Oracle Communications Diameter Signaling Router Cloud Disaster Recovery 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 will not be 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: 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 on My Oracle Support (MOS) in Appendix G.
<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Author</th>
<th>Description</th>
<th>Approved (Yes/No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/07/2017</td>
<td>1</td>
<td>Kawal Sapra</td>
<td>Initial Release</td>
<td>No</td>
</tr>
<tr>
<td>12/25/2017</td>
<td>2</td>
<td>Kawal Sapra</td>
<td>Bug 27294758 fix</td>
<td>No</td>
</tr>
<tr>
<td>01/02/2018</td>
<td>3</td>
<td>Kawal Sapra</td>
<td>Review comments</td>
<td>No</td>
</tr>
<tr>
<td>01/10/2018</td>
<td>4</td>
<td>Kawal Sapra</td>
<td>Approved for 8.2</td>
<td>Yes</td>
</tr>
<tr>
<td>04/01/2018</td>
<td>5</td>
<td>J. Carlino</td>
<td>Format, Edit, and Post to OTN</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table of Contents

1. Introduction ........................................................................................................... 6
   1.1 References ........................................................................................................ 6
   1.2 Acronyms......................................................................................................... 6
   1.3 Terminology .................................................................................................... 7
   1.4 Optional Features .......................................................................................... 7

2. Installation Overview ........................................................................................... 8
   2.1 Complete Server Outage (All Servers) — Recovery Scenario 1 ......................... 9
   2.2 Partial Server Outage with One NOAM Server Intact and Both SOAMs Failed — Recovery Scenario 2 ................................................................. 9
   2.3 Partial Server Outage with Both NOAM Servers Failed and One SOAM Server Intact — Recovery Scenario 3 ................................................................. 9
   2.4 Partial Server Outage with NOAM and One SOAM Server Intact — Recovery Scenario 4 ......................... 9
   2.5 Partial Server Outage with Corrupt Database .................................................. 10

3. Procedure Overview ............................................................................................ 10
   3.1 Required Materials ......................................................................................... 10
   3.2 Disaster Recovery Strategy ........................................................................... 10

4. Disaster Recovery Procedure ............................................................................. 12
   4.1 Recovery Scenario 1 — Complete Server Outage ............................................ 12
   4.2 Recovery Scenario 2 — Partial Server Outage with One NOAM Server Intact and ALL SOAMs Failed ................................................................. 41
   4.3 Recovery Scenario 3 — Partial Server Outage with All NOAM Servers Failed and One SOAM Server Intact ................................................................. 66
   4.4 Recovery Scenario 4 — Partial Server Outage with One NOAM Server and One SOAM Server Intact ........................................................................ 85
   4.5 Recovery Scenario 5 — Both NOAM Servers Failed with DR-NOAM Available .... 100
   4.6 Recovery Scenario 6 — Database Recovery — Case 1 .................................... 107
   4.7 Recovery Scenario 6 — Database Recovery — Case 2 .................................... 110

5. Resolve User Credential Issues after Database Restore ........................................ 112
   5.1 Restore a Deleted User ................................................................................... 112
   5.2 Keep a Restored User ..................................................................................... 113
   5.3 Remove a Restored User ................................................................................. 115
   5.4 Restore a Modified User ............................................................................... 116
   5.5 Restore an Archive that does not contain a Current User ............................... 116

6. IDIH Disaster Recovery ....................................................................................... 121

Appendix A. Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost) ......................................................... 123
Appendix B. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost) ................................................................. 125

Appendix C. Inhibit A and B Level Replication on C-level Servers ...................... 127
Appendix D. Un-Inhibit A and B Level Replication on C-level Servers ................ 128
Appendix E. DSR Database Backup ..................................................................... 129
Appendix F. Check and Create Backup Directory .............................................. 132
Appendix G. My Oracle Support (MOS) ............................................................. 133

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

List of Figures
Figure 1. Determine Recovery Scenario ........................................................ 11

List of Procedures
Procedure 1. Recovery Scenario 1 ................................................................. 13
Procedure 2. Recovery Scenario 2 ................................................................. 41
Procedure 3. Recovery Scenario 3 ................................................................. 66
Procedure 4. Recovery Scenario 4 ................................................................. 85
Procedure 5. Recovery Scenario 5 ................................................................. 101
Procedure 6. Recovery Scenario 6 (Case 1) ................................................ 107
Procedure 7. Recovery Scenario 6 (Case 2) ................................................ 110
Procedure 8. Keep Restored User ................................................................. 113
Procedure 9. Remove the Restored User ....................................................... 115
Procedure 10. Restore an Archive That Does Not Contain a Current User .... 117
Procedure 11. IDIH Disaster Recovery Preparation ....................................... 121
Procedure 12. IDIH Disaster Recovery (Re-Install Mediation and Application Servers) ................................................................. 122
Procedure 13. Inhibit A and B Level Replication on C-level Servers ............ 123
Procedure 14. Un-Inhibit A and B Level Replication on C-Level Servers ....... 125
Procedure 15. Inhibit A and B Level Replication on C-level Servers ............ 127
Procedure 16. Un-Inhibit A and B Level Replication on C-level Servers ....... 128
Procedure 17. DSR Database Backup .......................................................... 129
Procedure 18. Backup Directory .................................................................. 132
1. Introduction

This document is a guide to describe procedures used to execute disaster recovery (DR) for Diameter Signaling Router (DSR) (3-tier deployments). This includes recovery of partial or a complete loss of one or more DSR 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: Note that failures can happen from the host or Infrastructure level. Different infrastructures have different approaches to recover VMs, which is not covered in this document. For example, VMWare has a vMotion feature, which can migrate VM from one host to another. Any such Infrastructure/Hypervisor related migrations/disaster recovery scenarios are out of scope of this document. This document covers the DR scenarios within the DSR application.

1.1 References

[1] DSR 8.2 Cloud Installation Guide

1.2 Acronyms

An alphabetized list of acronyms used in the document.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DR</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>DSR</td>
<td>Diameter Signaling Router</td>
</tr>
<tr>
<td>ESXi</td>
<td>Elastic Sky X Integrated</td>
</tr>
<tr>
<td>FABR</td>
<td>Full Address Based Resolution</td>
</tr>
<tr>
<td>iDIIH</td>
<td>Integrated Diameter Intelligence Hub</td>
</tr>
<tr>
<td>IPFE</td>
<td>IP Front End</td>
</tr>
<tr>
<td>IWF</td>
<td>Inter Working Function</td>
</tr>
<tr>
<td>NAPD</td>
<td>Network Architecture Planning Diagram</td>
</tr>
<tr>
<td>NOAM</td>
<td>Network Operations, Administration &amp; Maintenance</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OVA</td>
<td>Open Virtualization Appliance</td>
</tr>
<tr>
<td>OVM-M</td>
<td>Oracle Virtual Machine Manager</td>
</tr>
<tr>
<td>OVM-S</td>
<td>Oracle Virtual Machine Server</td>
</tr>
</tbody>
</table>
### Table 2. Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base software</td>
<td>Base software includes deploying the VM image.</td>
</tr>
<tr>
<td>Failed server</td>
<td>A failed server in disaster recovery context refers to a VM that has suffered partial or complete software failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-install the software.</td>
</tr>
<tr>
<td>Software Centric</td>
<td>The business practice of delivering an Oracle software product, while relying upon the customer to procure the requisite hardware components. Oracle provides the hardware specifications, but does not provide the hardware or hardware firmware, and is not responsible for hardware installation, configuration, or maintenance.</td>
</tr>
<tr>
<td>Enablement</td>
<td>The business practice of providing support services (hardware, software, documentation, etc.) that enable a 3rd party entity to install, configuration, and maintain Oracle products for Oracle customers.</td>
</tr>
</tbody>
</table>

### Table 3. Optional Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Documents</th>
</tr>
</thead>
<tbody>
<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>Range Based Address Resolution (RBAR)</td>
<td>DSR RBAR Feature Activation Procedure</td>
</tr>
<tr>
<td>Map-Diameter Interworking (MAP-IWF)</td>
<td>DSR MAP-Diameter IWF Feature Activation Procedure</td>
</tr>
<tr>
<td>Policy and Charging Application (PCA)</td>
<td>DSR PCA Activation Procedure</td>
</tr>
<tr>
<td>Host Intrusion Detection System (HIDS)</td>
<td>DSR Security Guide, Section 3.2</td>
</tr>
</tbody>
</table>
2. Installation Overview

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

Table 4. Recovery Scenarios

<table>
<thead>
<tr>
<th>Category</th>
<th>When to Use</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>4.1 Recovery Scenario 1 — Complete Server Outage</td>
<td>• All SOAM servers failed</td>
</tr>
<tr>
<td></td>
<td>• 1 or more MP servers failed</td>
</tr>
<tr>
<td>Recovery of one or more servers with at least one NOAM server intact</td>
<td>• 1 or more NOAM servers intact</td>
</tr>
<tr>
<td>Recovery Scenario 2 — Partial Server Outage with One NOAM Server Intact and ALL SOAMs Failed</td>
<td>• All SOAM servers or MP servers failed</td>
</tr>
<tr>
<td>Recovery of the NOAM pair with one or more SOAM servers intact</td>
<td>• All NOAM servers failed</td>
</tr>
<tr>
<td>Recovery Scenario 3 — Partial Server Outage with All NOAM Servers Failed and One SOAM Server Intact</td>
<td>• 1 or more SOAM servers intact</td>
</tr>
<tr>
<td>Recovery of one or more server with at least one NOAM and one SOAM server intact</td>
<td>• 1 or more NOAM servers intact</td>
</tr>
<tr>
<td>Recovery Scenario 4 — Partial Server Outage with One NOAM Server and One SOAM Server Intact</td>
<td>• 1 or more SOAM servers intact</td>
</tr>
<tr>
<td></td>
<td>• 1 or more MP servers failed</td>
</tr>
<tr>
<td>Recovery of the NOAM pair with DR-NOAM available and one or more SOAM servers intact</td>
<td>• All NOAM servers failed</td>
</tr>
<tr>
<td>4.5 Recovery Scenario 5 — Both NOAM Servers Failed with DR-NOAM Available</td>
<td>• 1 or more SOAM servers intact</td>
</tr>
<tr>
<td></td>
<td>• DR-NOAM available</td>
</tr>
<tr>
<td>Recovery of one or more server with corrupt databases that cannot be restored via replication from the active parent node</td>
<td>• Server has a corrupted database</td>
</tr>
<tr>
<td>4.6 Recovery Scenario 6 — Database Recovery</td>
<td>• Server is intact</td>
</tr>
<tr>
<td></td>
<td>• Database gets corrupted on the server</td>
</tr>
<tr>
<td></td>
<td>• Replication is occurring to the server with corrupted database</td>
</tr>
<tr>
<td>4.6 Recovery Scenario 6 — Database Recovery — Case 1</td>
<td>• Server is intact</td>
</tr>
<tr>
<td></td>
<td>• Database gets corrupted on the server</td>
</tr>
<tr>
<td></td>
<td>• Latest Database backup of the corrupt server is NOT present</td>
</tr>
<tr>
<td></td>
<td>• Replication is inhibited (either manually or because of Comcol upgrade barrier)</td>
</tr>
</tbody>
</table>

Executing a disaster recovery procedure 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 failure to the extent that it cannot restart or be returned to normal operation and requires intrusive activities to re-deploy base software.

2.1 Complete Server Outage (All Servers) — Recovery Scenario 1

Scenario:
- All NOAM servers failed
- All SOAM servers failed
- 1 or more MP servers failed

This is the worst case scenario where all the servers in the network have suffered complete software failure. The servers are recovered using OVA images then restoring database backups to the active NOAM and SOAM servers.

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

2.2 Partial Server Outage with One NOAM Server Intact and Both SOAMs Failed — Recovery Scenario 2

Scenario:
- 1 or more NOAM servers intact
- All SOAM servers failed
- 1 or more MP servers failed

This case assumes that at least one NOAM servers intact. All SOAM servers have failed and are recovered using OVA images. 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 — Recovery Scenario 3

Scenario:
- All NOAM servers failed
- 1 or more SOAM servers intact

Database is restored on the NOAM and replication will recover the database of the remaining.

2.4 Partial Server Outage with NOAM and One SOAM Server Intact — Recovery Scenario 4

Scenario:
- 1 or more NOAM servers intact
- 1 or more SOAM servers intact
- 1 or more MP servers failed
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 software. Database replication from the active NOAM and SOAM servers will recover the database to all servers.

2.5 Partial Server 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 hard copies 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 network element XML file used for the VMs initial configuration.

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

3.2 Disaster Recovery Strategy

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

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

!!WARNING!! Contact My Oracle Support (MOS) before executing this procedure to ensure the proper recovery planning is performed.

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

**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 the disaster, it may be necessary to deviate from the documented process.

Disaster recovery requires configuring the system as it was before the disaster and restoring operational information. There are eight (8) distinct procedures to choose from depending on the type of recovery needed. Only one of these should be followed (not all).

!!WARNING!! When you need to restore the database backup for NOAM and SOAM servers in any of the recovery scenarios, the backup directory may not exist in the system since it is in DRed. In this case, refer to Appendix F Check and Create Backup Directory for issues not fixed in this release for the steps to check and create the backup directory.

File format for recovery is when the backup was taken. Generally, the backup file is in this format:

```
Backup.DSR.HPC02-NO2.FullDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2
```

4.1 Recovery Scenario 1 — Complete Server Outage

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

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

- Recover base software for all VMs
  - Recover the virtual machines hosting the NOAMs and SOAMs
  - Recover the active NOAM server by recovering the NOAMs base software
  - Recover the NOAM database
  - Reconfigure the application
- Recover the standby NOAM server by recovering base software. For a non-HA deployment, this can be skipped
  - Reconfigure the DSR application
Recover all SOAM and MP servers by recovering software. In a non-HA deployment, the standby/spare SOAM servers can be skipped

- Recover the SOAM database
- Reconfigure the DSR Application
- Reconfigure the signaling interface and routes on the MPs. The DSR software automatically reconfigures the signaling interface from the recovered database
- Restart process and re-enable provisioning replication

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

**Procedure 1. Recovery Scenario 1**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Workaround</td>
<td>Refer to Appendix F to Check and Create Backup Directory.</td>
</tr>
<tr>
<td>2.</td>
<td>Gather required materials</td>
<td>Gather the documents and required materials listed in section 3.1 Required Materials.</td>
</tr>
</tbody>
</table>
| 3.     | Recover the failed software | **For VMWare based deployments:**
|        |             | 1. For NOAMs, execute the following procedures from reference [1]:
|        |             | a. Procedure 1 (VMWare) Import DSR OVA
|        |             |   If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.
|        |             | b. Procedure 2 (VMWare Only) Configure NOAM Guests Based On Resource Profile
|        |             | 2. For SOAMs, execute the following procedures from reference [1]:
|        |             | a. Procedure 1 (VMWare) Import DSR OVA
|        |             |   If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.
|        |             | b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile
|        |             | 3. For failed MPs, execute the following procedures from reference [1]:
|        |             | a. Procedure 1 (VMWare) Import DSR OVA
|        |             |   If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.
|        |             | b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile
|        |             | **For KVM/OpenStack based deployments:**
|        |             | 1. For NOAMs, execute the following procedures from reference [1]:
|        |             |
Procedure 1. Recovery Scenario 1

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| a. | Procedure 4 (KVM/OpenStack) Import DSR OVA  
    If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA. |
| b. | Procedure 5 (KVM/OpenStack Only) Configure NOAM Guests Based On Resource Profile |

2. For SOAMs, execute the following procedures from reference [1]:
   a. Procedure 4 (KVM/OpenStack) Import DSR OVA  
      If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.  
   b. Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile

3. For failed MPs, execute the following procedures from reference [1]:
   a. Procedure 4 (KVM/OpenStack) Import DSR OVA  
      If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.  
   b. Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile

**For OVM-S/OVM-M based deployments:**
1. Execute the following procedures from reference [1]:
   a. Procedure 7 (OVM-S/OVM-M) Import DSR OVA and Prepare for VM creation  
   b. Procedure 8 (OVM-S/OVM-M) Configure each DSR VM  
      While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs).

4. □ 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. From required materials list in section 3.1 Required Materials; use site survey documents and Network Element report (if available) to determine network configuration data.

5. □ Execute DSR installation procedure for the first NOAM
   **Verify the network data for network elements.**  
   **Note:** Use the backup copy of network configuration data and site surveys (Step 2).  
   • Execute Configure the First NOAM NE and Server from reference [1].  
   • Execute Configure the NOAM Server Group from reference [1].
## Procedure 1. Recovery Scenario 1

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

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

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

2. Select the active NOAM server.

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

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

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

6. Click **Upload**.

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

8. **NOAM GUI:** Disable provisioning

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

2. Click **Disable Provisioning.**

3. A confirmation window displays. Click **OK** to disable provisioning.
   - Disable provisioning.
   - Are you sure?

   ![Confirmation Window](image)
Procedure 1. Recovery Scenario 1

9. NOAM GUI: Verify the archive contents and database compatibility

1. Select the Active NOAM server and click Compare.

2. Click the button for the restored database file uploaded as a part of step 7. of this procedure.

   ![Database Compare](image)

   Select archive to compare on server: ZombieNOAM1
   Archive: backup/Backup.ds rerZombieNOAM1.Configurations

   Ok Cancel

3. Verify the output window matches the screen below.

   ![Database Archive Compare](image)

   The selected database came from ZombieNOAM1 on 10/10/2016 at 10:36:44 EDT and contains the following:

   **Archive Contents**
   - Configuration data.

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

   **Node Type Compatibility**
   - The node types are compatible.

   **Topology Compatibility**
   - THE TOPOLOGY IS NOT COMPATIBLE. CONTACT ORACLE CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE.

   Discrepancies:
   - Server A160.012 on network XHI is in the current topology but not the selected backup file.
   - Server A160.012 on network XHI is in the current topology but not the selected backup file.
   - Server A0630.035 on network XHI is in the selected backup file but not the current topology.
   - Server B2934.011 on network XHI is in the selected backup file but not the current topology.
   - Server C0422.200 on network XHI is in the selected backup file but not the current topology.

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

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

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

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

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

4. If the verification is successful, click **Back**.
Procedure 1. Recovery Scenario 1

1. From **Status & Manage > Database**.
   
   ![Status & Manage Tree](image)

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

   ![Active NOAM Server Selection](image)

   2. Select the proper backup provisioning and configuration file.

   ![Backup Selection Dialog](image)

   3. Click **OK**.

   ![Database Restore Confirm](image)

   4. Click **OK**.

   ![Database Restore Confirm](image)

   5. If you get errors related to the warnings highlighted in the previous step, that is expected. If no other errors are displayed, mark the **Force** checkbox as shown above and Click **OK** to proceed with the DB restore.

   ![Force Checkbox](image)

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 11.  | **NOAM VIP GUI: Login**<br>1. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of:  
   http://<Primary_NOAM_VIP_IP_Address><br>2. Login as the guiadmin user:  
   ![Oracle System Login](image)
| 12.  | **NOAM VIP GUI: Monitor and confirm database restoral**<br>1. Wait for 5-10 minutes for the system to stabilize with the new topology:<br>2. Monitor the Info tab for Success. This indicates the restore is complete and the system is stabilized.<br>Ignore these alarms for NOAM and MP servers until all the servers are configured:<br>- Alarms with Type Column as REPL, COLL, HA (with mate NOAM), DB (about Provisioning Manually Disabled).<br>Note: Do not pay attention to alarms until all the servers in the system are completely restored.<br>Note: The Configuration and Maintenance information is in the same state it was when backed up during initial backup. |
| 13.  | **Active NOAM: Login**<br>Log into the recovered active NOAM using SSH terminal as admusr user. |
| 14.  | **NOAM VIP GUI: Recover standby NOAM**<br>Install the second NOAM server by executing these procedures from reference [1]:<br>- Execute Configure the Second NOAM Server, steps 3-5 and 7<br>- Execute Configure the NOAM Server Group, step 4 |
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 15. | Active NOAM: Correct the Recognized Authority table | 1. Establish an SSH session to the active NOAM and login as **admusr**.  
2. Execute the following command:  

```bash  
sudo top.setPrimary  
- Using my cluster: A1789  
- Updating A1789.022: <DSR_NOAM_B_hostname>  
- Updating A1789.144: <DSR_NOAM_A_hostname>  
``` |
| 16. | NOAM VIP GUI: Restart DSR application | 1. Navigate to **Status & Manage > Server**.  
2. Select the recovered standby NOAM server and click **Restart**. |
| 17. | 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 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
</table>
| 18. | **NOAM VIP GUI:**  
Perform key exchange with export server | 1. Navigate to **Administration > Remote Servers > Data Export.**
   
   - **Administration**
     - **General Options**
     - **Access Control**
     - **Software Management**
     - **Remote Servers**
       - **LDAP Authentication**
       - **SNMP Trapping**
       - **Data Export**
       - **DNS Configuration**
   
   2. Click **SSH Key Exchange** at the bottom of the screen.
   
   ![SSH Key Exchange](image)
   
   3. Type the **Password** and click **OK.**
   
   ![Password Input](image) |
| 19. | **NOAM VIP GUI:**  
Stop replication to the C-level servers of this site | **!!Warning!!**

Before continuing this procedure, replication to C-level servers at the SOAM site being recovered MUST be inhibited.

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 A 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. |
| 20. | Recover active SOAM server | Install the SOAM servers by executing Configure the SOAM Servers, steps 1 and 3-7 from reference [1].

**Note:** Wait for the server to reboot. |
Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21. NOAM VIP GUI:</td>
<td>Restart DSR application</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to Status &amp; Manage &gt; Server.</td>
</tr>
<tr>
<td>2.</td>
<td>Select the recovered active SOAM server and click Restart.</td>
</tr>
<tr>
<td>22. NOAM VIP GUI:</td>
<td>Upload the backed up SOAM database file</td>
</tr>
<tr>
<td>3.</td>
<td>Navigate to Status &amp; Manage &gt; Files.</td>
</tr>
<tr>
<td>4.</td>
<td>Select the active SOAM server tab. Click Upload and select the file SO Provisioning and Configuration file backed up after initial installation and provisioning.</td>
</tr>
<tr>
<td>5.</td>
<td>Click Browse and locate the backup file.</td>
</tr>
<tr>
<td>6.</td>
<td>Check This is a backup file checkbox.</td>
</tr>
<tr>
<td>7.</td>
<td>Click Upload.</td>
</tr>
</tbody>
</table>

The file takes a few seconds to upload depending on the size of the backup data.
Procedure 1. Recovery Scenario 1

23. Recovered SOAM GUI: Login

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

http://<Recovered_SOAM_IP_Address>

2. Login as the guiadmin user:

![Oracle System Login](image)

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

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

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

| Recovery SOAM GUI: Verify the archive contents and database compatibility |  
|---|---|
| 24. |  
| **Procedure 1. Recovery Scenario 1** | **1. Navigate to Status &Manage > Database.**  
| | - Navigate to **Status & Manage > Database.**  
| | - Select the **Active SOAM** server and click **Compare.**  
| | - Click the button for the restored database file uploaded as a part of step 22. of this procedure.  
| | - Verify the output window matches the screen below.  
| | - **Database Archive Compare**  
| | - The selected database came from ZombieSOAM1 on 1  
| | | - **Archive Contents:** Configuration data.  
| | | - **Database Compatibility:** The databases are compatible.  
| | **Note:** Archive Contents and Database Compatibilities must be the following:  
| | **Database Compatibility:** The topology should be compatible minus the nodeID.  
| | **Note:** We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in topology compatibility.  
| | - If the verification is successful, click **Back.**  
| | | **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. |
## Procedure 1. Recovery Scenario 1

| 25. | **Recovered SOAM GUI:**  
Restore the database  

| 1. | Select the Active SOAM server and click **Restore**.  
2. | Select the proper back up provisioning and configuration file.  

|  | **Database Compare**  
Select archive to compare on set  
Archive * backup/backup.dsr2  
**Ok** **Cancel**  

| 3. | Click **OK**. The following confirmation screen displays.  

|  | **Database Restore Confirm**  
Compatible archive.  

|  | The selected database came from Zombi  
| Archive Contents  
Configuration data  
Database Compatibility  
The databases are compatible.  

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

**Note:** After the restore has started, the user is logged out of XMI SOAM GUI since the restored Topology is old data.  

| 26. | **Recovered SOAM GUI:**  
Monitor and confirm database restoral  

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

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

**Note:** The Configuration and Maintenance information is in the same state it was when backed up during initial backup.
## Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 27.  | NOAM VIP GUI: Login | 1. Establish a GUI session on the NOAM server by using the VIP 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: |
| 28.  | NOAM VIP GUI: Recover the remaining SOAM servers | Executing Configure the SOAM Servers, steps 1 and 3-6, from reference [1].  
   **Note:** Wait for server to reboot before continuing. |
| 29.  | NOAM VIP GUI: Restart DSR application on remaining SOAM server(s) | 1. Navigate to Status & Manage > Server.  
   - Status & Manage  
     - Network Elements  
     - Server  
     - HA  
     - Database  
     - KPIs  
     - Processes  
   2. Select the recovered standby SOAM server and click Restart. |
Procedure 1. Recovery Scenario 1

30. **NOAM VIP GUI:**
Set HA on recovered standby SOAM server, if applicable

*Note:* For non-HA sites, skip this step

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

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>32.</th>
<th><strong>Active NOAM:</strong> Perform key exchange between the active-NOAM and recovered servers (DA-MP, SBRs, IPFE, SS7-MP, and vSTP-MP)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Establish an SSH session to the C-level server being recovered and login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Execute following command to set shared memory to unlimited:</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo shl.set -m 0</code></td>
</tr>
<tr>
<td></td>
<td>3. Execute Configure the MP Virtual Machines, steps 1, 11-14 (and 15 if required) of reference [1] for each server that has been recovered.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>33.</th>
<th><strong>NOAM VIP GUI:</strong> Restart DSR application</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Server</strong>.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diagram" /></td>
</tr>
<tr>
<td></td>
<td>2. Select the recovered standby NOAM server and click <strong>Restart</strong>.</td>
</tr>
</tbody>
</table>
Procedure 1. Recovery Scenario 1

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

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

1. Navigate to Status & Manage > Database.

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

2. If the Repl Status is set to Inhibited, click Allow Replication using this order:
   - Active NOAM Server
   - Standby NOAM Server
   - Active SOAM Server
   - Standby SOAM Server
   - Spare SOAM Server (if applicable)
   - MP/IPFE servers (if MPs are configured as active/standby, start with the Active MP; otherwise, the order of the MPs does not matter)

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

<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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **35.** | **NOAM VIP GUI:**  
Set HA on all C-level servers |
|   | 1. Navigate to **Status & Manage > HA.**  
   ![Status & Manage screen]  
   - **Network Elements**  
   - **Server**  
   - **HA**  
   - **Database**  
   - **KPIs**  
   - **Processes**  
   - **Tasks**  
   - **Files**  
   2. Click **Edit** at the bottom of the screen.  
   3. For each server with a Max Allowed HA Role set to OOS, set it to **Active.**  
   **Modifying HA attributes**  
   ![Modifying HA attributes](image)  
   4. Click **OK.** |
| **36.** | **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:  
   ```bash  
   $ keyexchange admusr@<Recovered Server Hostname>  
   ```  
   **Note:** If an export server is configured, perform this step. |
| **37.** | **Active NOAM:**  
Activate optional features  
**Note for PCA Activation:**  
If you have PCA installed in the system being recovered, re-activate PCA by executing PCA Activation on Entire Server on Recovered NOAM Server and PCA Activation on Active SOAM Server from [3].  
**Note:** While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:  
   ```bash  
   iload#31000{S/W Fault}  
   ```  
   **Note:** If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.  
   Refer to section 1.4 Optional Features to activate any features previously activated. |
Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>NOAM VIP GUI: Fetch and store the database report for the newly restored data and save it</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Database</strong>.</td>
</tr>
<tr>
<td>- Stream</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>2. Select the active NOAM server and click <strong>Report</strong>.</td>
</tr>
</tbody>
</table>

The following screen displays:

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

```
<table>
<thead>
<tr>
<th>dsn Database Status Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Active Network OAM6P on host ZombieNOAM1</td>
</tr>
<tr>
<td>Report Version: 8.6.0.0.0-30.9.0</td>
</tr>
<tr>
<td>User: quadmin</td>
</tr>
</tbody>
</table>

---

General

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

Capacities and Utilisation

- Disk Utilisation: 8.4%
- Memory Utilisation: 0.0%
```

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

39. **Active NOAM**: Verify replication between servers

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

2. Execute this command:

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

Output:

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

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

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

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

<table>
<thead>
<tr>
<th>Network Element</th>
<th>Server</th>
<th>Role</th>
<th>OAM Max HA Role</th>
<th>Application Max HA Role</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOAM_NE</td>
<td>SO1</td>
<td>System OAM</td>
<td>Standby</td>
<td>N/A</td>
<td>Normal</td>
</tr>
<tr>
<td>SOAM_NE</td>
<td>SO2</td>
<td>System OAM</td>
<td>Active</td>
<td>N/A</td>
<td>Normal</td>
</tr>
<tr>
<td>NOAM_NE</td>
<td>NO2</td>
<td>Network OAM&amp;P</td>
<td>Standby</td>
<td>N/A</td>
<td>Normal</td>
</tr>
<tr>
<td>SOAM_NE</td>
<td>DAMP1</td>
<td>MP</td>
<td>Active</td>
<td>Active</td>
<td>Normal</td>
</tr>
<tr>
<td>NOAM_NE</td>
<td>NO1</td>
<td>Network OAM&amp;P</td>
<td>Active</td>
<td>N/A</td>
<td>Normal</td>
</tr>
</tbody>
</table>
Procedure 1. Recovery Scenario 1

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

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

   ![Status and Manage](image)

   **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>

42. **NOAM GUI**: Enable provisioning

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

   ![Status and Manage](image)

2. Click **Enable Provisioning**.

3. A confirmation window displays. Click **OK** to enable provisioning.
### Procedure 1. Recovery Scenario 1

#### 43. **SOAM VIP GUI:** Verify the local node info

1. Navigate to **Diameter > Configuration > Local Node.**
   - [Diameter](#) > [Configuration](#) > [Local Nodes](#)

   2. Verify all the local nodes are shown.

#### 44. **SOAM VIP GUI:** Verify the peer node info

1. Navigate to **Diameter > Configuration > Peer Node.**
   - [Diameter](#) > [Configuration](#) > [Peer Nodes](#)

   2. Verify all the peer nodes are shown.

#### 45. **SOAM VIP GUI:** Verify the connections info

1. Navigate to **Diameter > Configuration > Connections.**
   - [Diameter](#) > [Configuration](#) > [Connections](#)

   2. Verify all the connections are shown.
### Procedure 1. Recovery Scenario 1

| 46. For vSTP Only | 1. Log into the SOAM VIP server console as **admusr**.  
| SOAM VIP Server Console (Optional): Verify vSTP MP local node information | 2. Execute the following command:  
| | [admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts  
| | 3. Verify the output similar to this output. |

```json
{
    "data": {
        "configurationLevel": "10",
        "localHostName": "AUTLocalHost1",
        "localHostPort": 4444,
        "localHostPriIPAddress": "145.168.100.2",
        "localHostSecIPAddress": "145.168.111.1"
    },
    "links": {},
    "messages": [],
    "status": true
}
```

| 47. For vSTP Only | 1. Log into the SOAM VIP server console as **admusr**.  
| SOAM VIP Server Console (Optional): Verify vSTP MP remote nodes information | 2. Execute the following command  
| | [admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts  
| | 3. Verify the output similar to this output. |

```json
{
    "data": {
        "remoteHostName": "AUTRemoteHost1",
        "remoteHostPort": 4444,
        "remoteHostPriIPAddress": "1.1.1.6",
        "remoteHostSecIPAddress": "1.1.1.7"
    },
    "links": {},
    "messages": [],
    "status": true
}
```
Procedure 1. Recovery Scenario 1

48. For vSTP Only
   SOAM VIP Server Console (Optional): Verify the vSTP MP connections information

1. Log into the SOAM VIP server console as admusr.
2. Execute the following command
   ```bash
   [admusr@SOAM1 ~]$ mmiclient.py /vstp/connections
   ```
3. Verify the output similar to this output.
   
   ```json
   "data": [
   {
   "configurationLevel": "13",
   "connCfgSetName": "Default",
   "connectionMode": "Server",
   "connectionType": "M3ua",
   "localHostName": "AUTLocalHost1",
   "name": "AUTLinkTestConn1",
   "remoteHostName": "AUTRemoteHost1"
   },
   {
   "configurationLevel": "14",
   "connCfgSetName": "Default",
   "connectionMode": "Server",
   "connectionType": "M3ua",
   "localHostName": "AUTLocalHost2",
   "name": "AUTLinkTestConn2",
   "remoteHostName": "AUTRemoteHost1"
   }],
   "links": {},
   "messages": [],
   "status": true
   }
   ```

49. MP Servers: Disable SCTP Auth Flag
   For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [1].
   Execute this procedure on all failed MP servers.

50. SOAM VIP GUI: Enable connections, if needed

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

**Note:** If a Disaster Recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution.
### Procedure 1. Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 51. | **SOAM VIP GUI:** Enable optional features  
1. Navigate to **Diameter > Maintenance > Applications.**  
   - [Maintenance](#)  
     - [Route Lists](#)  
     - [Route Groups](#)  
     - [Peer Nodes](#)  
     - [Connections](#)  
     - [Egress Throttle Groups](#)  
     - [Applications](#)  
2. Select the optional feature application configured in step 37.  
3. Click **Enable.**  
   ![Enable](#) ![Disable](#) ![Pause updates](#) |
| 52. | **SOAM VIP GUI:** Re-enable transports, if needed  
1. Navigate to **Transport Manager > Maintenance > Transport.**  
   - [Transport Manager](#)  
     - [Configuration](#)  
     - [Maintenance](#)  
     - [Transport](#)  
2. Select each transport and click **Enable.**  
   ![Enable](#) ![Disable](#) ![Block](#)  
3. Verify the Operational Status for each transport is **Up.** |
| 53. | **SOAM VIP GUI:** Re-enable MAPIWF application, if needed.  
   *This step is applicable when the MAP-IWF is activated.*  
1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users.**  
   - [SS7/Sigtran](#)  
     - [Configuration](#)  
     - [Maintenance](#)  
     - [Local SCCP Users](#)  
     - [Remote Signaling Points](#)  
     - [Remote MTP3 Users](#)  
     - [Linksets](#)  
     - [Links](#)  
2. Click the **Enable** button corresponding to MAPIWF Application Name.  
   ![Enable](#) ![Disable](#)  
3. Verify the SSN Status is **Enabled.** |
## Procedure 1. Recovery Scenario 1

### 54. SOAM VIP GUI: Re-enable links, if needed.
- Navigate to SS7/Sigtran > Maintenance > Links.
  - Click Enable for each link.
- Verify the Operational Status for each link is Up.

This step is applicable when the MAP-IWF is activated.

### 55. SOAM VIP GUI: Examine all alarms
- Navigate to Alarms & Events > View Active.
  - Examine all active alarms and refer to the on-line help on how to address them.
  - If needed, contact My Oracle Support (MOS).

### 56. NOAM VIP GUI: Examine all alarms
- Navigate to Alarms & Events > View Active.
  - Examine all active alarms and refer to the on-line help on how to address them.
  - If needed, contact My Oracle Support (MOS).

### 57. Restore GUI usernames and passwords
- If applicable, execute steps in section 5 to recover the user and group information restored.

### 58. Backup and archive all the databases from the recovered system
- Execute Appendix E DSR Database Backup to back up the Configuration databases.
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 for 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 for software. Database replication from the active NOAM server will recover the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures’ detailed steps are in Procedure 2. The major activities are summarized as follows:

- Recover standby NOAM server (if needed) by recovering software and the database
  - Recover the software
- Recover active SOAM server by recovering software
  - Recover the software
  - Recover the database
- Recover any failed SOAM and MP servers by recovering software
  - Recover the software
  - The database has already been restored at the active SOAM server and does not require restoration at the SO and MP servers

Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Workaround</td>
<td>Refer to Appendix F to Check and Create Backup Directory.</td>
</tr>
<tr>
<td>2.</td>
<td>Gather required materials</td>
<td>Gather the documents and required materials listed in section 3.1 Required Materials.</td>
</tr>
</tbody>
</table>
### Procedure 2. Recovery Scenario 2

<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 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

<table>
<thead>
<tr>
<th>Log In</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter your username and password to log in</td>
</tr>
<tr>
<td>Username:</td>
</tr>
<tr>
<td>Password:</td>
</tr>
<tr>
<td>[ ] Change password</td>
</tr>
<tr>
<td>Log In</td>
</tr>
</tbody>
</table>

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**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td><strong>Active NOAM:</strong> Set failed servers to OOS</td>
</tr>
</tbody>
</table>

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

### Modifying HA attributes

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

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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td><strong>Recover the failed software</strong></td>
</tr>
</tbody>
</table>

**For VMWare based deployments:**

1. For NOAMs, execute the following procedures from reference [1]:
   a. Procedure 1 (VMWare) Import DSR OVA
      If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.
   b. Procedure 2 (VMWare Only) Configure NOAM Guests Based On Resource Profile
2. For SOAMs, execute the following procedures from reference [1]:
   a. Procedure 1 (VMWare) Import DSR OVA
      If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.
   b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile
3. For failed MPs, execute the following procedures from reference [1]:
   a. Procedure 1 (VMWare) Import DSR OVA
      If OVA is already imported and present in the Infrastructure Manager,
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>6.</th>
<th>Repeat</th>
<th>If necessary, repeat step 5. for all remaining servers.</th>
</tr>
</thead>
</table>

- Skip this procedure to import OVA.
- Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile

### For KVM/OpenStack based deployments:

1. For NOAMs, execute the following procedures from reference [1]:
   - Procedure 4 (KVM/OpenStack) Import DSR OVA
     - If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.
   - Procedure 5 (KVM/OpenStack Only) Configure NOAM Guests Based On Resource Profile

2. For SOAMs, execute the following procedures from reference [1]:
   - Procedure 4 (KVM/OpenStack) Import DSR OVA
     - If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.
   - Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile

3. For failed MPs, execute the following procedures from reference [1]:
   - Procedure 4 (KVM/OpenStack) Import DSR OVA
     - If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.
   - Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile

### For OVM-S/OVM-M based deployments:

1. Execute the following procedures from reference [1]:
   - Procedure 7 (OVM-S/OVM-M) Import DSR OVA and Prepare for VM creation
   - Procedure 8 (OVM-S/OVM-M) Configure each DSR VM
     - While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs).

Repeat If necessary, repeat step 5. for all remaining servers.
## Procedure 2. Recovery Scenario 2

### 7. NOAM VIP GUI: Login

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

   ![Oracle System Login](image)

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

2. Login as the `guiadmin` user:

   ![Oracle Login](image)

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

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

### 8. NOAM VIP GUI: Recover standby NOAM

Install the second NOAM server by executing these procedures from reference [1]:

- Execute Configure the Second NOAM Server, steps 3-5 and 7
- Execute Configure the NOAM Server Group, step 4

**Note:** If topology or nodeID alarms are persistent after the database restore, refer to Appendix F to Check and Create Backup Directory.
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td><strong>NOAM VIP GUI:</strong> Restart DSR application</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Server.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Status &amp; Manage" /></td>
</tr>
<tr>
<td></td>
<td>2. Select the recovered standby NOAM server and click <strong>Restart.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Restart" /></td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong> on confirmation screen.</td>
</tr>
<tr>
<td>10.</td>
<td><strong>NOAM VIP GUI:</strong> Set HA on standby NOAM</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; HA.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Status &amp; Manage" /></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Edit.</strong></td>
</tr>
<tr>
<td></td>
<td>3. Select the standby NOAM server and set it to <strong>Active.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Active" /></td>
</tr>
<tr>
<td></td>
<td>Click <strong>OK.</strong></td>
</tr>
<tr>
<td>11.</td>
<td><strong>NOAM VIP GUI:</strong> Stop replication to the C-level servers of this site</td>
</tr>
<tr>
<td></td>
<td><strong>!!Warning!!</strong></td>
</tr>
<tr>
<td></td>
<td>Before continuing this procedure, replication to C-level servers at the SOAM site being recovered MUST be inhibited.</td>
</tr>
<tr>
<td></td>
<td>Failure to inhibit replication to the working C-level servers results in the database being destroyed!</td>
</tr>
<tr>
<td></td>
<td>If the spare SOAM is also present in the site and lost, execute Appendix A 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.</td>
</tr>
<tr>
<td></td>
<td>If the spare SOAM is NOT deployed in the site, execute Appendix C Inhibit A and B Level Replication on C-level Servers to inhibit replication to working C-level servers before continuing.</td>
</tr>
<tr>
<td>12.</td>
<td><strong>Recover active SOAM server</strong></td>
</tr>
<tr>
<td></td>
<td>Install the SOAM servers by executing Configure the SOAM Servers, steps 1 and 3-7 from reference [1].</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Wait for the server to reboot.</td>
</tr>
</tbody>
</table>
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>No.</th>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>13.</strong></td>
<td><strong>NOAM VIP GUI:</strong> Set HA on active NOAM</td>
<td></td>
</tr>
</tbody>
</table>

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

   ![Diagram](image1)

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

2. Click **Edit** at the bottom of the screen.
3. Select the active NOAM server and set it to **Active.**

   ![Modifying HA attributes](image2)

4. Click **OK.**

| **14.** | **NOAM VIP GUI:** Restart DSR application | 

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

   ![Diagram](image3)

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

   ![Restart button](image4)
Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>15.</th>
<th>NOAM VIP GUI: Upload the backed up SOAM database file</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Navigate to Status &amp; Manage &gt; Files.</td>
</tr>
<tr>
<td>4.</td>
<td>Select the active SOAM server tab. Click Upload and select the file SO Provisioning and Configuration file backed up after initial installation and provisioning.</td>
</tr>
<tr>
<td>5.</td>
<td>Click Browse and locate the backup file.</td>
</tr>
<tr>
<td>6.</td>
<td>Check This is a backup file checkbox.</td>
</tr>
<tr>
<td>7.</td>
<td>Click Upload.</td>
</tr>
</tbody>
</table>

The file takes a few seconds to upload depending on the size of the backup data.
### Procedure 2. Recovery Scenario 2

#### 16. Recovered SOAM GUI: Login

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to <strong>Status &amp; Manage &gt; 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 15. of this procedure.</td>
</tr>
<tr>
<td>4.</td>
<td><strong>Verify</strong> the output window matches the screen below.</td>
</tr>
</tbody>
</table>

![Database Compare](image)

**Database Archive Compare**

The selected database came from Zombie:SOAM1 on 1.

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

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

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

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

- **Topology Compatibility**: The topology should be compatible minus the nodeID.

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

5. If the verification is successful, click **Back**.
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 18. | Recovered SOAM GUI: Restore the database | 1. Select the **Active SOAM** server and click **Restore**.  
2. Select the proper backup provisioning and configuration file.  

![Database Compare](image)

3. Click **OK**. The following confirmation screen displays.  

![Database Restore Confirm](image)

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

*Note:* After the restore has started, the user is logged out of XMI SOAM GUI since the restored Topology is old data. |
| 19. | Recovered SOAM GUI: Monitor and confirm database restoral | Wait for **5-10 minutes** for the system to stabilize with the new topology:  
Monitor the Info tab for **Success**. This indicates the restore is complete and the system is stabilized.  

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

*Note:* The Configuration and Maintenance information is in the same state it was when backed up during initial backup. |
| 20. | NOAM VIP GUI: Recover the remaining SOAM servers | Execute **Configure the SOAM Servers**, steps 1 and 3-6, from reference [1].  

*Note:* Wait for server to reboot before continuing. |
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>NOAM VIP GUI: Start replication on the recovered SOAMs</th>
<th>Un-Inhibit (Start) Replication to the recovered SOAM servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>21.</td>
<td>1. Navigate to Status &amp; Manage &gt; Database.</td>
</tr>
<tr>
<td></td>
<td>- <a href="#">Status &amp; Manage</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="#">Network Elements</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="#">Server</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="#">HA</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="#">Database</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="#">KPIs</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="#">Processes</a></td>
</tr>
<tr>
<td></td>
<td>2. Click Allow Replication on the recovered SOAM servers.</td>
</tr>
<tr>
<td></td>
<td>3. Verify the replication on all SOAMs servers is allowed. This can be done by checking Repl status column of respective server</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td>- <a href="#">Status &amp; Manage</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="#">Network Elements</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="#">Server</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="#">HA</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="#">Database</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="#">KPIs</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="#">Processes</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="#">Tasks</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="#">Files</a></td>
</tr>
<tr>
<td></td>
<td>2. Select the recovered server and click NTP Sync.</td>
</tr>
<tr>
<td></td>
<td>3. Click OK to confirm.</td>
</tr>
</tbody>
</table>

*Are you sure you wish to force an NTP Sync on the following server(s)? SOAM2*
## Procedure 2. Recovery Scenario 2

### 23. NOAM VIP GUI:

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

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

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

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

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

3. For each SOAM server with a Max Allowed HA Role set to **Standby**, set it to **Active**.

   - **ZombieDAMP1**
     - Max Desired HA Role: **Active**
     - The maximum desired HA Role for ZombieDAMP1

   - **ZombieDAMP2**
     - Max Desired HA Role: **Standby**
     - The maximum desired HA Role for ZombieDAMP2

4. Click **OK**.

### 24. NOAM VIP GUI:

**Restart DSR application**

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

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

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

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

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

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

2. Click **Enable Site Provisioning**.

3. A confirmation window displays. Click **OK** to enable Provisioning.


Procedure 2. Recovery Scenario 2

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

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

   If the spare SOAM is also present in the site and lost, execute Appendix A

   If the spare SOAM is also present in the site and lost, execute Appendix A 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 B:

   - If the spare SOAM is also present in the site:
     - Execute Appendix A Inhibit A and B Level Replication on C-level Servers.
     - Navigate to **Status & Manage > Database**.

       - 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)*
         - 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)*

   - Verify the replication on all the working servers is allowed. This can be done by examining the Repl Status table as shown here:

     | OAM Repl Status | SIG Repl Status | Repl Status | Repl Audit Status |
     |-----------------|-----------------|-------------|-------------------|
     | NotApplicable   | NotApplicable   | Allowed     | NotApplicable     |
     | Normal          | NotApplicable   | Allowed     | NotApplicable     |
     | Normal          | NotApplicable   | Allowed     | NotApplicable     |
     | Normal          | NotApplicable   | Allowed     | NotApplicable     |
**Procedure 2. Recovery Scenario 2**

<table>
<thead>
<tr>
<th>27.</th>
<th><strong>Active NOAM:</strong> Perform key exchange between the active-NOAM and recovered servers (DA-MP, SBRs, IPFE, SS7-MP, and vSTP-MP)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Establish an SSH session to the C-level server being recovered and login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Execute following command to set shared memory to unlimited:</td>
</tr>
<tr>
<td></td>
<td>$ sudo shl.set -m 0</td>
</tr>
<tr>
<td></td>
<td>3. Execute Configure the MP Virtual Machines, steps 1, 11-14 (and 15 if required) of reference [1] for each server that has been recovered.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>28.</th>
<th><strong>NOAM VIP GUI:</strong> Start replication on all C-level servers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Un-inhibit (start) replication to the ALL C-level servers.</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Database</strong>.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Network Elements" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Server" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="HA" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Database" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="KPIs" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Processes" /></td>
</tr>
<tr>
<td></td>
<td>2. If the Repl Status is set to <strong>Inhibited</strong>, click <strong>Allow Replication</strong> using this order:</td>
</tr>
<tr>
<td></td>
<td>• Active NOAM Server</td>
</tr>
<tr>
<td></td>
<td>• Standby NOAM Server</td>
</tr>
<tr>
<td></td>
<td>• Active SOAM Server</td>
</tr>
<tr>
<td></td>
<td>• Standby SOAM Server</td>
</tr>
<tr>
<td></td>
<td>• Spare SOAM Server (if applicable)</td>
</tr>
<tr>
<td></td>
<td>• MP/IPFE servers (if MPs are configured as active/standby, start with the Active MP; otherwise, the order of the MPs does not matter)</td>
</tr>
<tr>
<td></td>
<td>3. Verify the replication on all the working servers is allowed. This can be done by examining the Repl Status table as shown here:</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Repl Status Table" /></td>
</tr>
</tbody>
</table>
### Procedure 2. Recovery Scenario 2

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

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

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

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

   ![Modifying HA attributes](image)

   Click **OK.**

**30. 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 keyexchange from the active NOAM to each recovered server:

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

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

**31. Active NOAM:** Activate optional features

**Note for PCA Activation:**

If you have PCA installed in the system being recovered, re-activate PCA by executing PCA Activation on Entire Server on Recovered NOAM Server and PCA Activation on Active SOAM Server from [3].

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

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

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

Refer to section 1.4 Optional Features to activate any features previously activated.
Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>32. NOAM VIP GUI: Fetch and store the database report for the newly restored data and save it</th>
</tr>
</thead>
</table>

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

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

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

   The following screen displays:

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

   ![Database Status Report](image)

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 33. | **Active NOAM**: Verify replication between servers<br>1. Log into the active NOAM using SSH terminal as `admusr`.  
2. Execute this command:  
   ```
   $ sudo irepstat -m
   ```
   **Output:**
   ```
   -- Policy 0 ActStb [DbReplication] ---------------------
   RDU06-MP1 -- Stby  
   BC From RDU06-SO1 Active  0 0.50 ^0.17%cpu 42B/s A=none  
   CC From RDU06-MP2 Active  0 0.10 ^0.17 0.88%cpu 32B/s A=none  
   RDU06-MP2 -- Active  
   BC From RDU06-SO1 Active  0 0.50 ^0.10%cpu 33B/s A=none  
   CC To RDU06-MP1 Active  0 0.10 0.08%cpu 20B/s A=none  
   RDU06-NO1 -- Active  
   AB To RDU06-SO1 Active  0 0.50 1%R 0.03%cpu 21B/s  
   RDU06-SO1 -- Active  
   AB From RDU06-NO1 Active  0 0.50 ^0.04%cpu 24B/s  
   BC To RDU06-MP1 Active  0 0.50 1%R 0.04%cpu 21B/s  
   BC To RDU06-MP2 Active  0 0.50 1%R 0.07%cpu 21B/s
   ``` |
| 34. | **NOAM VIP GUI**: Verify the database states<br>1. Navigate to **Status & Manage > Database**.<br>2. Verify the OAM Max HA Role is either **Active** or **Standby** for NOAM and SOAM; Application Max HA Role for MPs is **Active**; and the status is **Normal**.  

![Status & Manage > Database](image.png)
Procedure 2. Recovery Scenario 2

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

1. **Navigate to Status and Manage > HA.**
   - **Verify the HA status**
     - **Select the row for all of the servers.**
     - **Verify the HA Role is either Active or Standby.**

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

2. **Select the row for all of the servers.**
3. **Verify the HA Role is either Active or Standby.**

36. **SOAM VIP GUI:** Verify the local node info

1. **Navigate to Diameter > Configuration > Local Node.**
   - **Verify all the local nodes are shown.**

37. **SOAM VIP GUI:** Verify the peer node info

1. **Navigate to Diameter > Configuration > Peer Node.**
   - **Verify all the peer nodes are shown.**
**Procedure 2. Recovery Scenario 2**

<table>
<thead>
<tr>
<th>38.</th>
<th>SOAM VIP GUI: Verify the connections info</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Navigate to <strong>Diameter &gt; Configuration &gt; Connections</strong>.</td>
</tr>
<tr>
<td></td>
<td>![Diagram of Diameter menu structure]</td>
</tr>
<tr>
<td></td>
<td>2. Verify all the connections are shown.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>39.</th>
<th>For vSTP Only SOAM VIP Server Console (Optional): Verify vSTP MP local node information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Log into the SOAM VIP server console as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Execute the following command:</td>
</tr>
<tr>
<td></td>
<td><code>[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts</code></td>
</tr>
<tr>
<td></td>
<td>3. Verify the output similar to this output.</td>
</tr>
</tbody>
</table>

```json
{
    "data": {
        "configurationLevel": "10",
        "localHostName": "AUTLocalHost1",
        "localHostPort": 4444,
        "localHostFqdnAddress": "145.168.100.2",
        "localHostSockAddress": "145.168.111.1"
    },
    "configurationLevel": "11",
    "localHostName": "AUTLocalHost2",
    "localHostPort": 4445,
    "localHostFqdnAddress": "145.168.100.2",
    "localHostSockAddress": "145.168.111.1"
}
```


**Procedure 2. Recovery Scenario 2**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 40. | For vSTP Only
SOAM VIP Server Console (Optional):
Verify vSTP MP remote nodes information |
|   | 1. Log into the SOAM VIP server console as **admusr**. |
|   | 2. Execute the following command |
|   | [admusr@SOAM1 ~]$ mmiclient.py /vstp/remotesitipnodes |
|   | 3. Verify the output similar to this output. |

```
{
    "data": [
        {
            "configurationLevel": "12",
            "remoteHostName": "AUTRemoteHost1",
            "remoteHostPort": 4444,
            "remoteHostSslIPAddress": "1.1.1.6",
            "remoteHostSslTCPAddress": "1.1.1.7"
        },
        
        "links": {},
        "messages": [],
        "status": true
    ]
}
```

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 41. | For vSTP Only
SOAM VIP Server Console (Optional):
Verify the vSTP MP connections information |
|   | 1. Log into the SOAM VIP server console as **admusr**. |
|   | 2. Execute the following command |
|   | [admusr@SOAM1 ~]$ mmiclient.py /vstp/connections |
|   | 3. Verify the output similar to this output. |

```
{
    "data": [
        {
            "configurationLevel": "13",
            "connCfSetName": "Default",
            "connectionMode": "Server",
            "connectionType": "M3ua",
            "localHostName": "AUTLocalHost1",
            "name": "AUTLinkTestConn1",
            "remoteHostName": "AUTRemoteHost1"
        },
        
        {
            "configurationLevel": "14",
            "connCfSetName": "Default",
            "connectionMode": "Server",
            "connectionType": "M3pa",
            "localHostName": "AUTLocalHost2",
            "name": "AUTLinkTestConn2",
            "remoteHostName": "AUTRemoteHost1"
        },
        
        "links": {},
        "messages": [],
        "status": true
    ]
}
```

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 42. | **MP Servers:**
Disable SCTP Auth Flag |
|   | For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [1]. |
|   | Execute this procedure on all failed MP servers. |
### Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 43. | **SOAM VIP GUI:** Enable connections, if needed  
   - Navigate to **Diameter > Maintenance > Connections**.  
   - Select each connection and click **Enable**. Alternatively, you can enable all the connections by clicking **EnableAll**.  
   - Verify the Operational State is **Available**. |
| 44. | **SOAM VIP GUI:** Enable optional features  
   - Navigate to **Diameter > Maintenance > Applications**.  
   - Select the optional feature application configured in step 31.  
   - Click **Enable**. |
| 45. | **SOAM VIP GUI:** Re-enable transports, if needed  
   - Navigate to **Transport Manager > Maintenance > Transport**.  
   - Select each transport and click **Enable**.  
   - Verify the Operational Status for each transport is **Up**. |
## Procedure 2. Recovery Scenario 2

<table>
<thead>
<tr>
<th>46.</th>
<th><strong>SOAM VIP GUI:</strong> Re-enable MAPIWF application, if needed. This step is applicable when the MAP-IWF is activated.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>1.</strong> Navigate to <strong>SS7/Sigtran &gt; Maintenance &gt; Local SCCP Users.</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>SS7/Sigtran</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Configuration</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Maintenance</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Local SCCP Users</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Remote Signaling Points</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Remote MTP3 Users</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Linksets</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Links</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>1.</strong> Click the Enable button corresponding to MAPIWF Application Name.</td>
</tr>
<tr>
<td></td>
<td>- <strong>2.</strong> Verify the SSN Status is Enabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>47.</th>
<th><strong>SOAM VIP GUI:</strong> Re-enable links, if needed. This step is applicable when the MAP-IWF is activated.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>1.</strong> Navigate to <strong>SS7/Sigtran &gt; Maintenance &gt; Links.</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>SS7/Sigtran</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Configuration</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Maintenance</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Local SCCP Users</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Remote Signaling Points</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Remote MTP3 Users</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Linksets</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Links</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>1.</strong> Click Enable for each link.</td>
</tr>
<tr>
<td></td>
<td>- <strong>2.</strong> Verify the Operational Status for each link is Up.</td>
</tr>
</tbody>
</table>
### Procedure 2. Recovery Scenario 2

#### 48. NOAM VIP GUI: Perform Key exchange with export server

1. Navigate to Administration > Remote Servers > Data Export.
   - Administration
     - General Options
     - Access Control
     - Software Management
     - Remote Servers
       - LDAP Authentication
       - SNMP Trapping
       - Data Export
       - DNS Configuration

2. Click the Task Name and click Key Exchange.

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Remote Server</th>
<th>Username</th>
<th>Directory on Export Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>APDE Remote Server Copy</td>
<td>10.10.10.10</td>
<td>admusr</td>
<td>exp</td>
</tr>
</tbody>
</table>

3. Type the Password and click OK.

Repeat for each task.

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

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

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

#### 50. Backup and archive all the databases from the recovered system

 Execute Appendix E DSR Database Backup to back up the Configuration databases.
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 for 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. All other servers are recovered using recovery procedures for software. Database replication from the active NOAM/active SOAM server will recover the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure. The actual procedures’ detailed steps are in Procedure 3. The major activities are summarized as follows:

- Recover Active NOAM server by recovering software and the database
  - Recover the software
  - Recover the database
- Recover NOAM servers by recovering software
  - Recover the software
- Recover any failed SOAM and MP servers by recovering software
  - Recover the software
  - Database is already intact at one SOAM server and does not require restoration at the other SOAM and MP servers

Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Workaround</td>
<td>Refer to Appendix F to Check and Create Backup Directory.</td>
</tr>
<tr>
<td>2.</td>
<td>Gather required materials</td>
<td>Gather the documents and required materials listed in section 3.1 Required Materials.</td>
</tr>
</tbody>
</table>
| 3.     | Recover the failed software | For VMWare based deployments:  
1. For NOAMs, execute the following procedures from reference [1]:  
   a. Procedure 1 (VMWare) Import DSR OVA  
      If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.  
   b. Procedure 2 (VMWare Only) Configure NOAM Guests Based On Resource Profile  
2. For SOAMs, execute the following procedures from reference [1]:  
   a. Procedure 1 (VMWare) Import DSR OVA  
      If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.  
   b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based |
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>4.</th>
<th>Obtain latest database backup and network configuration data</th>
</tr>
</thead>
</table>

1. Obtain the most recent database backup file from external backup sources (for example, file servers) or tape backup sources.

2. From required materials list in section 3.1 Required Materials; use site survey documents and Network Element report (if available) to determine network configuration data.

<table>
<thead>
<tr>
<th>3.</th>
<th>For failed MPs, execute the following procedures from reference [1]:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Procedure 1 (VMWare) Import DSR OVA</td>
</tr>
<tr>
<td>b.</td>
<td>Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile</td>
</tr>
</tbody>
</table>

**For KVM/OpenStack based deployments:**

1. For NOAMs, execute the following procedures from reference [1]:
   a. Procedure 4 (KVM/OpenStack) Import DSR OVA
   b. Procedure 5 (KVM/OpenStack Only) Configure NOAM Guests Based On Resource Profile

2. For SOAMs, execute the following procedures from reference [1]:
   a. Procedure 4 (KVM/OpenStack) Import DSR OVA
   b. Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile

3. For failed MPs, execute the following procedures from reference [1]:
   a. Procedure 4 (KVM/OpenStack) Import DSR OVA
   b. Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile

**For OVM-S/OVM-M based deployments:**

1. Execute the following procedures from reference [1]:
   a. Procedure 7 (OVM-S/OVM-M) Import DSR OVA and Prepare for VM creation
   b. Procedure 8 (OVM-S/OVM-M) Configure each DSR VM

While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs).

Obtain latest database backup and network configuration data.
### Procedure 3. Recovery Scenario 3

|   | Execute DSR installation procedure for the first NOAM | Verify the network data for network elements.  
|---|-----------------------------------------------------|-------------------------------------------------------------------|
| 5. |                                                     | **Note:** Use the backup copy of network configuration data and site surveys (Step 2).  
|    |                                                     | - Execute Configure the First NOAM NE and Server from reference [1].  
|    |                                                     | - Execute Configure the NOAM Server Group from reference [1]. |

|   | NOAM GUI: Login | 1. Establish a GUI session on the recovered NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of:  
|---|-----------------|-------------------------------------------------------------------|
| 6. |                 | **http://<Recovered_NOAM_IP_Address>**  
|    |                 | 2. Log into the NOAM GUI as the **guiadmin** user:  

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

7. NOAM GUI: Upload the backed up database file

1. Navigate to Status & Manage > Files.

2. Select the active NOAM server.

   ![NOAM GUI](image)

   **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.

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

6. Click **Upload**.

7. 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1. | **NOAM GUI:** Navigate to **Status & Manage > Database**.  
    - Click **Disable Provisioning**.  
    - A confirmation window displays. Click **OK** to disable provisioning.  
    - Are you sure?  
    - OK | **Cancel** |
| 2. | **NOAM GUI:** Disable provisioning |
| 3. | **NOAM GUI:** Disable provisioning |
**Procedure 3. Recovery Scenario 3**

1. **Select the Active NOAM server and click Compare.**
   
   ![Comparison button]

2. **Click the button for the restored database file uploaded as a part of step 7 of this procedure.**
   
   ![Database Compare]

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**

   ![Archive and Database Compatibility]

   **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.**
### Procedure 3. Recovery Scenario 3

| Procedure 3. Recovery Scenario 3 | 1. From **Status & Manage > Database**.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Select the <strong>Active NOAM</strong> server and click <strong>Restore</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Select the proper backup provisioning and configuration file.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td><strong>Active NOAM:</strong> Restore the database</td>
<td><img src="image1.png" alt="Image" /></td>
</tr>
<tr>
<td><strong>Database Restore Confirm</strong></td>
<td><img src="image2.png" alt="Image" /></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> After the restore has started, the user is logged out of XMI NO GUI since the restored topology is old data.</td>
</tr>
</tbody>
</table>
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.</td>
<td><strong>NOAM VIP GUI: Login</strong>&lt;br&gt;1. Establish a GUI session on the NOAM server by using the VIP address of the NOAM server. Open the web browser and enter a URL of: <a href="http://%3CPrimary_NOAM_VIP_IP_Address%3E">http://&lt;Primary_NOAM_VIP_IP_Address&gt;</a>&lt;br&gt;2. Login as the <code>guiadmin</code> user:</td>
</tr>
<tr>
<td>12.</td>
<td><strong>NOAM VIP GUI: Monitor and confirm database restoral</strong>&lt;br&gt;1. Wait for <strong>5-10 minutes</strong> for the system to stabilize with the new topology:&lt;br&gt;2. Monitor the Info tab for <strong>Success</strong>. This indicates the restore is complete and the system is stabilized.&lt;br&gt;Ignore these alarms for NOAM and MP servers until all the servers are configured:&lt;br&gt;• Alarms with Type Column as REPL, COLL, HA (with mate NOAM), DB (about Provisioning Manually Disabled).&lt;br&gt;<strong>Note:</strong> Do not pay attention to alarms until all the servers in the system are completely restored.&lt;br&gt;<strong>Note:</strong> The Configuration and Maintenance information is in the same state it was when backed up during initial backup.</td>
</tr>
<tr>
<td>13.</td>
<td><strong>Active NOAM: Login</strong>&lt;br&gt;Log into the recovered active NOAM using SSH terminal as <code>admusr</code> user.</td>
</tr>
</tbody>
</table>
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 14. | **NOAM GUI:** Enable provisioning  
1. Navigate to **Status & Manage > Database**.  
   - Enable Provisioning
   - Click **Enable Provisioning**.  
   - A confirmation window displays. Click **OK** to enable provisioning.  
2. Navigate to **Status & Manage > Database**.  
   - Enable Provisioning
   - Click **Enable Provisioning**.  
   - A confirmation window displays. Click **OK** to enable provisioning.  
3. Navigate to **Status & Manage > Database**.  
   - Enable Provisioning
   - Click **Enable Provisioning**.  
   - A confirmation window displays. Click **OK** to enable provisioning.  
4. Navigate to **Status & Manage > Database**.  
   - Enable Provisioning
   - Click **Enable Provisioning**.  
   - A confirmation window displays. Click **OK** to enable provisioning.  
5. Navigate to **Status & Manage > Database**.  
   - Enable Provisioning
   - Click **Enable Provisioning**.  
   - A confirmation window displays. Click **OK** to enable provisioning.  
6. Navigate to **Status & Manage > Database**.  
   - Enable Provisioning
   - Click **Enable Provisioning**.  
   - A confirmation window displays. Click **OK** to enable provisioning.  
7. Navigate to **Status & Manage > Database**.  
   - Enable Provisioning
   - Click **Enable Provisioning**.  
   - A confirmation window displays. Click **OK** to enable provisioning.  
8. Navigate to **Status & Manage > Database**.  
   - Enable Provisioning
   - Click **Enable Provisioning**.  
   - A confirmation window displays. Click **OK** to enable provisioning.  
9. Navigate to **Status & Manage > Database**.  
   - Enable Provisioning
   - Click **Enable Provisioning**.  
   - A confirmation window displays. Click **OK** to enable provisioning.  
10. Navigate to **Status & Manage > Database**.  
    - Enable Provisioning
    - Click **Enable Provisioning**.  
    - A confirmation window displays. Click **OK** to enable provisioning.  
11. Navigate to **Status & Manage > Database**.  
    - Enable Provisioning
    - Click **Enable Provisioning**.  
    - A confirmation window displays. Click **OK** to enable provisioning.  
12. Navigate to **Status & Manage > Database**.  
    - Enable Provisioning
    - Click **Enable Provisioning**.  
    - A confirmation window displays. Click **OK** to enable provisioning.  
13. Navigate to **Status & Manage > Database**.  
    - Enable Provisioning
    - Click **Enable Provisioning**.  
    - A confirmation window displays. Click **OK** to enable provisioning.  
14. Navigate to **Status & Manage > Database**.  
    - Enable Provisioning
    - Click **Enable Provisioning**.  
    - A confirmation window displays. Click **OK** to enable provisioning.  
15. **NOAM VIP GUI:** Recover standby NOAM  
   Install the second NOAM server by executing these procedures from reference [1]:  
   - Execute Configure the Second NOAM Server, steps 3-5 and 7  
   **Note:** If topology or nodeID alarms are persistent after the database restore, refer to Appendix F to Check and Create Backup Directory.  
16. **NOAM VIP GUI:** Restart DSR application  
   1. Navigate to **Status & Manage > Server**.  
   2. Select the recovered standby NOAM server and click **Restart**.  
   3. Click **OK** on confirmation screen.  
17. Recover remaining failed SOAM server(s), if needed  
   1. Install the SOAM servers by executing Configure the SOAM Servers, steps 1 and 3-7 from reference [1].  
   **Note:** Wait for the server to reboot.  
   2. Repeat for each remaining SOAM server (standby, spare).
### Procedure 3. Recovery Scenario 3

#### 18. 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**.

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

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

   - [Status & Manage](#) > [Network Elements](#) > [Server](#) > [HA](#) > [Database](#) > [KPIs](#) > [Processes](#) > [Tasks](#) > [Files](#)

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

3. For each server with a Max Allowed HA Role set to not active, set it to **Active**.

   - **Modifying HA attributes**

     | Hostname     | Max Allowed HA Role | Description |
     |--------------|--------------------|-------------|
     | ZombieNOAM1  | Active             | The maximum |
     | ZombieNOAM2  | Active             | The maximum |
     | ZombieDSRNOAM | Standby            | The maximum |

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>20.</strong></td>
<td>NOAM VIP GUI: Restart DSR application</td>
</tr>
</tbody>
</table>
| 1. | Navigate to **Status & Manage > Server**.  
   ![Status & Manage](image)  
   - Network Elements  
   - Server  
   - HA  
   - Database  
   - KPIs  
   - Processes  
   - Tasks  
   - Files  
   2. Select each recovered server and click **Restart**. |
| **21.** | 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**.  
   ```bash  
   $ keyexchange admusr@<Recovered Server Hostname>  
   ```  
   **Note**: If an export server is configured, perform this step. |
| **22.** | Active NOAM: Activate optional features |
| **Note for PCA Activation:** | If you have PCA installed in the system being recovered, re-activate PCA by executing **PCA Activation on Entire Server** on Recovered NOAM Server and **PCA Activation on Active SOAM Server** from [3]. |
| **Note:** | While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:  
   ```plaintext  
   iload#31000{S/W Fault}  
   ```  
   **Note**: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.  
   Refer to section 1.4 Optional Features to activate any features previously activated. |
Procedure 3. Recovery Scenario 3

23. 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]
- 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]**

```
<table>
<thead>
<tr>
<th>dsr Database Status Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>FROM: Active Network OAH6P on host ZombieNOAM1</td>
</tr>
<tr>
<td>Report Version: 8.6.0.6.0-80.0.0</td>
</tr>
<tr>
<td>User: guiadmin</td>
</tr>
</tbody>
</table>

---

**General**

<table>
<thead>
<tr>
<th>Hostname</th>
<th>ZombieNOAM1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Birthday</td>
<td>2016-07-11 11:21:59 EDT</td>
</tr>
<tr>
<td>Application Database Version</td>
<td>6.0</td>
</tr>
</tbody>
</table>

**Capacities and Utilization**

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

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

24. **Active NOAM**: Verify replication between servers

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

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

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

1. Navigate to **Status & Manage > Database**.
2. Verify the OAM Max HA Role is either **Active** or **Standby** for NOAM and SOAM; Application Max HA Role for MPs is **Active**; and the status is **Normal**.
Procedure 3. Recovery Scenario 3

26. **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>ZomeleNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZomeleNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZomeleERNOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZomeleERNOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZomeleSOAM1</td>
<td>Active</td>
<td>N/A</td>
<td>Active</td>
</tr>
<tr>
<td>ZomeleSOAM2</td>
<td>Standby</td>
<td>N/A</td>
<td>Standby</td>
</tr>
</tbody>
</table>

27. **SOAM VIP GUI:**

    Verify the local node info

    1. Navigate to **Diameter > Configuration > Local Node.**
       
    2. Verify all the local nodes are shown.

28. **SOAM VIP GUI:**

    Verify the peer node info

    1. Navigate to **Diameter > Configuration > Peer Node.**
       
    2. Verify all the peer nodes are shown.
## Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29.</td>
<td><strong>SOAM VIP GUI:</strong> Verify the connections info</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Diameter &gt; Configuration &gt; Connections.</strong></td>
</tr>
<tr>
<td></td>
<td>- Verify all the connections are shown.</td>
</tr>
<tr>
<td></td>
<td>2. <strong>For vSTP Only</strong> <strong>SOAM VIP Server Console (Optional):</strong> Verify vSTP MP local node information</td>
</tr>
<tr>
<td></td>
<td>- Log into the SOAM VIP server console as <strong>admusr.</strong></td>
</tr>
<tr>
<td></td>
<td>- Execute the following command:</td>
</tr>
<tr>
<td></td>
<td>```bash</td>
</tr>
<tr>
<td></td>
<td>[admusr@SOAM1 ~]$ mniclient.py /vstp/localhosts</td>
</tr>
<tr>
<td></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td>- Verify the output similar to this output.</td>
</tr>
</tbody>
</table>
Procedure 3. Recovery Scenario 3

31. For vSTP Only
SOAM VIP Server Console (Optional):
Verify vSTP MP remote nodes information

1. Log into the SOAM VIP server console as admusr.
2. Execute the following command

   [admusr@SOAM1 ~]$ mmiclient.py /vstp/remotes

3. Verify the output similar to this output.

   ```json
   { "data": [
   { "configurationLevel": "12",
   "remoteHostName": "AUTRemoteHost1",
   "remoteHostPort": 4444,
   "remoteHostFqetAddress": "1.1.1.6",
   "remoteHostSecIPAddress": "1.1.1.7"
   },
   "links": {},
   "messages": [],
   "status": true
   }
   
   { "data": [
   { "configurationLevel": "13",
   "connCfgSetId": "Default",
   "connectionMode": "Server",
   "connectionType": "MSua",
   "localHostName": "AUTLocalHost2",
   "name": "AUTLinkTestConn3",
   "remoteHostName": "AUTRemoteHost1"
   },
   { "configurationLevel": "14",
   "connCfgSetId": "Default",
   "connectionMode": "Server",
   "connectionType": "MSpa",
   "localHostName": "AUTLocalHost2",
   "name": "AUTLinkTestConn2",
   "remoteHostName": "AUTRemoteHost1"
   }
   
   "links": {},
   "messages": [],
   "status": true
   }
   ```

32. For vSTP Only
SOAM VIP Server Console (Optional):
Verify the vSTP MP connections information

1. Log into the SOAM VIP server console as admusr.
2. Execute the following command

   [admusr@SOAM1 ~]$ mmiclient.py /vstp/connections

3. Verify the output similar to this output.

   ```json
   
   ```
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Procedure 3. Recovery Scenario 3</th>
<th>33. SOAM VIP GUI: Enable connections, if needed</th>
<th>34. SOAM VIP GUI: Enable optional features</th>
<th>35. SOAM VIP GUI: Re-enable transports, if needed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Navigate to <strong>Diameter &gt; Maintenance &gt; Connections</strong>.</td>
<td>1. Navigate to <strong>Diameter &gt; Maintenance &gt; Applications</strong>.</td>
<td>1. Navigate to <strong>Transport Manager &gt; Maintenance &gt; Transport</strong>.</td>
</tr>
<tr>
<td></td>
<td>1. Select each connection and click <strong>Enable</strong>. Alternatively, you can enable all the connections by clicking <strong>EnableAll</strong>.</td>
<td>2. Select the optional feature application configured in step 37.</td>
<td>2. Select each transport and click <strong>Enable</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Verify the Operational State is <strong>Available</strong>.</td>
<td>3. Click <strong>Enable</strong>.</td>
<td>3. Verify the Operational Status for each transport is <strong>Up</strong>.</td>
</tr>
</tbody>
</table>
**Procedure 3. Recovery Scenario 3**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **36. SOAM VIP GUI:** Re-enable MAPIWF application, if needed. This step is applicable when the MAP-IWF is activated. | 1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users.**
   - **SS7/Sigtran**
     - **Configuration**
     - **Maintenance**
       - **Local SCCP Users**
       - **Remote Signaling Points**
       - **Remote MTP3 Users**
       - **Linksets**
       - **Links**
   2. Click the **Enable** button corresponding to MAPIWF Application Name.
   3. Verify the SSN Status is **Enabled**. |
| **37. SOAM VIP GUI:** Re-enable links, if needed. This step is applicable when the MAP-IWF is activated. | 1. Navigate to **SS7/Sigtran > Maintenance > Links.**
   - **SS7/Sigtran**
     - **Configuration**
     - **Maintenance**
       - **Local SCCP Users**
       - **Remote Signaling Points**
       - **Remote MTP3 Users**
       - **Linksets**
       - **Links**
   2. Click **Enable** for each link.
   3. Verify the Operational Status for each link is **Up**. |
### Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 38. | **NOAM VIP GUI:** Perform key exchange with export server | 1. Navigate to Administration > Remote Servers > Data Export.  
   - Administration  
     - General Options  
     - Access Control  
     - Software Management  
     - Remote Servers  
       - LDAP Authentication  
       - SNMP Trapping  
       - Data Export  
       - DNS Configuration  
   2. Click **SSH Key Exchange** at the bottom of the screen.  
   3. Type the **Password** and click **OK**. |
| 39. | **SOAM VIP GUI:** Examine all alarms | 1. Navigate to Alarms & Events > View Active.  
   - Alarms & Events  
     - View Active  
     - View History  
     - View Trap Log  
   2. Examine all active alarms and refer to the on-line help on how to address them.  
   If needed, contact My Oracle Support (MOS). |
| 40. | **SOAM VIP GUI:** Re-enable transports, if needed | Navigate to Transport Manager > Maintenance > Transport.  
   - Transport Manager  
   - Configuration  
   - Maintenance  
   - Transport  
   Select each transport and click **Enable**.  
   Verify the Operational Status for each transport is **Up**. |
| 41. | **Restore GUI usernames and passwords** | If applicable, execute steps in section 5 to recover the user and group information restored. |
Procedure 3. Recovery Scenario 3

<table>
<thead>
<tr>
<th>Procedure 3. Recovery Scenario 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>42.</strong></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 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 software
  - Recover the software
  - The database is intact at the active NOAM server and does not require restoration at the standby NOAM server
    - Recover any failed SO and MP servers by recovering software
    - Recover the software
  - The database is intact at the active NOAM server and does not require restoration at the SO and MP servers
    - Re-apply signaling networks configuration if the failed blade is an MP

Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th><strong>STEP #</strong></th>
<th><strong>Workaround</strong></th>
<th><strong>Gather required materials</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong></td>
<td>Refer to Appendix F to Check and Create Backup Directory.</td>
<td>Gather the documents and required materials listed in section 3.1 Required Materials.</td>
</tr>
<tr>
<td><strong>2.</strong></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><strong>3.</strong></td>
<td>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td>
<td></td>
</tr>
</tbody>
</table>
# Procedure 4. Recovery Scenario 4

<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 address of the NOAM server. Open the web browser and enter a URL of:

   ![URL](http://<Primary_NOAM_VIP_IP_Address>)

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

   ![Login Page]

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

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

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

Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.
### Procedure 4. Recovery Scenario 4

**Active NOAM:** Set failed servers to OOS

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

2. **Modifying HA attributes**

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

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

**Recover the failed software**

**For VMWare based deployments:**

1. For NOAMs, execute the following procedures from reference [1]:
   a. Procedure 1 (VMWare) Import DSR OVA
      - If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.
   b. Procedure 2 (VMWare Only) Configure NOAM Guests Based On Resource Profile
2. For SOAMs, execute the following procedures from reference [1]:
   a. Procedure 1 (VMWare) Import DSR OVA
      - If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.
   b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile
3. For failed MPs, execute the following procedures from reference [1]:
   a. Procedure 1 (VMWare) Import DSR OVA
      - If OVA is already imported and present in the Infrastructure Manager,
## Procedure 4. Recovery Scenario 4

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
|   | skip this procedure to import OVA.  
|   | b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile  
| For KVM/OpenStack based deployments: |   |
| 1. For NOAMs, execute the following procedures from reference [1]: |   |
|   | a. Procedure 4 (KVM/OpenStack) Import DSR OVA  
|   | If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.  
|   | b. Procedure 5 (KVM/OpenStack Only) Configure NOAM Guests Based On Resource Profile  
| 2. For SOAMs, execute the following procedures from reference [1]: |   |
|   | a. Procedure 4 (KVM/OpenStack) Import DSR OVA  
|   | If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.  
|   | b. Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile  
| 3. For failed MPs, execute the following procedures from reference [1]: |   |
|   | a. Procedure 4 (KVM/OpenStack) Import DSR OVA  
|   | If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.  
|   | b. Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile  
| For OVM-S/OVM-M based deployments: |   |
| 1. Execute the following procedures from reference [1]: |   |
|   | a. Procedure 7 (OVM-S/OVM-M) Import DSR OVA and Prepare for VM creation  
|   | b. Procedure 8 (OVM-S/OVM-M) Configure each DSR VM  
| | While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs).  
| 6. Repeat | If necessary, repeat step 5. for all remaining servers. |
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
</table>
| 7.   | **NOAM VIP GUI:** Login  
1. Establish a GUI session on the NOAM server by using the VIP 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: |
| 8.   | **NOAM VIP GUI:** Revert standby NOAM  
Install the second NOAM server by executing these procedures from reference [1]:  
- Execute Configure the Second NOAM Server, steps 3-5 and 7  
- Execute Configure the NOAM Server Group, step 4  
  *Note:* If topology or nodeID alarms are persistent after the database restore, refer to Appendix F to Check and Create Backup Directory. |
| 9.   | Recover remaining failed SOAM server(s), if needed  
1. Install the SOAM servers by executing Configure the SOAM Servers, steps 1 and 3-7 from reference [1].  
  *Note:* Wait for the server to reboot.  
2. Repeat for each remaining SOAM server (standby, spare). |
| 10.  | **Recovered Server:** Login  
Log into the recovered server using SSH terminal as `admusr` user. |
## Procedure 4. Recovery Scenario 4

### Recovered Server: Synchronize NTP

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

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

2. **Select the recovered server and click NTP Sync.**

   ![Start NTP Sync button]

3. **Click OK to confirm.**

   Are you sure you wish to force an NTP Sync on the following server(s)?
   
   SOAM2
## Procedure 4. Recovery Scenario 4

### 12. NOAM VIP GUI:

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

1. Navigate to Status & Manage > HA.

   ![Status & Manage menu]

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

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

3. For each SOAM server with a Max Allowed HA Role set to **Standby**, set it to **Active**.

   ![SOAM server roles]

4. Click **OK**.

### 13. NOAM VIP GUI:

**Restart DSR application**

1. Navigate to Status & Manage > Server.

   ![Status & Manage menu]

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

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

### 14. Active NOAM:

**Perform key exchange between the active-NOAM and recovered servers (DA-MP, SBRs, IPFE, SS7-MP, and vSTP-MP)**

1. Establish an SSH session to the C-level server being recovered and login as admusr.

2. Execute following command to set shared memory to unlimited:

   ```bash
   $ sudo shl.set -m 0
   ```

3. Execute Configure the MP Virtual Machines, steps 1, 11-14 (and 15 if required) of reference [1] for each server that has been recovered.
### Procedure 4. Recovery Scenario 4

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

- **Restart DSR application**

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

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

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

#### 16. NOAM VIP GUI: Restart DSR application on recovered C-level servers

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

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

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

     - For each SOAM server with a Max Allowed HA Role set to **Standby**, set it to **Active**.

     - Click **OK**.

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

- **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 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.</td>
<td><strong>Active NOAM:</strong>&lt;br&gt;Activate optional features</td>
<td><strong>Note for PCA Activation:</strong>&lt;br&gt;If you have PCA installed in the system being recovered, re-activate PCA by executing PCA Activation on Entire Server on Recovered NOAM Server and PCA Activation on Active SOAM Server from [3].&lt;br&gt;&lt;br&gt;<strong>Note:</strong> While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:&lt;br&gt;<code>iload#31000{S/W Fault}</code>&lt;br&gt;&lt;br&gt;<strong>Note:</strong> If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.&lt;br&gt;Refer to section 1.4 Optional Features to activate any features previously activated.</td>
</tr>
</tbody>
</table>
| 19. | **NOAM VIP GUI:**<br>Fetch and store the database report for the newly restored data and save it | 1. Navigate to **Status & Manage > Database.**<br>   - **Status & Manage**<br>     - Network Elements<br>     - Server<br>     - HA<br>     - Database<br>     - KPIs<br>     - Processes<br>   - **Report**<br>2. Select the active NOAM server and click **Report.**<br>   - The following screen displays:<br>   - **Main Menu: Status & Manage -> Database [Report]**<br>   - ![Database Status Report](image)
   - **General**
     - `Host name`: ZombieNOAM1<br>     - `Database Birthday`: 2016-07-11 11:21:50 EDT<br>     - `Application Database Version`: 6.0<br>   - **Capacities and Utilization**
     - `Disk Utilization`: 8.4%: 5GB used of 7.00 total, 6.00 available<br>     - `Memory Utilization`: 0.0%: used of total, 0K available<br>3. Click **Save** and save the report to your local machine. |
Procedure 4. Recovery Scenario 4

20. **Active NOAM:** Verify replication between servers

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

   ```
   $ sudo irepstat -m
   ```

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

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

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

2. Verify the OAM Max HA Role is either **Active** or **Standby** for NOAM and SOAM; Application Max HA Role for MPs is **Active**; and the status is **Normal**.
**Procedure 4. Recovery Scenario 4**

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

1. Navigate to Status and Manage > HA.

   ![Diagram of Status and Manage]

   - Select the row for all of the servers.
   - Verify the HA Role is either **Active** or **Standby**.

   ![Table of Hostname, OAM HA Role, Application HA Role, Max Allow HA Role]

2. Select the row for all of the servers.

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

23. **SOAM VIP GUI:** Verify the local node info

1. Navigate to Diameter > Configuration > Local Node.

   ![Diagram of Configuration]

   - Verify all the local nodes are shown.

24. **SOAM VIP GUI:** Verify the peer node info

1. Navigate to Diameter > Configuration > Peer Node.

   ![Diagram of Configuration]

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

<table>
<thead>
<tr>
<th>25.</th>
<th><strong>SOAM VIP GUI:</strong> Verify the connections info</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Verify all the connections are shown.</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Diameter &gt; Configuration &gt; Connections.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Diameter Configuration tree" /></td>
</tr>
<tr>
<td></td>
<td>2. Log into the SOAM VIP server console as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Execute the following command:</td>
</tr>
<tr>
<td></td>
<td>[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts</td>
</tr>
<tr>
<td></td>
<td>4. Verify the output similar to this output.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>26.</th>
<th><strong>For vSTP Only SOAM VIP Server Console (Optional): Verify vSTP MP local node information</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Execute the following command:</td>
</tr>
<tr>
<td></td>
<td>[admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts</td>
</tr>
<tr>
<td></td>
<td>2. Verify the output similar to this output.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="JSON output" /></td>
</tr>
</tbody>
</table>
### Procedure 4. Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>27.</td>
<td>For vSTP Only&lt;br&gt;SOAM VIP Server Console (Optional): Verify vSTP MP remote nodes information</td>
<td>1. Log into the SOAM VIP server console as <code>admusr</code>.&lt;br&gt;2. Execute the following command&lt;br&gt;<code>[admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts</code>&lt;br&gt;3. Verify the output similar to this output.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="vSTP remote nodes output" /></td>
</tr>
<tr>
<td>28.</td>
<td>For vSTP Only&lt;br&gt;SOAM VIP Server Console (Optional): Verify the vSTP MP connections information</td>
<td>1. Log into the SOAM VIP server console as <code>admusr</code>.&lt;br&gt;2. Execute the following command&lt;br&gt;<code>[admusr@SOAM1 ~]$ mmiclient.py /vstp/connections</code>&lt;br&gt;3. Verify the output similar to this output.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="vSTP MP connections output" /></td>
</tr>
<tr>
<td>29.</td>
<td><strong>MP Servers:</strong>&lt;br&gt;Disable SCTP Auth Flag</td>
<td>For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [1].&lt;br&gt;Execute this procedure on all failed MP servers.</td>
</tr>
</tbody>
</table>
### Procedure 4. Recovery Scenario 4

**30. SOAM VIP GUI:** Enable connections, if needed

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

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

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

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

**31. SOAM VIP GUI:** Enable optional features

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

2. Select the optional feature application configured in step 37.
3. Click **Enable**.

**32. SOAM VIP GUI:** Re-enable transports, if needed

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

2. Select each transport and click **Enable**.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>33.</td>
<td><strong>SOAM VIP GUI:</strong> Re-enable MAPIWF application, if needed. This step is applicable when the MAP-IWF is activated.</td>
</tr>
</tbody>
</table>
| | 1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users.**  
| | 1.1. Navigate to **Management > Configuration > Maintenance > Local SCCP Users.**  
| | 2. Click the **Enable** button corresponding to MAPIWF Application Name.  
| | 2.1. Enable button is displayed.  
| | 3. Verify the SSN Status is **Enabled.** |
| 34. | **SOAM VIP GUI:** Re-enable links, if needed. This step is applicable when the MAP-IWF is activated. |
| | 1. Navigate to **SS7/Sigtran > Maintenance > Links.**  
| | 1.1. Navigate to **Management > Configuration > Maintenance > Links.**  
| | 2. Click **Enable** for each link.  
| | 2.1. Enable button is displayed.  
| | 3. Verify the Operational Status for each link is **Up.** |
| 35. | **SOAM VIP GUI:** Examine all alarms  
| | 1. Navigate to **Alarms & Events > View Active.**  
| | 1.1. Navigate to **Management > Alarms & Events > View Active.**  
| | 2. Examine all active alarms and refer to the on-line help on how to address them.  
| | 2.1. If needed, contact My Oracle Support (MOS). |
Procedure 4. Recovery Scenario 4

36. NOAM VIP GUI: Examine all alarms

1. Log into the NOAM VIP if not already logged in.
2. Navigate to Alarms & Events > View Active.

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

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

37. Restart oampAgent, if needed

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

   1. Establish an SSH session to each server that has the alarm and login as admusr.
   2. Execute these commands:

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

38. Backup and archive all the databases from the recovered system

   Execute Appendix E DSR Database Backup to back up the Configuration databases.

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 software
  - 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 software
  - Recover the software
  - The database in intact at the active NOAM server and does not require restoration at the SOAM and MP servers
### Procedure 5. Recovery Scenario 5

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.

<table>
<thead>
<tr>
<th>Step #</th>
<th>Workaround</th>
<th>Gather required materials</th>
<th>Switch DR NOAM to primary</th>
<th>Recover the failed software</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td>Refer to Appendix F to Check and Create Backup Directory.</td>
<td>Gather the documents and required materials listed in section 3.1 Required Materials.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td></td>
<td></td>
<td>For VMWare based deployments:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1. For NOAMs, execute the following procedures from reference [1]:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>a. Procedure 1 (VMWare) Import DSR OVA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>b. Procedure 2 (VMWare Only) Configure NOAM Guests Based On Resource Profile</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2. For SOAMs, execute the following procedures from reference [1]:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>a. Procedure 1 (VMWare) Import DSR OVA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3. For failed MPs, execute the following procedures from reference [1]:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>a. Procedure 1 (VMWare) Import DSR OVA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>b. Procedure 3 (VMWare Only) Configure Remaining DSR Guests Based On Resource Profile</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>For KVM/OpenStack based deployments:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1. For NOAMs, execute the following procedures from reference [1]:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>a. Procedure 4 (KVM/OpenStack) Import DSR OVA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>b. Procedure 5 (KVM/OpenStack Only) Configure NOAM Guests Based On Resource Profile</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2. For SOAMs, execute the following procedures from reference [1]:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>a. Procedure 4 (KVM/OpenStack) Import DSR OVA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.</td>
</tr>
</tbody>
</table>
## Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>b.</td>
<td>Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile</td>
</tr>
<tr>
<td>3.</td>
<td>For failed MPs, execute the following procedures from reference [1]:</td>
</tr>
<tr>
<td>a.</td>
<td>Procedure 4 (KVM/OpenStack) Import DSR OVA</td>
</tr>
<tr>
<td></td>
<td>If OVA is already imported and present in the Infrastructure Manager, skip this procedure to import OVA.</td>
</tr>
<tr>
<td>b.</td>
<td>Procedure 6 (KVM/OpenStack Only) Configure Remaining DSR Guests Based On Resource Profile</td>
</tr>
</tbody>
</table>

**For OVM-S/OVM-M based deployments:**

1. Execute the following procedures from reference [1]:
   a. Procedure 7 (OVM-S/OVM-M) Import DSR OVA and Prepare for VM creation
   b. Procedure 8 (OVM-S/OVM-M) Configure each DSR VM
      While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs).

### 5. Recover failed SOAMs

- If all SOAM servers failed, execute Procedure 2.

### 6. DR-NOAM VIP GUI: Login

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

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

2. Login as the `guiadmin` user:

   ![Oracle System Login](image)

   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 5. Recovery Scenario 5

7. **DR-NOAM VIP GUI** Set failed NOAM servers to standby

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

2. Click **Edit**.

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

4. Click **OK**.

    ![Ok Cancel]

8. **DR-NOAM VIP GUI** Export the initial configuration

1. Navigate to **Configuration > Servers**.

2. From the GUI screen, select the failed NOAM server and click **Export** to generate the initial configuration data for that server.

    ![Insert Edit Delete Export Report]

9. **DR-NOAM VIP GUI** Copy configuration file to failed NOAM server

1. Obtain a terminal session to the DR-NOAM VIP, login as the **admusr** user.

2. Configure the failed NOAM server:

    ```bash
    $ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<Failed_NOAM_Hostname>.sh admusr@<Failed_NOAM_xmi_IP_address>:/var/tmp/TKLCConfigData.sh
    ```
### Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
<th>Steps</th>
</tr>
</thead>
</table>
| 10. | **Recovered NOAM Server:** Verify configuration was called and reboot the server | 1. Establish an SSH session to the recovered NOAM server (Recovered_NOAM_xmi_IP_address).  
2. Login as the `admusr` user.  
3. The automatic configuration daemon looks for the file named `TKLCCfgData.sh` in the `/var/tmp` directory, implements the configuration in the file, and asks the user to reboot the server.  
4. Verify `awpushcfg` was called by checking the following file.  
   
   ```bash
   $ sudo cat /var/TKLC/appw/logs/Process/install.log
   ```  
   Verify this message displays:  
   ```bash
   [SUCCESS] script completed successfully!
   ```  
5. Reboot the server:  
   ```bash
   $ sudo init 6
   ```  
6. Wait for the server to reboot. |
| 11. | **Recovered NOAM Server:** Verify server health | Execute this command on the failed NOAM server and make sure no errors are returned:  
   ```bash
   $ sudo syscheck
   ```  
   Running modules in class hardware...OK  
   Running modules in class disk...OK  
   Running modules in class net...OK  
   Running modules in class system...OK  
   Running modules in class proc...OK  
   LOG LOCATION: /var/TKLC/log/syscheck/fail_log |
| 12. | Repeat for additional 2nd failed NOAM | Repeat steps 8.-11. for the 2nd failed NOAM server. |
| 13. | Perform keyexchange between active NOAM and recovered NOAM servers | 1. From a terminal window connection on the active NOAM as the `admusr` user, exchange SSH keys for `admusr` between the active NOAM and the recovered NOAM servers using the keyexchange utility, using the host names of the recovered NOAMs.  
2. When prompted for the password, enter the password for the `admusr` user of the recovered NOAM servers.  
   ```bash
   $ keyexchange admusr@<Recovered_NOAM Hostname>
   ``` |
### Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.</td>
<td><strong>NOAM VIP GUI:</strong> Set HA on recovered NOAMs</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; HA.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Status &amp; Manage" /></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Edit.</strong></td>
</tr>
<tr>
<td></td>
<td>3. For each NOAM server with a Max Allowed HA Role set to <strong>Standby</strong>, set it to <strong>Active.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Active Role" /></td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK.</strong></td>
</tr>
<tr>
<td>15.</td>
<td><strong>NOAM VIP GUI:</strong> Restart DSR application</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Status &amp; Manage &gt; Server.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Status &amp; Manage" /></td>
</tr>
<tr>
<td></td>
<td>2. Select each recovered NOAM server and click <strong>Restart.</strong></td>
</tr>
</tbody>
</table>
### Procedure 5. Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>16.</strong></td>
<td><strong>Recovered NOAM Servers:</strong> Activate optional features</td>
</tr>
<tr>
<td></td>
<td>Map-Diameter Interworking (MAP-IWF) and/or Policy and Charging Application (PCA) Only</td>
</tr>
<tr>
<td></td>
<td>Activate the features Map-Diameter Interworking (MAP-IWF) and Policy and Charging Application (PCA) as follows:</td>
</tr>
<tr>
<td></td>
<td><strong>For PCA:</strong></td>
</tr>
<tr>
<td></td>
<td>1. Establish SSH sessions to the all the recovered NOAM servers and login as <strong>admusr</strong>. Refer [3] DSR PCA Activation Guide and execute PCA Activation on Standby NOAM Server on all recovered NOAM servers to re-activate PCA.</td>
</tr>
<tr>
<td></td>
<td>2. Establish SSH session to the recovered active NOAM and login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>For MAP-IWF:</strong></td>
</tr>
<tr>
<td></td>
<td>1. Establish SSH session to the recovered active NOAM and login as <strong>admusr</strong>. Refer to [4] DSR MAP-Diameter IWF Feature Activation Procedure to activate Map-Diameter Interworking (MAP-IWF).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:</td>
</tr>
<tr>
<td></td>
<td><code>iload#31000{S/W Fault}</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If any of the MPs are failed and recovered, then these MP servers should be restarted after activation of the feature.</td>
</tr>
<tr>
<td><strong>17.</strong></td>
<td>Switch DR NOAM back to secondary</td>
</tr>
<tr>
<td></td>
<td>Once the system have been recovered: Refer Document [2] DSR/SDS 8.2 NOAM Failover User’s Guide.</td>
</tr>
<tr>
<td><strong>18.</strong></td>
<td><strong>NOAM VIP GUI:</strong> Perform key exchange with export server</td>
</tr>
<tr>
<td></td>
<td>Navigate to Administration &gt; Remote Servers &gt; Data Export.</td>
</tr>
<tr>
<td></td>
<td>1. Click <strong>SSH Key Exchange</strong> at the bottom of the screen.</td>
</tr>
<tr>
<td></td>
<td>2. Type the <strong>Password</strong> and click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
Procedure 5. Recovery Scenario 5

19. **NOAM VIP GUI:** Examine all alarms
   
   1. Log into the NOAM VIP if not already logged in.
   2. Navigate to **Alarms & Events > View Active**.

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

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

   If needed, contact My Oracle Support (MOS).

20. **NOAM VIP GUI:** Recover standby/spare SOAM and C-level servers
   
   If necessary, refer to Procedure 3 to recover any standby or spare SOAMs, or any C-level servers.

### 4.6 Recovery Scenario 6 — Database Recovery — Case 1

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

**Note:** During recovery, the corrupted database is replaced by the server runtime backup. Any configuration done after taking the backup is not available post recovery.

Procedure 6. Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th>STEP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Workaround</td>
</tr>
<tr>
<td></td>
<td>Refer to Appendix F to Check and Create Backup Directory.</td>
</tr>
</tbody>
</table>
### Procedure 6. Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong></td>
<td>Navigate to <strong>Status &amp; Manage &gt; HA</strong>.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Status &amp; Manage menu with HA option selected" /></td>
</tr>
<tr>
<td>2.</td>
<td><strong>NOAM VIP GUI:</strong> Set failed servers to standby</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="NOAM VIP GUI interface" /></td>
</tr>
<tr>
<td>2.</td>
<td>Select <strong>Edit</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Set the Max Allowed HA Role to <strong>OOS</strong> for the failed servers.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>OK</strong>.</td>
</tr>
<tr>
<td><strong>3.</strong></td>
<td><strong>Server in Question:</strong> Establish an SSH session to the server in question and login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td><strong>4.</strong></td>
<td><strong>Server in Question:</strong> Bring the system to runlevel 3.</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo init 3</code></td>
</tr>
<tr>
<td><strong>5.</strong></td>
<td><strong>Server in Question:</strong> Execute this command and follow the instructions appearing in the console prompt.</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo /usr/TKLC/appworks/sbin/backout_restore</code></td>
</tr>
<tr>
<td><strong>6.</strong></td>
<td><strong>Server in Question:</strong> Bring the system back to runlevel 4.</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo init 6</code></td>
</tr>
</tbody>
</table>
### Procedure 6. Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td><strong>Server in Question:</strong> Verify the server&lt;br&gt;$ sudo pm.getprocs&lt;br&gt;Example Output:</td>
</tr>
<tr>
<td>8.</td>
<td><strong>NOAM VIP GUI:</strong> Set failed servers to active&lt;br&gt;1. Navigate to Status &amp; Manage &gt; HA.&lt;br&gt;2. Click <strong>Edit</strong>.&lt;br&gt;3. Select the failed server and set it to <strong>Active</strong>.&lt;br&gt;4. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>9.</td>
<td><strong>Backup and archive all the databases from the recovered system</strong>&lt;br&gt;Execute Appendix E DSR Database Backup to back up the Configuration databases.</td>
</tr>
</tbody>
</table>
4.7 Recovery Scenario 6 — Database Recovery — Case 2

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

Procedure 7. Recovery Scenario 6 (Case 2)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Workaround</td>
<td>Refer to Appendix F to Check and Create Backup Directory.</td>
</tr>
<tr>
<td>2. NOAM VIP GUI: Set failed servers to standby</td>
<td></td>
</tr>
<tr>
<td>1. Navigate to <strong>Status &amp; Manage &gt; HA</strong>.</td>
<td></td>
</tr>
<tr>
<td>2. Click <strong>Edit</strong>.</td>
<td></td>
</tr>
<tr>
<td>3. Set the Max Allowed HA Role to <strong>OOS</strong> for the failed servers.</td>
<td></td>
</tr>
<tr>
<td>4. Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>3. <strong>Server in Question</strong>: Login</td>
<td>Establish an SSH session to the server in question and login as <strong>admusr</strong>.</td>
</tr>
</tbody>
</table>
### Procedure 7. Recovery Scenario 6 (Case 2)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command(s)</th>
</tr>
</thead>
</table>
| 4.   | **Server in Question**: Take server out of service | Take the server out of service.  
$ sudo bash -l  
$ prod.clobber |
| 5.   | **Server in Question**: Take server to DbUp state and start the application | Take the server to Dbup and start the DSR application.  
$ sudo bash -l  
$ prod.start |
| 6.   | **Server in Question**: Verify server state | 1. Execute the following commands to verify the processes are up and running:  
$ sudo pm.getprocs  
2. Execute the following command to verify if replication channels are up and running:  
$ sudo irepstat  
3. Execute the following command to verify if merging channels are up and running:  
$ sudo inetmstat |
| 7.   | **NOAM VIP GUI**: Restart DSR application | 1. Navigate to **Status & Manage > Server**.  
   - Network Elements  
   - Server  
   - HA  
   - Database  
   - KPIs  
   - Processes  
2. Select each recovered server and click **Restart**. |
Procedure 7. Recovery Scenario 6 (Case 2)

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**.

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

   Execute Appendix E DSR Database Backup to back up the Configuration databases.

5. **Resolve User Credential Issues after Database Restore**

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

5.1 **Restore a Deleted User**

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

These users were removed before creation of the backup and archive file. They are reintroduced by system restoration of that file.
## 5.2 Keep a Restored User

### Procedure 8. Keep Restored User

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Before Restoration: Notify Affected Users Before Restoration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Contact each user affected before the restoration and notify them that you will reset their password during this maintenance operation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STEP #</th>
<th>After Restoration: Log into the NOAM VIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Establish a GUI session on the NOAM server by using the VIP 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](image)
## Procedure 8. Keep Restored User

<table>
<thead>
<tr>
<th>3.</th>
<th>After Restoration: Reset user passwords</th>
</tr>
</thead>
</table>

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

2. Select the user.

3. Click **Change Password**.

4. Type a new password.

![Password Change Form](image)

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

- Old Password: 
- New Password: 
- Retype New Password: 

- [ ] **Force password change on next login**

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 (1@#$%^&*?)
### 5.3 Remove a Restored User

#### Procedure 9. Remove the Restored User

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>After Restoration:</strong>&lt;br&gt;Log into the NOAM VIP</td>
</tr>
</tbody>
</table>
|        | 1. Establish a GUI session on the NOAM server by using the VIP 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**

---

Unformatted text:

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.

1. After Restoration:<br>Log into the NOAM VIP

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

   `http://<Primary_NOAM_VIP_IP_Address>`

   2. Login as the *guiadmin* user:
### Procedure 9. Remove the Restored User

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset user passwords</td>
<td><img src="image" alt="Diagram" /></td>
</tr>
<tr>
<td></td>
<td>2. Select the user.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Delete</strong>.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Delete Button" /></td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong> to confirm.</td>
</tr>
</tbody>
</table>

#### 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:**
Log in and reset the passwords for all users in this category. See the steps in Procedure 8 for resetting passwords for a user.

#### 5.5 Restore an Archive that does not contain a Current User

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

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

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Before Restoration: Notify affected users before restoration</td>
<td>Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.</td>
</tr>
</tbody>
</table>
| 2. | Before Restoration: Log into the NOAM VIP | 1. Establish a GUI session on the NOAM server by using the VIP 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

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

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

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

3. Before Restoration: Record user settings

1. Navigate to Administration > Access Control > 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></th>
<th>After Restoration:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Login</td>
<td></td>
</tr>
</tbody>
</table>

1. Establish a GUI session on the NOAM server by using the VIP 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>After restoration: recreate affected user</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Administration &gt; Access Control &gt; Users</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Insert</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Recreate the user using the data collected from step 3.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

**Adding new user**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username*</td>
<td></td>
</tr>
<tr>
<td>Group*</td>
<td>admin</td>
</tr>
<tr>
<td>Authentication Options</td>
<td></td>
</tr>
<tr>
<td>Allow Remote Authentication</td>
<td></td>
</tr>
<tr>
<td>Allow Local Authentication</td>
<td></td>
</tr>
<tr>
<td>Access Options</td>
<td></td>
</tr>
<tr>
<td>Allow GUI Access</td>
<td></td>
</tr>
<tr>
<td>Allow MFA Access</td>
<td></td>
</tr>
<tr>
<td>Access Allowed</td>
<td></td>
</tr>
<tr>
<td>Account Enabled</td>
<td>Is th</td>
</tr>
<tr>
<td>Maximum Concurrent Logins</td>
<td>0</td>
</tr>
<tr>
<td>Session Inactivity Limit</td>
<td>120</td>
</tr>
<tr>
<td>Comment*</td>
<td></td>
</tr>
</tbody>
</table>
Procedure 10. Restore an Archive That Does Not Contain a Current User

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

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

6. IDIH Disaster Recovery

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

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

Procedure 11. IDIH Disaster Recovery Preparation

STEP #

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

1. Oracle Gues:
Login and perform database and health check
Establish an SSH session to the Oracle gues and login as admusr.
Execute following command to set shared memory to unlimited:

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

Output:

```
[admusr@thunderbolt-ora ~]$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i
10:16:52: STARTING HEALTHCHECK PROCEDURE
10:16:52: ORACLE_DB: ORACLE_HOME: /etc/oracle/12.2.0.4.0/oracle
10:16:52: ERP VERSION: 7.0.1.9.0-66.20.0
10:16:52: -----------------------------------------------
10:16:52: Checking disk free space
10:16:52: No disk space issues found
10:16:52: Checking syscheck - this can take a while
10:16:52: No errors in syncheck modules
10:16:52: Checking Alarm Manager alarmStatus
10:16:52: No alarms found
10:16:52: Checking statefiles
10:16:52: Statefiles do not exist
10:16:52: Checking runlevel
10:16:52: Runlevel is OK (N 4)
10:16:52: Checking upgrade log
10:16:52: Install logs are free of errors
10:16:52: Analyzing date
10:16:52: NTP daemon is running
10:16:52: Server is synchronized with ntp server
10:16:52: Checking NTP status
10:16:52: twre-host is integrated
10:16:52: Ntp settings is OK
10:16:52: oracle is present in /etc/hosts
10:16:52: mediation is present in /etc/hosts
10:16:52: appserver is present in /etc/hosts
10:16:52: Ping server entries in host file.
10:16:52: Ping server oracle
10:16:52: Ping server mediation
10:16:52: Ping server appserver
10:16:52: Check oracle Server
10:16:52: Oracle server and resources online
10:16:52: All tests passed:
10:16:52: ENDING HEALTHCHECK PROCEDURE WITH CODE 0

[admusr@thunderbolt-ora ~]$
### Procedure 11. IDIH Disaster Recovery Preparation

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Note:</td>
<td>If this step fails, a re-installation is necessary using these procedures from reference [1].</td>
</tr>
<tr>
<td></td>
<td><strong>For VMware-based deployments:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Section 5.6: (VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Section 5.9: Configure iDIH Virtual Machines</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>For KVM/OpenStack-based deployments:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Section 5.7: Create iDIH Virtual Machines (KVM/Openstack)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Section 5.9: Configure iDIH Virtual Machines</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>For OVM-S/OVM-M-based deployments:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Section 5.8: Create iDIH Virtual Machines (OVM-S/OVM-M)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Section 5.9: Configure iDIH Virtual Machines</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>This procedure performs disaster recovery for the IDIH by re-installing the mediation and application servers.</strong></td>
<td>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>Create iDIH Application and Mediation VMs</td>
<td>Execute the following procedure from [1] to recover the Application and Mediation VMs: <strong>For VMware-based deployments:</strong> Section 5.6: (VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional) <strong>For KVM/OpenStack-based deployments:</strong> Section 5.7: Create iDIH Virtual Machines (KVM/Openstack) <strong>For OVM-S/OVM-M-based deployments:</strong> Section 5.8: Create iDIH Virtual Machines (OVM-S/OVM-M). Import three IDIH OVAs and create and configure a VM for each.</td>
</tr>
<tr>
<td>2.</td>
<td>Configure iDIH VM Networks</td>
<td>Execute the following procedure from [1] to configure the VM networks on the Application and Mediation VMs only: Section 5.9: Configure iDIH VM Networks</td>
</tr>
<tr>
<td>3.</td>
<td>Configure VMs</td>
<td>Execute the following procedure from [1]: Section 5.10, Post iDIH Installation Configuration, Procedure 38. Run Post Installation Scripts on iDIH VMs, steps 3 through 7</td>
</tr>
<tr>
<td>4.</td>
<td>Integrate into DSR (Optional)</td>
<td>If integration is needed, execute the following procedure from [1]: Section 5.10, Post iDIH Installation Configuration, Procedure 41. Integrate iDIH into DSR</td>
</tr>
</tbody>
</table>
Procedure 12. IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

<table>
<thead>
<tr>
<th>Step</th>
<th>PMAC GUI: Monitor the configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>If not already done so, establish a GUI session on the PMAC server.</td>
</tr>
<tr>
<td></td>
<td>Navigate to Status &amp; Manage &gt; Task Monitoring.</td>
</tr>
<tr>
<td>1.</td>
<td>Monitor the IDIH configuration to completion.</td>
</tr>
<tr>
<td></td>
<td>Alternatively, you can monitor the fdconfig status through the command line after executing the fdconfig command:</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><img src="image-url" alt="Image" /></td>
</tr>
</tbody>
</table>

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

Procedure 13. Inhibit A and B Level Replication on C-level Servers

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

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

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

If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.
Procedure 13. Inhibit A and B Level Replication on C-level Servers

<table>
<thead>
<tr>
<th></th>
<th>Active NOAM: Inhibit replication on all C-level servers</th>
</tr>
</thead>
</table>
| 2. | 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.
Procedure 13. Inhibit A and B Level Replication on C-level Servers

3. **Active NOAM:**
   - Verify replication has been inhibited

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

   Verification of replication inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO_SG is set as **A B**.

   **Execute this command:**

   ```
   $ iqt NodeInfo
   ```

   **Output:**

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

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

Procedure 14. Un-Inhibit A and B Level Replication on C-Level Servers

**STEP #**

<table>
<thead>
<tr>
<th>1. <strong>Active NOAM:</strong></th>
<th>Log into the active NOAM server using SSH as <em>admusr</em>.</th>
</tr>
</thead>
</table>

This procedure un-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 14. Un-Inhibit A and B Level Replication on C-Level Servers

<table>
<thead>
<tr>
<th>2.</th>
<th>Active NOAM: Un-Inhibit replication on all C-level servers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Execute the script from <code>/usr/TKLC/dsr/tools/InhibitReplication.sh</code>, if available. If the <code>/usr/TKLC/dsr/tools/</code> path does not have the <code>InhibitReplication.sh</code> script, then use this manual command. <code>#/usr/TKLC/dsr/tools/InhibitReplication.sh --replication=allow --SO_SG_Name=&lt;SOAM server group name&gt;</code></td>
</tr>
<tr>
<td></td>
<td>Alternatively to the above script, if the script is not in the specific path:</td>
</tr>
</tbody>
</table>

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

For example, if SOAM1 belongs to the site being recovered, then the server group is SO_SG.
Procedure 14. Un-Inhibit A and B Level Replication on C-Level Servers

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Un-Inhibit A and B Level Replication on C-Level Servers</td>
</tr>
</tbody>
</table>

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

Verification of replication inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO_SG is set as **A B**.

Execute this command:

```
$ sudo iqt NodeInfo
```

**Output:**

```
nodeId  nodeName  hostName  nodeCapability  inhibitRe
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 C. Inhibit A and B Level Replication on C-level Servers

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

**STEP #**

1. **Active NOAM:**
   - Login

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

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

   Execute this command:

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

   **Note:** SOAM Site_NAME 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 15. Inhibit A and B Level Replication on C-level Servers

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

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

   Execute this command:

   ```
   $ iqt NodeInfo
   ```

   **Output:**

   ```
   nodeId  nodeName  hostName  nodeCapability  inhibitRepPlans  siteId
   00_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 D. Un-Inhibit A and B Level Replication on C-level Servers

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

<table>
<thead>
<tr>
<th>STEP</th>
<th><strong>Active NOAM:</strong> Un-Inhibit replication on all C-level servers</th>
<th>Execute this command:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log into the active NOAM server using SSH as admusr.</td>
<td>$ for i in $(iqt -p -z -h -fhostName NodeInfo where &quot;nodeId like 'C*' and siteId='&lt;SOAM_Site_NE_name&gt;'&quot;); do iset -finhibitRepPlans=''; NodeInfo where &quot;nodeName='$i'&quot;; done</td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td><strong>Note:</strong> SOAM Site NE name of the site can be found out by logging into the active NOAM GUI and navigating to Configuration &gt; 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.</td>
</tr>
</tbody>
</table>
Procedure 16. Un-Inhibit A and B Level Replication on C-level Servers

<table>
<thead>
<tr>
<th>Procedure 16. Un-Inhibit A and B Level Replication on C-level Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. <strong>Active NOAM:</strong> Verify replication has been Inhibited</td>
</tr>
<tr>
<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.</td>
</tr>
<tr>
<td>Verification of replication un-inhibition on MPs can be done by analyzing NodeInfo output. The InhibitRepPlans field for all the MP servers for the selected site, for example, Site SO_HPC03 is set as A B.</td>
</tr>
<tr>
<td>Execute this command:</td>
</tr>
<tr>
<td>$ sudo igt NodeInfo</td>
</tr>
<tr>
<td><strong>Output:</strong></td>
</tr>
<tr>
<td>nodeId  nodeName  hostName  nodeCapability  inhibitRepPlans  siteId</td>
</tr>
<tr>
<td>excludeTables</td>
</tr>
<tr>
<td>A1386.099  NO1  NO1  Active  NO_HPC03</td>
</tr>
<tr>
<td>B1754.109  SO1  SO1  Active  SO_HPC03</td>
</tr>
<tr>
<td>C2254.131  MP2  MP2  Active  A B  SO_HPC03</td>
</tr>
<tr>
<td>C2254.233  MP1  MP1  Active  A B  SO_HPC03</td>
</tr>
</tbody>
</table>

Appendix E. DSR Database Backup

Procedure 17. DSR Database Backup

**STEP #**

The intent of this procedure is to back up the provision and configuration information from an NOAM or SOAM server after the disaster recovery is complete.

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>NOAM/SOAM VIP: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Login</td>
</tr>
<tr>
<td>1.</td>
<td>Establish a GUI session on the NOAM or SOAM server by using the VIP address of the NOAM or SOAM server. Open the web browser and enter a URL of:</td>
</tr>
<tr>
<td></td>
<td>http://&lt;Primary_NOAM/SOAM_VIP_IP_Address&gt;</td>
</tr>
<tr>
<td>2.</td>
<td>Login as the guiadmin user:</td>
</tr>
</tbody>
</table>
### Procedure 17. DSR Database Backup

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

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

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

   ![Backup Window]

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

   **Database Backup**
   
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server: ZombieNOAM1</td>
<td></td>
</tr>
<tr>
<td>Select data for backup</td>
<td></td>
</tr>
<tr>
<td>Compression</td>
<td>gzip, bzip2, none</td>
</tr>
<tr>
<td>Archive Name</td>
<td>Backup.dsr.ZombieNOAM1.Configuration.NETV</td>
</tr>
<tr>
<td>Comment</td>
<td></td>
</tr>
</tbody>
</table>

4. Enter a filename for the backup and click **OK**.

- **NOAM/SOAM VIP**: Backup configuration data for the system
### Procedure 17. DSR Database Backup

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

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

2. Select the active NOAM or SOAM tab.

3. The files on this server display. Verify the existence of the backup file.

4. **NOAM/SOAM VIP**: Download the file to a local machine
   - From the previous step, select the backup file.
   - Click **Download**.
   - Click **OK** to confirm the download.

5. **Upload the image to a secure location**
   - Transfer the backed up image saved in the previous step to a secure location where the server backup files are located in case of system disaster recovery.

6. **Backup active SOAM**
   - Repeat steps 2. through 5. to back up the active SOAM.
Appendix F. Check and Create Backup Directory

Procedure 18. Backup Directory

This procedure checks and creates the backup directory. 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. **NOAM/SOAM VIP Console:**
   - Determine if backup directory exists
   - Execute this command on an active NOAM/SOAM server console (accessed using the VIP) and compare the output.
     - $ cd /var/TKLC/db/filemgmt/
     - $ ls -ltr
   - Look for the backup directory in the output.
   - 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
   - If the directory is already there with correct permissions, then skip steps 2 and 3.
   - If directory does not have the correct permissions, then go to step 3.

2. **NOAM/SOAM VIP Console:**
   - Create backup directory
   - Go to the backup directory location.
     - cd /var/TKLC/db/filemgmt/
   - Create backup directory.
     - $ mkdir backup
   - 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.

3. **NOAM/SOAM VIP Console:**
   - Change permissions of backup directory
   - 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.
   - Change permissions for the backup directory.
     - $ chmod 770 /var/TKLC/db/filemgmt/backup
   - Change ownership of backup directory.
     - $ sudo chown -R awadmin:awadm /var/TKLC/db/filemgmt/backup
   - Directory displays as follows:
     - drwxrwx--- 2 awadmin awadm 4096 Dec 22 02:15 backup
Procedure 18. Backup Directory

| 4. | NOAM/SOA M VIP Console: Copy the backup file to the backup directory |
|    | 1. Copy the backup file to the backup directory. |
|    | $ cp BACKUPFILE /var/TKLC/db/filemgmt/backup |
|    | 2. Change permissions of files in the backup directory. |
|    | $ chmod 666 Backup.* |
|    | 3. Change ownership of files in the backup directory. |
|    | $ sudo chown -R awadmin:awadm Backup.* |

Appendix G. My Oracle Support (MOS)

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

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