ sudo scp /var/TKLC/db/filemgmt/DpiKf.bin.encr user@<customer IP>:<path of customer setup>
   ```

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

### Appendix B. Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only)

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

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

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

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Recover failed Aggregation Switches: Cisco 4948E/4948E-F</td>
</tr>
</tbody>
</table>

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>
   ```

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

**Note:** You need a copy of the HP Misc Firmware DVD or ISO (or firmware file obtained from the appropriate hardware vendor) and the original networking XML files custom for this installation. These are either stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.

**Note:** Copy the switch appropriate init file and use it for respective switch:

Older platform init files may not work on platform 7.2 systems. Copy the switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy switch1A_4948_4948E_init.xml.

4. The templates can be found using the following method:

From the PMAC CLI:

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

Sample output:

```
/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
/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
/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
```

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

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

Example:

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


Example:

```
$ ll
```

```
-rw-r--r-- 1 root root 611 Feb 21 19:18 change_ilo_admin_passwd.xml
-rw-r--r-- 1 root root 107086 Feb 21 19:18 DSR_NetConfig_Templates.zip
-rw-r--r-- 1 root root 13346 Feb 21 19:18 DSR_NOAM_FD_RMS.xml
-rwxr-xr-x 2 root root 2048 Feb 21 19:18 RMS
-rw-r--r-- 1 root root 812 Feb 21 19:18 SAMPLE-NetworkElement.xml
-rw-r--r-- 1 root root 2309 Feb 21 19:20 TRANS.TBL
-rwxr-xr-x 1 root root 2186 Feb 21 19:18 TVOEcfg.sh
-rwxr-xr-x 1 root root 598 Feb 21 19:18 TVOEclean.sh
-rw-r--r-- 1 root root 128703 Feb 21 19:18 UpgradeHCplugin.php-ovl
-rw-r--r-- 1 root root 19658 Feb 21 19:18 upgradeHealthCheck-ovl
```
 Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F) (HP DL380 Gen 9 Only)

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/

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

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

This procedure inhibits A and B level replication on all C-level servers of this site.

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

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

1. Active NOAM: Login
   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 15. Inhibit A and B Level Replication on C-level Servers

3. Active NOAM: Verify replication has been Inhibited

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

Verify replication inhibition on MPs by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site, for example, Site SO_HPC03 is set as A B.

```
$iqt NodeInfo
```

Example output:
```
nodeId  nodeName  hostName nodeCapability  inhibitRepPlans  siteId  excludeTables
A1386.099  NO1  NO1  Active  NO             NO_HPC03
B1754.109  SO1  SO1  Active  NO             SO_HPC03
C2254.131  MP2  MP2  Active  A B             SO_HPC03
C2254.233  MP1  MP1  Active  A B             SO_HPC03
```

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

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

This procedure un-inhibits A and B level replication on all C-level servers of this site.

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

1. Active NOAM: Login
   - Log into the active NOAM server using SSH as admusr.

2. Active NOAM: Un-Inhibit replication on all C-level servers
   - Execute this command:
   ```
   $ for i in `($iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<SOAM_Site_NE_name>'"); do
    iset -finhibitRepPlans='' NodeInfo where "nodeName='$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 16. Un-Inhibit A and B Level Replication on C-level Servers

3. Active NOAM:
Verify replication has been Inhibited

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

```
$ sudo iqt 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 17. Inhibit A and B Level Replication on C-level Servers

1. **Active NOAM:**
   Log into the active NOAM server using SSH as **admusr**.

   **Note:** 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 17. Inhibit A and B Level Replication on C-level Servers

### 2. **Active NOAM:**

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=inhibit --SO_SG_Name=<SOAM server group name>
```

Alternatively to the above script, if the script is not in the specific path:

```
```

**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.

### 3. **Active NOAM:**

Verify replication has been inhibited

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

Verify replication inhibition on MPs by analyzing 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:

```
$ 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 F. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost)

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Active NOAM: Un-Inhibit replication on all C-level servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Active NOAM: Login</td>
</tr>
<tr>
<td></td>
<td>Log into the active NOAM server using SSH as admusr.</td>
</tr>
<tr>
<td>2.</td>
<td>Execute the script from <code>/usr/TKLC/dsr/tools/InhibitReplication.sh</code>, if available.</td>
</tr>
<tr>
<td></td>
<td>If the <code>/usr/TKLC/dsr/tools/</code> path does not have the <code>InhibitReplication.sh</code> script, then use this manual command.</td>
</tr>
<tr>
<td></td>
<td>/usr/TKLC/dsr/tools/InhibitReplication.sh --replication=allow --SO_SG_Name=&lt;SOAM server group name&gt;</td>
</tr>
<tr>
<td></td>
<td>Alternatively to the above script, if the script is not in the specific path:</td>
</tr>
<tr>
<td></td>
<td>$ for i in $(sudo mysql -B -N -e &quot;</td>
</tr>
<tr>
<td></td>
<td>SELECT DISTINCT CS.hostname</td>
</tr>
<tr>
<td></td>
<td>WHERE CS._h_Server_ID = C2SG._h_Server_ID</td>
</tr>
<tr>
<td></td>
<td>AND C2SG._h_SG_ID = CSG._h_SG_ID</td>
</tr>
<tr>
<td></td>
<td>AND CSG.clusterId = CCI.clusterId</td>
</tr>
<tr>
<td></td>
<td>AND CCI.groups = comcol.ClusterGroupInfo.groupId</td>
</tr>
<tr>
<td></td>
<td>AND comcol.ClusterGroupInfo.parentGroup = PCI.groups</td>
</tr>
<tr>
<td></td>
<td>AND PCI.clusterId = PSG.clusterId</td>
</tr>
<tr>
<td></td>
<td>AND PSG.ServerGroupName='&quot;&lt;SOAM_SG_NAME&gt;&quot;'</td>
</tr>
<tr>
<td></td>
<td>&quot;); do iset -finhibitRepPlans='&quot; NodeInfo where &quot;nodeName='$i'&quot;'; done</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.
**Procedure 18. Un-Inhibit A and B Level Replication on C-Level Servers**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td><strong>Active NOAM:</strong> Verify replication has been Inhibited</td>
<td>After executing above steps to un-inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled. Verify replication inhibition on MPs by analyzing 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:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo iqt NodeInfo</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example output:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>nodeId  nodeName  hostName nodeCapability  inhibitRepPlans  siteId  excludeTables</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A1386.099  NO1  NO1  Active  NO_HPC03  NO_HPC03  NO_HPC03</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B1754.109  SO1  SO1  Active  SO_HPC03  SO_HPC03  SO_HPC03</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C2254.131  MP2  MP2  Active  A B  SO_HPC03  SO_HPC03</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C2254.233  MP1  MP1  Active  A B  SO_HPC03  SO_HPC03</td>
</tr>
</tbody>
</table>

**Appendix G. Restore TVOE Configuration from Backup Media**

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Steps</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:

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

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

**Windows:**
Use WinSCP to copy the Backup ISO image into the `/var/TKLC/bkp` directory. Refer to [8], the Using WinSCP procedure, to copy the backup image to the customer system.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Login</td>
<td>Establish an SSH session to the TVOE server and login as <strong>admusr</strong>.</td>
</tr>
</tbody>
</table>
Procedure 19. Restore TVOE Configuration from Backup Media

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

   ```bash
   $ sudo su - placonfig
   ```


3. Select the desired archive.

4. Click OK.

5. Click Restore Backup Archive.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Wait for the restore to complete.</td>
</tr>
<tr>
<td>2</td>
<td>Exit platcfg.</td>
</tr>
<tr>
<td>7</td>
<td>Monitor TVOE backup process</td>
</tr>
<tr>
<td>8</td>
<td>TVOE Server: Exit restore backup menu</td>
</tr>
</tbody>
</table>

**Note:** This typically takes less than 5 minutes.
Procedure 19. Restore TVOE Configuration from Backup Media

9. □ TVOE Server: Restart

1. Restart the TVOE server.

2. Click Yes to restart.

3. Confirm restart.
## Procedure 19. Restore TVOE Configuration from Backup Media

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.</td>
<td><strong>TVOE Server:</strong> Wait for restart to successfully complete</td>
</tr>
<tr>
<td>11.</td>
<td><strong>TVOE Server:</strong> Verify storage pools are active</td>
</tr>
</tbody>
</table>

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
   
<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Autostart</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpguests</td>
<td>active</td>
<td>yes</td>
</tr>
</tbody>
</table>
   
   [admusr@5010441-TVOE ~]$ 
   ```

**Note:** If any storage pools are missing or inactive, contact My Oracle Support (MOS).
Procedure 19. Restore TVOE Configuration from Backup Media

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:

```
$ /usr/TKLC/plat/bin/hidsMgr -initialize
LOG: HIDS monitoring has been Initialized
HIDS baseline has been initialized

$ /usr/TKLC/plat/bin/hidsMgr --enable
HIDS monitoring has successfully been enabled
New State: ENABLED

$ /usr/TKLC/plat/bin/hidsMgr --update --all
HIDS baseline has successfully been updated
```
### Procedure 19. Restore TVOE Configuration from Backup Media

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

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

**Procedure 20. Restore PMAC from Backup Media**

This procedure provides steps to restore the PMAC application configuration from backup media.

**Prerequisite:** TVOE management server has been restored.

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

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

<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 [8].</td>
</tr>
<tr>
<td>2.</td>
<td>PMAC: Login</td>
<td>Establish an SSH session to the PMAC server and login as admusr.</td>
</tr>
<tr>
<td>3.</td>
<td>Restore PMAC Backup image to the PMAC host</td>
<td>From the remote backup location, copy the backup file to the deployed PMAC. This is 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@&lt;ipV6addr&gt;:/&lt;file&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Execute the scp command from the recovered PMAC and the backup file is pulled/retried from the backup location.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/bin/scp -p \ admusr@&lt;remoteserver&gt;:&lt;var/TKLC/smac/backup/&gt;.*.pef &lt;var/TKLC/smac/backup/&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>4.</td>
<td>PMAC: Verify no Alarms are present</td>
<td>Verify no alarms are present.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</td>
</tr>
<tr>
<td>5.</td>
<td>Restore the PMAC Data from Backup</td>
<td>1. Restore the PMAC data from backup.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/smac/bin/pmacadm restore PM&amp;C Restore been successfully initiated as task ID 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Check the status of the background task.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: The result eventually displays PMAC Restore successful.</td>
</tr>
</tbody>
</table>
## Procedure 20. Restore PMAC from Backup Media

<table>
<thead>
<tr>
<th>Step</th>
<th>Action Details</th>
</tr>
</thead>
</table>
| 6. PMAC GUI: Login | 1. Open web browser and navigate to the PMAC GUI.  
2. Login as **PMACadmin** user:  
   ```  
   https://<pmac_network_ip>  
   ``` |
| 7. PMAC GUI: Verify restore task completed | 1. Navigate to **Task Monitoring**.  
2. Verify the restore background task completed successfully.  
**Note:** After the restore is complete, you should see **Add Enclosure** tasks start for all previously provisioning servers. These should be allowed to complete before continuing.  
**Note:** After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior. ISO images are added in the next step. |
### Procedure 20. Restore PMAC from Backup Media

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 8. | **PMAC GUI:** Verify system inventory  
1. Navigate to **Hardware > System Inventory.**  
2. **Main Menu**  
   - **Hardware**  
     - **System Inventory**  
       - **Cabinet 1**  
       - **Cabinet 2**  
       - **Cabinet 101**  
       - **Cabinet Undesignated**  
       - **FRU Info**  
   - **System Inventory**  
2. Verify previously provisioned enclosures are present. |
| 9. | **PMAC:** Verify PMAC  
Perform a system health check on the PMAC.  
$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus  
This command should return no output on a healthy system.  
$ sudo /usr/TKLC/smac/bin/sentry status  
All processes should be running, displaying output similar to the following:  
PM&c Sentry Status  
------------------  
sentryd started: Mon Jul 23 17:50:49 2012  
Current activity mode: ACTIVE  
Process PID Status StartTS NumR  
------------------  
smacTalk 9039 running Tue Jul 24 12:50:29 2012 2  
smacMon 9094 running Tue Jul 24 12:50:29 2012 2  
hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2  
snmEventHandler 9176 running Tue Jul 24 12:50:29 2012 2  
Fri Aug 3 13:16:35 2012  
Command Complete. |
| 10. | **PMAC:** Add ISO images to the PMAC  
Re-add any needed ISO images to the PMAC by executing procedure **Load DSR, SDS (Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only), and TPD ISOs to the PMAC Server** from reference [8] for all required ISO images. |
### Procedure 21. Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Deploy the PMAC guest</td>
<td>Execute Install PMAC from reference [8].</td>
</tr>
<tr>
<td></td>
<td>Prerequisite: TVOE management server has been restored.</td>
<td></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>
<td></td>
</tr>
<tr>
<td></td>
<td>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</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 <strong>admusr</strong>.</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><code>$sudo virsh list</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This produces a listing of currently running virtual machines.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Virtual Machine Listing" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Find the VM name for your PMAC and note its ID number in the first column.</td>
</tr>
<tr>
<td>4.</td>
<td>Connect to console of the VM using the VM number obtained in step 3</td>
<td>On the TVOE host, execute this command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$sudo virsh console &lt;PMAC-VMID&gt;</code></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><img src="image" alt="Console Output" /></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>
## Procedure 21. Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC: Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus</th>
<th>Execute these commands on the PMAC.</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>$ sudo /sbin/service iptables stop&lt;br&gt;iptables: Flushing firewall rules: [OK]&lt;br&gt;iptables: Setting chains to policy ACCEPT: filter [OK]&lt;br&gt;$ sudo /usr/TKLC/smac/etc/services/netbackup start&lt;br&gt;Modified menu NBConfig&lt;br&gt;---&lt;br&gt;show&lt;br&gt;Set the following menus: NBConfig to visible=1&lt;br&gt;Modified menu NBInit&lt;br&gt;---&lt;br&gt;show&lt;br&gt;Set the following menus: NBInit to visible=1&lt;br&gt;Modified menu NBDeInit&lt;br&gt;---&lt;br&gt;show&lt;br&gt;Set the following menus: NBDeInit to visible=1&lt;br&gt;Modified menu NBInstall&lt;br&gt;---&lt;br&gt;show&lt;br&gt;Set the following menus: NBInstall to visible=1&lt;br&gt;Modified menu NBVerifyEnv&lt;br&gt;---&lt;br&gt;show&lt;br&gt;Set the following menus: NBVerifyEnv to visible=1&lt;br&gt;Modified menu NBVerify&lt;br&gt;---&lt;br&gt;show&lt;br&gt;Set the following menus: NBVerify to visible=1=</td>
<td></td>
</tr>
</tbody>
</table>
**Procedure 21. Restore PMAC from Backup Server**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>PMAC: Verify the TPD platcfg backup menus are visible, then exit the TPD platcfg Utility</td>
<td>Verify the TPD platcfg backup menus are visible.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /bin/su - platcfg</td>
</tr>
<tr>
<td></td>
<td>Note: In the example image above of the TPD platcfg utility Main Menu the backup menu is identified as <strong>NetBackup Configuration</strong>.</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>PMAC: Verify the iptables rules are disabled on the PMAC guest</td>
<td>Verify the iptables rules are disabled on the PMAC guest.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo /sbin/iptables -nL</td>
</tr>
<tr>
<td></td>
<td>Note: The <strong>Initial PMAC Application</strong> and <strong>Configure PMAC Application</strong> prerequisites can be ignored.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The <strong>Initialize PMAC Application</strong> and <strong>Configure PMAC Application</strong> prerequisites can be ignored.</td>
</tr>
<tr>
<td>9.</td>
<td>Backup server: verify appropriate PMAC backup exists</td>
<td>This step is likely executed by customer IT personnel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Log into the backup server as the appropriate user using the user password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Execute the appropriate commands to verify the PMAC backup exists for the desired date.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
## Procedure 21. Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.</td>
<td><strong>Backup Server:</strong> Verify appropriate PMAC backup exists</td>
<td>This step is likely executed by customer IT personnel.  &lt;br&gt;1. Log into the backup server as the appropriate user using the user password.  &lt;br&gt;2. Execute the appropriate commands to verify the PMAC backup exists for the desired date.  &lt;br&gt;3. Execute the appropriate commands to restore the PMAC management server backup for the desired date.  &lt;br&gt;<em>Note:</em> 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.</td>
</tr>
<tr>
<td>11.</td>
<td><strong>PMAC:</strong> Verify no alarms are present</td>
<td>Verify no alarms are present.  &lt;br&gt;$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</td>
</tr>
<tr>
<td>12.</td>
<td>Restore the PMAC data from backup</td>
<td>1. Restore the PMAC data from backup.  &lt;br&gt;$ sudo /usr/TKLC/smac/bin/pmacadm restore  &lt;br&gt;PM&amp;C Restore been successfully initiated as task ID 1  &lt;br&gt;2. Check the status of the background task:  &lt;br&gt;$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks  &lt;br&gt;<em>Note:</em> The result eventually displays PMAC Restore successful.</td>
</tr>
</tbody>
</table>
### Procedure 21. Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC GUI:</th>
<th>Description</th>
</tr>
</thead>
</table>
| 13. | Login     | 1. Open web browser and navigate to the PMAC GUI.  
       |            | [https://<pmac_network_ip>](https://<pmac_network_ip>)  
       |            | 2. Login as **PMACadmin** user: |

#### PMAC GUI: Login

![Oracle System Login](image)

*Log In*

Enter your username and password to log in

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.

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC GUI:</th>
<th>Description</th>
</tr>
</thead>
</table>
| 14. | Verify restore task completed | 1. Navigate to **Task Monitoring**.  
       |            | 2. Verify the restore background task completed successfully.  

**Note:** After the restore is complete, you should see **Add Enclosure** tasks start for all previously provisioning servers. These should be allowed to complete before continuing.

**Note:** After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior. ISO images are added in the next step.
## Procedure 21. Restore PMAC from Backup Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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:** Perform a system health check on the PMAC.  
   1. $ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus  
      This command should return no output on a healthy system.  
   2. $ 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  
1. 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. Restore Provisioning Database

Procedure 22. Restore Provisioning Database

This procedure restores the SDS provisioning database. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

1. Primary SDS NOAM GUI: Log into the primary SDS NOAM GUI using its static IP (not the VIP).

2. Primary SDS NOAM GUI: Place the newly recovered standby NOAM into forced standby.

   1. Navigate to Status & Manage > HA.
   2. Click Edit.
   3. Move the newly recovered standby server to forced Standby.

3. Primary SDS NOAM GUI: Restore provisioning data.

   1. Navigate to Status & Manage > Database.
   2. Select the active NOAM and click Restore.
   3. Select the Provisioning backup file from the list (which was previously placed...
Procedure 22. Restore Provisioning Database

in the /var/TKLC/db/filemgmt/backup directory in step 5 of section 2.6.2) and click OK.

**Note:** You must use a provisioning only backup file. Combined backup files contain configuration and provisioning data and cause catastrophic issues, which could lead to a complete re-installation.

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

Database Restore

**Select archive to Restore on server: rghnc-sds:NO-a**

- backup/backup.sds.rghnc-sds: NO-a.Configuration NETWORK_OAMP.20170318_021512.AUTO.tar.gz
- backup/backup.sds.rghnc-sds: NO-a.Provisioning.NETWORK_OAMP.20170318_021512.AUTO.tar.gz
- backup/backup.sds.rghnc-sds: NO-a.Configuration NETWORK_OAMP.20170317_021512.AUTO.tar.gz
- backup/backup.sds.rghnc-sds: NO-a.Provisioning.NETWORK_OAMP.20170317_021512.AUTO.tar.gz
- backup/backup.sds.rghnc-sds: NO-a.Configuration NETWORK_OAMP.20170318_021512.AUTO.tar.gz
- backup/backup.sds.rghnc-sds: NO-a.Provisioning.NETWORK_OAMP.20170318_021512.AUTO.tar.gz
- backup/backup.sds.rghnc-sds: NO-a.Configuration NETWORK_OAMP.20170319_021512.AUTO.tar.gz
- backup/backup.sds.rghnc-sds: NO-a.Provisioning.NETWORK_OAMP.20170319_021512.AUTO.tar.gz
- backup/backup.sds.rghnc-sds: NO-a.Configuration NETWORK_OAMP.20170320_021512.AUTO.tar.gz
- backup/backup.sds.rghnc-sds: NO-a.Provisioning.NETWORK_OAMP.20170320_021512.AUTO.tar.gz

**Ok**  **Cancel**

4. Verify compatibility and click OK to restore.

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

Database Restore Confirm

**Select archive to Restore on server: rghnc-sds:NO-a**

- The selected database came from rghnc-sds:NO-a on 01/17/2017 at 02:15:12 EST and contains the following components:
  - Configuration Data
  - Database Compatibility

**Ok**  **Cancel**

4. **Primary SDS NOAM GUI:** Wait for the restore to begin and track progress until the restore is complete

1. Wait 60 seconds for the restore to begin.
2. Monitor the Info tab under the **Status & Manage > Database** screen and look for the following message:
   
   Restore on <Active_NO_hostname> status MAINT_IN_PROGRESS.

3. Wait for the restore to complete by looking for the following message:
   
   Success: - Restore on rghnc-sds:NO-b status MAINT_CMD_SUCCESS.

   **Note:** Refresh the Info tab manually to see updated status by navigating to **Status & Manage > Database** again and selecting the Info tab.
Procedure 22. Restore Provisioning Database

5. **Primary SDS NOAM GUI: Uninhibit servers**

   Uninhibit all servers in the following staggered arrangement:
   1. Uninhibit active NOAM.
      - Refresh/monitor the Status & Manage > Database screen until a valid DB Level displays for the active NOAM.
   2. Uninhibit standby NOAM/Query server.
      - Refresh/monitor the Status & Manage > Database screen until a valid DB Level displays for the standby NOAM/Query server.
   3. Uninhibit active SOAMs.
      - Refresh/monitor the Status & Manage > Database screen until a valid DB Level displays for the active SOAMs.
   4. Uninhibit standby SOAMs/DPs.
      - Refresh/monitor the Status & Manage > Database screen until a valid DB Level displays for the standby SOAMs/DPs.

6. **Recover Pdbrelay (if needed)**

   Verify whether PDB Relay is **Enabled** by following the instructions in Appendix J Recover PDB Relay.

7. **Primary SDS NOAM GUI: Enable provisioning**

   Navigate to Status & Manage > Database and click **Enable Provisioning**.
Procedure 22. Restore Provisioning Database

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to Status &amp; Manage &gt; HA and click Edit.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the server, which was moved to forced standby in step 2, change Max HA Role to Active, and click OK.</td>
</tr>
</tbody>
</table>

### Main Menu: Status & Manage -> HA [Edit]

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Max Allowed HA Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rightnc-sds-NO-a</td>
<td>Active</td>
<td>The maximum desired HA Role for rightnc-sds-NO-a</td>
</tr>
<tr>
<td>rightnc-sds-NO-b</td>
<td>Active</td>
<td>The maximum desired HA Role for rightnc-sds-NO-b</td>
</tr>
<tr>
<td>rightnc-sds-GS</td>
<td>Observer</td>
<td>The maximum desired HA Role for rightnc-sds-GS</td>
</tr>
</tbody>
</table>

Appendix J. Recover PDB Relay

Procedure 23. Recover PDB Relay

1. **NOAM VIP console**: Determine if pdbrelay is enabled
   - Execute following command on console of Active NOAM server (accessed via the VIP) and compare the output:
     ```
     $ iqt -zhp -fvalue ProvOptions where "var='pdbRelayEnabled'"
     
     TRUE
     ```
   - Proceed to next step only if the result of above command is true.

2. **NOAM VIP GUI**: Disable pdbrelay
   - Unmark the PDB Relay Enabled checkbox on the SDS > Configuration > Options screen and click Apply.

3. **NOAM VIP Console**: Emergency restart (start from beginning of Cmd log)
   - Execute following command on console:
     ```
     $ iset -fvalue=0 ProvOptions where "var='pdbRelayMsgLogTimeStamp'"
     ```

4. **NOAM VIP GUI**: Enable pdbrelay
   - Mark the PDB Relay Enabled checkbox on the SDS > Configuration > Options screen and click Apply.
## Appendix K. SNMP Configuration

### Procedure 24. Configure SNMP

This workaround configures SNMP with SNMPv2c and SNMPv3 as the enabled versions for SNMP traps configuration since PMAC does not support SNMPv3.

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

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

<table>
<thead>
<tr>
<th>STEP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>(Workaround)</strong></td>
<td>NOAM VIP GUI: Login</td>
</tr>
</tbody>
</table>

**Note:** This workaround step should be performed only in the following cases:

1. If SNMP is not configured.
2. If SNMP is already configured and SNMPv3 is selected as enabled version.

**Note:** This is a workaround step to configure SNMP with 'SNMPv2c and SNMPv3' as the enabled versions for SNMP Traps configuration, since PMAC does not support SNMPv3.

1. If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server.
2. Open the web browser and enter a URL of:
   
   ```
   http://<Primary_NOAM_VIP_IP_Address>
   ```
3. Log into the NOAM GUI as the `guiadmin` user:

   ![Oracle System Login](image)
Procedure 24. 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 24. Configure SNMP

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 3. | NOAMP VIP: Enable traps from individual servers (optional) | **Note:** By default SNMP traps from MPs are aggregated and displayed at the active NOAMP. If, instead, you want every server to send its own traps directly to the NMS, then execute this procedure.

This procedure requires all servers, including MPs, to have an XMI interface on which the customer SNMP target server (NMS) is reachable.

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

   ![Main Menu](image) - Administration > Remote Servers > SNMP Trapping

   - General Options
   - Access Control
   - Software Management
   - Remote Servers
     - LDAP Authentication
     - SNMP Trapping
     - Data Export
     - DNS Configuration

   2. Make sure the **Enabled** checkbox is marked.

   - Traps from Individual Servers
     - Enabled

   3. Click **Apply** and verify the data is committed.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 4. | PMAC GUI: Update the TVOE host SNMP community string | **Note:** When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest on the PMAC control network are updated. All those servers that match the existing Site Specific Community String are not updated again until the string name is changed.

1. Establish an SSH session to the PMAC.
2. Login as **admusr** user:
3. Update the TVOE host SNMP community string with this command:

   ```bash
   $ sudo pmaccli setCommStr --accessType=rw -- commStr=<site specific value>
   ```

   **Note:** When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest on the PMAC control network are updated. All those servers that match the existing Site Specific Community String are not updated again until the string name is changed.
## Appendix L. Backup Directory

### Procedure 25. Backup Directory

<table>
<thead>
<tr>
<th>STEP #</th>
<th>NOAM/SOAM VIP Console: Determine if backup directory exists</th>
<th>NOAM/SOAM VIP Console: Create backup directory</th>
</tr>
</thead>
</table>
| 1. | **1.** Execute this command an active NOAM/SOAM server console (accessed using the VIP) and compare the output.  

   $ cd /var/TKLC/db/filemgmt/  
   $ ls -ltr  

   

   2. Look for the backup directory in the output.  

   3. Make sure the directory is already created with correct permission. The directory looks like this:  

   drwxrwx--- 2 awadmin awadm 4096 Dec 19 02:15 backup  

   4. If the directory is already there with correct permissions, then skip steps 2 and 3.  

   5. If directory does not have the correct permissions, then go to step 3. |  

| 2. | **1.** Go to the backup directory location.  

   cd /var/TKLC/db/filemgmt/  

   2. Create backup directory.  

   $ mkdir backup  

   3. Verify directory has been created.  

   $ ls -ltr /var/TKLC/db/filemgmt/backup |

**Note:** A No such file or directory error message should not display. The directory should show as empty with the total as 0 for content.
Procedure 25. Backup Directory

1. Verify directory has been created.
   
   ```bash
   $ ls -ltr /var/TKLC/db/filemgmt/backup
   ```

   **Note:** A *No such file or directory* error message should not display. The directory should show as empty with the total as 0 for content.

2. Change permissions for the backup directory.
   
   ```bash
   $ chmod 770 /var/TKLC/db/filemgmt/backup
   ```

3. Change ownership of backup directory.
   
   ```bash
   $ sudo chown -R awadmin:awadm /var/TKLC/db/filemgmt/backup
   ```

4. Directory displays as follows:
   
   ```bash
   drwxrwx--- 2 awadmin awadm        4096 Dec 22 02:15 backup
   ```

4. Copy the backup file to the backup directory.

   ```bash
   $ cp BACKUPFILE /var/TKLC/db/filemgmt/backup
   ```

2. Change permissions of files in the backup directory.
   
   ```bash
   $ chmod 666 Backup.*
   ```

3. Change ownership of files in the backup directory.
   
   ```bash
   $ sudo chown -R awadmin:awadm Backup.*
   ```

Appendix M. 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.