Oracle Communications Diameter Signaling Router, DSR Cloud Disaster Recovery Guide

Copyright ©2010, 2017 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, 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:** Use only the DR procedures included in the Disaster Recovery Kit.

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

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

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

See more information on MOS in the Appendix section.
Table of Contents

Table of Contents ..................................................................................................................... 3
List of Procedures ....................................................................................................................... 5
List of Tables ................................................................................................................................. 5
List of Figures ................................................................................................................................. 5
1.0 Introduction ............................................................................................................................... 6
  1.1 Purpose and Scope .................................................................................................................. 6
  1.2 References .............................................................................................................................. 6
  1.3 Acronyms ................................................................................................................................ 7
  1.4 Terminology ............................................................................................................................ 8
  1.5 Optional Features ................................................................................................................... 9
  1.6 Revision History ...................................................................................................................... 9
2.0 General Description ................................................................................................................. 10
  2.1 Complete Server Outage (All Servers) - Recovery Scenario 5.1.1 .......................................... 11
  2.2 Partial server outage with one NOAM server intact and both SOAMs failed- Recovery Scenario 5.1.2 ........................................................................................................................................... 11
  2.3 Partial server outage with both NOAM servers failed and one SOAM server intact- Recovery Scenario 5.1.3 ........................................................................................................................................... 11
  2.4 Partial server outage with NOAM and one SOAM server intact- Recovery Scenario 5.1.4.......... 12
  2.5 Partial server outage with both NOAM servers failed with DR-NOAM available- Recovery Scenario 5.1.5 ........................................................................................................................................... 12
  2.6 Partial Service outage with corrupt database ......................................................................... 12
3.0 Procedure Overview ................................................................................................................. 13
  3.1 Required Materials ................................................................................................................ 13
  3.2 Disaster Recovery Strategy .................................................................................................... 14
4.0 Procedure Preparation ............................................................................................................. 16
5.0 Disaster Recovery Procedure .................................................................................................. 17
  5.1 Recovering and Restoring System Configuration .................................................................. 18
    5.1.1 Recovery Scenario 1 (Complete Server Outage) ............................................................... 18
    5.1.2 Recovery Scenario 2 (Partial Server Outage with one NOAM server intact and both SOAMs failed) ................................................................................................................................................... 18
    5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact) ................................................................................................................................................... 49
    5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact) ................................................................................................................................................... 78
    5.1.5 Recovery Scenario 5 (Partial Server Outage with all NOAM servers failed with DR-NOAM available) ................................................................................................................................................... 99
## Table of Contents

- **5.1.6 Recovery Scenario 6 (Database Recovery)** ................................................................. 126
- **6.0 Resolving User Credential Issues after Database Restore** ............................................ 132
  - **6.1 Restoring a Deleted User** ............................................................................................ 132
  - **6.2 Keeping a Restored user** ............................................................................................ 133
  - **6.3 Removing a Restored User** .......................................................................................... 135
  - **6.4 Restoring a Modified User** .......................................................................................... 137
  - **6.5 Restoring an Archive that does not contain a Current User** ........................................ 138
- **7.0 IDIH Disaster Recovery** .................................................................................................. 141
- **Appendix A. DSR Database Backup** .................................................................................. 144
- **Appendix B. Inhibit A and B Level Replication on C-Level Servers** .................................... 148
- **Appendix C. Un-Inhibit A and B Level Replication on C-Level Servers** .............................. 150
- **Appendix D. Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)** .............................................................................. 151
- **Appendix E. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)** .............................................................................. 153
- **Appendix F. Workarounds for Issues not fixed in this Release** ............................................ 156
- **Appendix G. My Oracle Support (MOS)** .............................................................................. 156
List of Procedures

Table 1: Acronyms ........................................................................................................... 7
Table 2: Terminology ........................................................................................................ 8
Table 3: Optional Features............................................................................................... 9
Table 4: Revision History ............................................................................................... 9
Table 5: Recovery Scenarios ............................................................................................ 16
Procedure 1: Recovery Scenario 1 .................................................................................. 19
Procedure 2: Recovery Scenario 2 .................................................................................. 50
Procedure 3: Recovery Scenario 3 ................................................................................... 79
Procedure 4: Recovery Scenario 4 ................................................................................... 100
Procedure 5: Recovery Scenario 5 .................................................................................. 119
Procedure 6: Recovery Scenario 6 (Case 1) .................................................................... 127
Procedure 6: Recovery Scenario 6 (Case 2) .................................................................... 128
Procedure 7: Keep Restored User .................................................................................. 133
Procedure 8: Remove the Restored User ........................................................................ 135
Procedure 9: Restoring an Archive that does not Contain a Current User .................... 138
Procedure 10: IDIH Disaster Recovery Preparation ....................................................... 141
Procedure 11: IDIH Disaster Recovery (Re-Install Mediation and Application Servers) .... 143
Procedure 12: Back up the provision and configuration data .......................................... 144
Procedure 13: Inhibit A and B Level Replication on C-Level Servers ............................... 148
Procedure 14: Un-Inhibit A and B Level Replication on C-Level Servers ....................... 150
Procedure 13: Inhibit A and B Level Replication on C-Level Servers ............................... 151
Procedure 14: Un-Inhibit A and B Level Replication on C-Level Servers ....................... 153

List of Tables

Table 1: Acronyms ........................................................................................................... 7
Table 2: Terminology ........................................................................................................ 8
Table 3: Optional Features............................................................................................... 9
Table 4: Revision History ............................................................................................... 9
Table 5: Recovery Scenarios ............................................................................................ 16

List of Figures

Figure 1. Determining Recovery Scenario ....................................................................... 15
1.0 Introduction

1.1 Purpose and Scope

This document is a guide to describe procedures used to execute disaster recovery for 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 that components dependent on DSR might need to be recovered as well, for example SDS and IDIH.

Note: Please note that failures can happen from the host or Infrastructure level too. 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.

1.2 References

### 1.3 Acronyms

**Table 1: Acronyms**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIOS</td>
<td>Basic Input Output System</td>
</tr>
<tr>
<td>CD</td>
<td>Compact Disk</td>
</tr>
<tr>
<td>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>iDIH</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>
<tr>
<td>PDRA</td>
<td>Policy Diameter Routing Agent</td>
</tr>
<tr>
<td>PCA</td>
<td>Policy and Charging Application</td>
</tr>
<tr>
<td>RBAR</td>
<td>Range Based Address Resolution</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage Area Network</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure File Transfer Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SOAM</td>
<td>Systems Operations, Administration &amp; Maintenance</td>
</tr>
<tr>
<td>TPD</td>
<td>Tekelec Platform Distribution</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>vSTP</td>
<td>Virtual Signaling Transfer Point</td>
</tr>
</tbody>
</table>
1.4 Terminology

Table 2: Terminology

<table>
<thead>
<tr>
<th>Base software</th>
<th>Base software includes deploying the VM image.</th>
</tr>
</thead>
<tbody>
<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>
1.5 Optional Features

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

Table 3: Optional Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diameter Mediation</td>
<td>DSR Meta Administration Feature Activation Procedure, E58661</td>
</tr>
<tr>
<td>Full Address Based Resolution (FABR)</td>
<td>DSR FABR Feature Activation Procedure, E78925</td>
</tr>
<tr>
<td>Range Based Address Resolution (RBAR)</td>
<td>DSR RBAR Feature Activation Procedure, E78926</td>
</tr>
<tr>
<td>Map-Diameter Interworking (MAP-IWF)</td>
<td>DSR MAP-Diameter IWF Feature Activation Procedure, E78927</td>
</tr>
<tr>
<td>Policy and Charging Application (PCA)</td>
<td>DSR PCA Activation Procedure, E81528</td>
</tr>
<tr>
<td>Host Intrusion Detection System (HIDS)</td>
<td>DSR Security Guide, E76974-01, Section 3.2</td>
</tr>
</tbody>
</table>

1.6 Revision History

Table 4: Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 22, 2016</td>
<td>Initial Release</td>
</tr>
</tbody>
</table>
## 2.0 General Description

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

<table>
<thead>
<tr>
<th>Recovery Scenario</th>
<th>Description</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1</td>
<td>Recovery Scenario 1 (Complete Server Outage)</td>
<td>All NOAM servers failed, All SOAM servers failed, 1 or more MP servers failed</td>
</tr>
<tr>
<td>5.1.2</td>
<td>Recovery Scenario 2 (Partial Server Outage with one NOAM server intact and both SOAMs failed)</td>
<td>1 or more NOAM servers intact, All SOAM servers or MP servers failed</td>
</tr>
<tr>
<td>5.1.3</td>
<td>Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact)</td>
<td>All NOAM servers failed, 1 or more SOAM servers intact</td>
</tr>
<tr>
<td>5.1.4</td>
<td>Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)</td>
<td>1 or more NOAM servers intact, 1 or more SOAM servers intact, 1 or more MP servers failed</td>
</tr>
<tr>
<td>5.1.5</td>
<td>Recovery Scenario 5 (Partial Server Outage with all NOAM servers failed with DR-NOAM available)</td>
<td>All NOAM servers failed, 1 or more SOAM servers intact, DR-NOAM available</td>
</tr>
<tr>
<td>5.1.6</td>
<td>Recovery Scenario 6 (Database Recovery)</td>
<td>Server having a corrupted database</td>
</tr>
</tbody>
</table>
2.1 Complete Server Outage (All Servers) - Recovery Scenario 5.1.1

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 5.1.2

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 5.1.3

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 servers.
2.4 Partial server outage with NOAM and one SOAM server intact- Recovery Scenario 5.1.4

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 both NOAM servers failed with DR-NOAM available- Recovery Scenario 5.1.5

Scenario:

- All NOAM servers failed
- 1 or more SOAM servers intact
- DR-NOAM available

This case assumes that a partial outage with both NOAM servers failed but a DR NOAM available. The DR NOAM is switched from secondary to primary then recovers the failed NOAM servers.

2.6 Partial Service outage with corrupt database

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

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

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

3.1 Required Materials

The following items are needed for disaster recovery:

1. A hardcopy of this document (E76332) and hardcopies of all documents in the reference list.
2. Hardcopy of all NAPD performed at the initial installation and network configuration of this customer’s site. If the NAPD cannot be found, escalate this issue within My Oracle Support (MOS) until the NAPD documents can be located.
3. DSR recent backup files: electronic backup file (preferred) or hardcopy of all DSR configuration and provisioning data.
5. The 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 2.0.
2. Read and review the content in this document.
3. Gather required materials in section 3.1 Required Materials
4. From the failure conditions, determine the Recovery Scenario and procedure to follow (using Figure 1. Determining Recovery Scenario.)
5. Execute appropriate recovery procedures (listed in section 5.0).
Figure 1. Determining Recovery Scenario

- Identify all failed servers
- Follow Recovery Scenario 6 (Case 2)
- Is database Corrupted?
  - Yes
  - Follow Recovery Scenario 6 (Case 2)
  - No
  - Is Replication inhibited on the failed server?
    - Yes
    - Follow Recovery Scenario 5
    - No
    - Is the recent database backup available that can be restored?
      - Yes
      - Follow Recovery Scenario 6 (Case 1)
      - No
      - Are both NOAM Servers Failed?
        - Yes
        - Follow Recovery Scenario 2
        - No
        - Are both SOAM servers failed?
          - Yes
          - Follow Recovery Scenario 4
          - No
          - Follow Recovery Scenario 3
    - No
    - Are ALL (including Spare) SOAM servers failed?
      - Yes
      - Follow Recovery Scenario 1
      - No
      - Re-Install
4.0 Procedure Preparation

Disaster recovery procedure execution is dependent on the failure conditions in the network. The severity of the failure determines the recovery scenario for the network. Use Table 5: Recovery Scenarios below to evaluate the correct recovery scenario and follow the procedure(s) listed to restore operations.

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

Table 5: Recovery Scenarios

<table>
<thead>
<tr>
<th>Recovery Scenario</th>
<th>Failure Condition</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>- All NOAM servers failed.</td>
<td>Section 5.1.1 Recovery Scenario 1 (Complete Server Outage)</td>
</tr>
<tr>
<td></td>
<td>- All SOAM servers failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- MP servers may or may not be failed.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>- At least 1 NOAM server is intact and available.</td>
<td>Section 5.1.2 Recovery Scenario 2 (Partial Server Outage with one NOAM server intact and both SOAMs failed)</td>
</tr>
<tr>
<td></td>
<td>- All SOAM servers failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- MP servers may or may not be failed.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>- All NOAM servers failed.</td>
<td>Section 5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact)</td>
</tr>
<tr>
<td></td>
<td>- At least 1 SOAM server out of Active, StandBy, Spare is intact and available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- MP servers may or may not be failed.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>- At least 1 NOAM server is intact and available.</td>
<td>Section 5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)</td>
</tr>
<tr>
<td></td>
<td>- At least 1 SOAM server out of Active, StandBy, Spare is intact and available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 1 or more MP servers have failed.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>- Both NOAM servers failed in Primary site</td>
<td>Section 5.1.5 Recovery Scenario 5 (Partial Server Outage with all</td>
</tr>
<tr>
<td></td>
<td>- At least 1 SOAM server out of Active, StandBy, Spare is intact and available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- DR-NOAM is available</td>
<td></td>
</tr>
</tbody>
</table>
| 6: Case 1 | Server is intact  
Database gets corrupted on the server  
Replication is occurring to the server with corrupted database | Section 5.1.6.1 Recovery Scenario 6: Case 1 |
|---|---|---|
| 6: Case 2 | Server is intact  
Database gets corrupted on the server  
Latest Database backup of the corrupt server is NOT present  
Replication is inhibited (either manually or because of comcol upgrade barrier) | Section 5.1.6.2 Recovery Scenario 6: Case 2 |

### 5.0 Disaster Recovery Procedure

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

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

```
**** WARNING *****

**** WARNING *****
```

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

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

5.1.1 Recovery Scenario 1 (Complete Server Outage)
For a complete server outage, 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 will automatically reconfigure 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 (i.e. stale DB on DP servers will not receive updates until SDS-SOAM servers are recovered.
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step #</th>
<th>Workarounds</th>
<th>Gather Required Materials</th>
<th>Recover the Failed Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Workarounds</strong></td>
<td>Refer to Appendix F. Workarounds for Issues not fixed in this Release to understand/apply any workarounds required during this procedure.</td>
<td>For VMWare based deployments:</td>
</tr>
<tr>
<td>2.</td>
<td><strong>Gather Required Materials</strong></td>
<td>Gather the documents and required materials listed in Section 3.1 Required Materials</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td><strong>Recover the Failed Software</strong></td>
<td>For VMWare based deployments:</td>
<td>1. For NOAMs execute the following procedures from reference [1]:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>a. Procedure 1 (VMWare). Import DSR OVA [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]</td>
</tr>
<tr>
<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>2. For SOAMs execute the following procedures from reference [1]:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>a. Procedure 1 (VMWare). Import DSR OVA [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]</td>
</tr>
<tr>
<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>3. For failed MPs execute the following procedures from reference [1]:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>a. Procedure 1 (VMWare). Import DSR OVA [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]</td>
</tr>
<tr>
<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>For KVM / Openstack based deployments:</td>
</tr>
<tr>
<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>a. Procedure 4 (KVM / Openstack). Import DSR OVA [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]</td>
</tr>
<tr>
<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>2. For SOAMs execute the following procedures from reference [1]:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>a. Procedure 4 (KVM / Openstack). Import DSR OVA [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]</td>
</tr>
</tbody>
</table>
## Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Procedure 4 (KVM / Openstack). Import DSR OVA [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]</td>
</tr>
<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 [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]</td>
</tr>
<tr>
<td>b.</td>
<td>Procedure 6 (KVM / Openstack Only). Configure Remaining DSR guests based on resource profile</td>
</tr>
<tr>
<td>For OVM-S / OVM-M based deployments:</td>
<td></td>
</tr>
<tr>
<td>Execute the following procedures from reference [1]:</td>
<td></td>
</tr>
<tr>
<td>a.</td>
<td>Procedure 7 (OVM-S/OVM-M). Import DSR OVA and prepare for VM creation</td>
</tr>
<tr>
<td>b.</td>
<td>Procedure 8 (OVM-S/OVM-M). Configure each DSR VM</td>
</tr>
<tr>
<td>Note: While executing Procedure 8, configure the required failed VMs only (NOAMs/NOAMs/MPs)</td>
<td></td>
</tr>
</tbody>
</table>

### Section 4: Obtain Latest Database Backup and Network Configuration Data.

Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources.

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

### Section 5: Execute DSR Installation Procedure for the First NOAM

Verify the networking data for Network Elements

**Note:** Use the backup copy of network configuration data and site surveys (Step 2)

**Execute** installation procedures for the first NOAM server from reference [1]:

Procedure 9 “Configure the First NOAM NE and Server” and

Procedure 10 “Configure the NOAM Server Group”.
## Procedure 1: Recovery Scenario 1

| 6. | **NOAM GUI:** Login | Login to the NOAM GUI as the `guiadmin` user: |

| **Oracle System Login** |

Log In  
Enter your username and password to log in  
Session was logged out at 6:41:39 am.  
Username: guiadmin  
Password:  
[ ] Change password  
Log In

Welcome to the Oracle System Login.

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

Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
Procedure 1: Recovery Scenario 1

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

   - **NOAM GUI:**
     - **Browse to** Main Menu->Status & Manage->Files
   
     Select the Active NOAM server. The following screen will appear:

     Main Menu: Status & Manage -> Files

     ![Main Menu Screen]

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

     Click on **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>8.</th>
<th><strong>NOAM GUI:</strong> Disable Provisioning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Click on <strong>Main Menu-&gt;Status &amp; Manage-&gt;Database</strong></td>
</tr>
<tr>
<td></td>
<td>Disable Provisioning by clicking on <strong>Disable Provisioning</strong> button at the bottom of the screen as shown below.</td>
</tr>
<tr>
<td></td>
<td>A confirmation window will appear, press <strong>OK</strong> to disable Provisioning.</td>
</tr>
<tr>
<td></td>
<td>The message <em>“Warning Code 002”</em> will appear.</td>
</tr>
</tbody>
</table>
**Procedure 1: Recovery Scenario 1**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td><strong>NOAM GUI:</strong> Verify the Archive Contents and Database Compatibility</td>
</tr>
</tbody>
</table>

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

The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 13** of this procedure.

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

**Note:** You will get a database mismatch regarding the NodeIDs of the VMs. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix G. My Oracle Support (MOS).

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

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

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

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

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

If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>10.</th>
<th><strong>ACTIVE NOAM:</strong> Restore the Database</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Click on Main Menu-&gt;Status &amp; Manage-&gt;Database</strong></td>
</tr>
<tr>
<td></td>
<td>Select the Active NOAM server, and click on <strong>Restore</strong> as shown below.</td>
</tr>
<tr>
<td></td>
<td>The following screen will be displayed. Select the proper back up provisioning and configuration file.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Select archive to Restore on server: Zombie" /></td>
</tr>
<tr>
<td></td>
<td>Click <strong>OK</strong> Button. The following confirmation screen will be displayed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You will get a database mismatch regarding the NodeIDs of the servers. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix G. My Oracle Support (MOS).</td>
</tr>
<tr>
<td></td>
<td>Select the <strong>Force</strong> checkbox as shown above and Click <strong>OK</strong> to proceed with the DB restore.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Database Restore Confirm" /></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> After the restore has started, the user will be logged out of XMI NO GUI since the restored Topology is old data.</td>
</tr>
</tbody>
</table>
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Login</th>
<th>Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.</td>
<td></td>
<td><strong>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</strong></td>
</tr>
<tr>
<td></td>
<td><em>NOAM VIP GUI: Login</em></td>
<td>Login as the <code>guiadmin</code> user:</td>
</tr>
</tbody>
</table>

![Oracle System Login](image)

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Monitor and Confirm database restoral</th>
<th>Wait for <strong>5-10 minutes</strong> for the System to stabilize with the new topology:</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.</td>
<td></td>
<td>Monitor the Info tab for <strong>“Success”</strong>. This will indicate that the backup is complete and the system is stabilized.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Following alarms <strong>must</strong> be ignored for NOAM and MP Servers until all the Servers are configured:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alarms with Type Column as <strong>“REPL”</strong>, <strong>“COLL”</strong>, <strong>“HA”</strong> (with mate NOAM), <strong>“DB”</strong> (about Provisioning Manually Disabled)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: Do not pay attention to alarms until all the servers in the system are completely restored.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: The Configuration and Maintenance information will be in the same state it was backed up during initial backup.</td>
</tr>
</tbody>
</table>
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.</td>
<td><strong>ACTIVE NOAM:</strong> Login</td>
<td>Login to the recovered Active NOAM via SSH terminal as <code>admusr</code> user.</td>
</tr>
<tr>
<td>14.</td>
<td><strong>NOAM VIP GUI:</strong> Recover Standby NOAM</td>
<td>Install the second NOAM server by executing procedures from reference [1] Procedure 11 “Configure the Second NOAM Server” steps 1, 3-7 Procedure 12 “Complete Configuring the NOAM Server Group” Step 4</td>
</tr>
</tbody>
</table>
| 15.  | **Active NOAM:** Correct the Recognized Authority table             | Establish an SSH session to the active NOAM, login as `admusr`.  
- 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                            | Navigate to `Main Menu->Status & Manage->Server`,  
- Select the recovered standby NOAM server and click on **Restart**.  

---

**Note:** The steps provided are for illustrative purposes and may need to be adapted based on specific system configurations and requirements.
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.</td>
<td>NOAM VIP GUI: Set HA on Standby NOAM</td>
<td>Navigate to <strong>Status &amp; Manage -&gt; HA</strong>&lt;br&gt;Click on <strong>Edit</strong> at the bottom of the screen&lt;br&gt;Select the standby NOAM server, set it to <strong>Active</strong>&lt;br&gt;Press <strong>OK</strong></td>
</tr>
<tr>
<td>18.</td>
<td>NOAM VIP GUI: Perform Keyexchange with Export Server</td>
<td>Navigate to <strong>Main Menu -&gt; Administration -&gt; Remote Servers -&gt; Data Export</strong>&lt;br&gt;Click on <strong>SSH Key Exchange</strong> at the bottom of the screen&lt;br&gt;Enter the Password and press <strong>OK</strong></td>
</tr>
</tbody>
</table>
## Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 19. | **NOAM VIP GUI:** Stop Replication to the C-Level Servers of this Site. | Inhibit Replication to the working C Level Servers which belong to the same site as of the failed SOAM servers, as the recovery of Active SOAM will cause the database wipeout in the C level servers because of the replication.  
*If the spare SOAM is also present in the site and lost:* Appendix D. 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. Inhibit A and B Level Replication on C-Level Servers |
| 20. | **NOAM VIP GUI:** Recover Active SOAM Server | Install the SOAM servers by executing procedures from reference [1]  
Procedure 18 “Configure the SOAM Servers”, steps 1, 3-7  
**NOTE:** Wait for server to reboot before continuing. |
| 21. | **NOAM VIP GUI:** Restart DSR application on Recovered Active SOAM Server | Navigate to **Main Menu->Status & Manage->Server,**  
Select the recovered server and click on Restart. |

[DSR Cloud Disaster Recovery Guide](#) | [Disaster Recovery Procedure](#)
Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>22.</th>
<th>NOAM VIP GUI: Upload the backed up SOAM Database file</th>
<th>Navigate to Main Menu-&gt;Status &amp; Manage-&gt;Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td>NOAM VIP GUI: Upload the backed up SOAM Database file</td>
<td>Navigate to Main Menu-&gt;Status &amp; Manage-&gt;Files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the <strong>Active SOAM server</strong>. The following screen will appear. Click on Upload as shown below and select the file “SO Provisioning and Configuration:” file backed up after initial installation and provisioning.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Click on <strong>Browse</strong> and locate the backup file</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Check <strong>This is a backup file</strong> Box</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click on Open as shown below.</td>
</tr>
</tbody>
</table>

![Backup File Selection Screen]

Click on the **Upload** button. The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.
Procedure 1: Recovery Scenario 1

23. Recovered SOAM GUI: Login

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

http://<Recovered_SOAM_IP_Address>

Login as the guiadmin user:

Oracle System Login

Log In
Enter your username and password to log in

Session was logged out at 6:41:39 am.

username: guiadmin
password: 

Change password

Log In

Welcome to the Oracle System Login.

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

Unauthorized access is prohibited.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
### Procedure 1: Recovery Scenario 1

| 24. Recovered SOAM GUI: Verify the Archive Contents and Database Compatibility | Navigate to Main Menu->Status & Manage->Database |

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

The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 13** of this procedure.

![Database Compare](image)

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

**Note:** You will get a database mismatch regarding the NodeIDs of the VMs. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix G. My Oracle Support (MOS)

![Database Archive Compare](image)

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

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

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

**Topology Compatibility**

THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.

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

If the verification is successful, Click **BACK** button and continue to **next step** in this procedure.
**Procedure 1: Recovery Scenario 1**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 25.  | **Recovered SOAM GUI: Restore the Database**  
   - Click on **Main Menu->Status & Manage->Database**  
   - Select the **Active SOAM** server, and click on **Restore** as shown below.  
   - The following screen will be displayed. Select the proper backup provisioning and configuration file.  
   - Click **OK** button. The following confirmation screen will be displayed.  
   - If you get an error that the NodeIDs do not match. That is expected. If no other errors beside the NodeIDs are displayed, select the **Force** checkbox as shown below and click **OK** to proceed with the DB restore.  
   - **Note:** After the restore has started, the user will be logged out of XMI SOAM GUI since the restored Topology is old data.  

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 will indicate that the backup 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 will be in the same state it was backed up during initial backup. |
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>No.</th>
<th>Task Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>27.</td>
<td><strong>NOAM VIP GUI: Login</strong></td>
<td>Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Login as the <em>guiadmin</em> user:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Oracle System Login" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>NOTE:</em> Wait for server to reboot before continuing.</td>
</tr>
<tr>
<td>28.</td>
<td><strong>NOAM VIP GUI: Recover remaining SOAM Server</strong></td>
<td>Install the SOAM servers by executing procedure from reference [1]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Procedure 18 “Configure the SOAM Servers”, steps 1, 3-6</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> Wait for server to reboot before continuing.</td>
</tr>
</tbody>
</table>
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Restart DSR application on remaining SOAM Server(s)</th>
<th>Navigate to Main Menu-&gt;Status &amp; Manage-&gt;Server,</th>
</tr>
</thead>
<tbody>
<tr>
<td>29.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOAM VIP GUI: Set HA on Recovered Standby SOAM Server</td>
<td></td>
</tr>
<tr>
<td>30.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**29.**

- **NOAM VIP GUI:** Restart DSR application on remaining SOAM Server(s)

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

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

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

- Stop
- Restart
- Reboot
- NTP Sync
- Report

**30.**

- **NOAM VIP GUI:** Set HA on Recovered Standby SOAM Server

**NOTE:** For Non-HA sites **SKIP** this step.

Navigate to Status & Manage -> HA

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

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

Set Max Allowed HA Role to **Active**

Press **OK**
Procedure 1: Recovery Scenario 1

31. **NOAM VIP GUI:** Start Replication on Working C-Level Servers

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

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

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

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

   - If the “Repl Status” is set to “Inhibited”, click on the **Allow Replication** button as shown below using the following order, otherwise if none of the servers are inhibited, skip this step and continue with the next step:
     - Active NOAM Server
     - Standby NOAM Server
     - Active SOAM Server
     - Standby SOAM Server
     - Spare SOAM Server (if applicable)
     - 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 that the replication on all the working servers is allowed. This can be done by examining the Repl Status table as seen below:

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

32. **NOAM VIP GUI:** Recover the C-Level Server (DA-MP, SBRs, IPFE, SS7-MP, vSTP-MP)

   - Establish a SSH session to the C Level server being recovered, login as **admusr**.
   - Execute following command to set shared memory to unlimited:
     
     ```
     $ sudo shl.set -m 0
     ```
   - Execute the following procedures from [1] **FOR EACH** server that has been recovered:
     - Procedure 21 “Configure the MP Virtual Machines”, Steps 1, 11-14 (& 15 if required).
### Procedure 1: Recovery Scenario 1

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>33.</td>
<td><strong>NOAM VIP GUI:</strong> Restart DSR application for Recovered C-Level Server</td>
</tr>
</tbody>
</table>

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

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

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

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

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

<table>
<thead>
<tr>
<th>OAM Repl Status</th>
<th>SIG Repl Status</th>
<th>Repl Status</th>
<th>Repl Audit Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NotApplicable</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
<tr>
<td>Normal</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
<tr>
<td>Normal</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
<tr>
<td>Normal</td>
<td>NotApplicable</td>
<td>Allowed</td>
<td>NotApplicable</td>
</tr>
</tbody>
</table>
| 35. | **NOAM VIP GUI:** Set HA on all C-Level Servers | Navigate to **Status & Manage -> HA**

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

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

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

  Press **OK** |
| 36. | **ACTIVE NOAM:** Perform key exchange between the active-NOAM and recovered servers. | Establish an SSH session to the active NOAM, login as **admusr**.

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

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

  **Note:** If an export server is configured, perform this step. |
| 37. | **ACTIVE NOAM:** Activate Optional Features | Establish an SSH session to the active NOAM, login as **admusr**.

  **Note for PCA Feature Activation:**
  If you have PCA installed in the system being recovered, execute the procedure “PCA Activation on Stand By NOAM server” on recovered Standby NOAM Server and procedure “PCA Activation on Active SOAM server” on recovered Active SOAM Server from [3] to re-activate PCA

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

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

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

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

  Refer to section 1.5 Optional Features to activate any features that were previously activated. |
38. NOAM VIP GUI:
Fetch and Store the database Report for the Newly Restored Data and Save it

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

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

Select the active NOAM server and click on the Report button at the bottom of the page. The following screen is displayed:

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

```
--- d s r  Database Status Report
From: Active Network OAM&P on host ZombieNOAM1
Report Version: 2.0.0.0.0-50.9.5
User: guiadmin

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

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

Click on Save and save the report to your local machine.
39. **ACTIVE NOAM**: Verify Replication Between Servers.

Login to the Active NOAM via SSH terminal as `admusr` user. Execute the following command:

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

Output like below shall be generated:

```
-- 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

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

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

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

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

42. **NOAM GUI: Enable Provisioning**

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

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

A confirmation window will appear, press **OK** to enable Provisioning.
<table>
<thead>
<tr>
<th>Step</th>
<th>SOAM VIP GUI: Verify the Local Node Info</th>
<th>SOAM VIP GUI: Verify the Peer Node Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>43.</td>
<td>Navigate to <strong>Main Menu-&gt;Diameter-&gt;Configuration-&gt;Local Node</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Verify that all the local nodes are shown.</td>
<td></td>
</tr>
<tr>
<td>44.</td>
<td>Navigate to <strong>Main Menu-&gt;Diameter-&gt;Configuration-&gt;Peer Node</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Verify that all the peer nodes are shown.</td>
<td></td>
</tr>
</tbody>
</table>
45. **SOAM VIP GUI:** Verify the Connections Info

Navigate to **Main Menu->Diameter->Configuration->Connections**

Verify that all the connections are shown.

46. **For vSTP Only-SOAM VIP Server Console (Optional):** Verify the local nodes info

To verify the vSTP MP **Local nodes** info:

1. Login to the SOAM VIP Server console as **admusr**
2. Execute the following command
   
   ```bash
   [admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts
   ```
3. Verify the output similar to the below output

   ```json
   {
   "data": [    
   {
   "configurationLevel": "10",
   "localHostName": "AUTLocalHost1",
   "localHostPort": 4444,
   "localHostPrimIPAddress": "145.168.100.2",
   "localHostSecIPAddress": "145.168.111.1"
   },
   {
   "configurationLevel": "11",
   "localHostName": "AUTLocalHost2",
   "localHostPort": 4445,
   "localHostPrimIPAddress": "145.168.100.2",
   "localHostSecIPAddress": "145.168.111.1"
   }
   ],
   "links": {},
   "message": {},
   "status": "true"
   }
   ```
For vSTP Only-**SOAM VIP Server Console (Optional):**
Verify the remote nodes info

To verify the vSTP MP **Remote nodes** info:

1. Login to the SOAM VIP Server console as `admusr`
2. Execute the following command
   ```bash
   [admusr@SOAM1 ~]$ mmiclient.py /vstp/remotes
   ```
3. Verify the output similar to the below output

```
{
   "data": [
   {
   "configurationLevel": "12",
   "remoteHostName": "AUTRemoteHost1",
   "remoteHostPort": 4444,
   "remoteWebHostIPv4Address": "1.1.1.6",
   "remoteHostSecIPv4Address": "1.1.1.7"
   }]
   "links": {},
   "messages": [],
   "status": true
}
```

---

For vSTP Only-**SOAM VIP Server Console (Optional):**
Verify the Connections info

To verify the vSTP MP **Connections** info:

1. Login to 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 the below output

```
{
   "data": [
   { 
   "configurationLevel": "13",
   "conftCfgSetName": "Default",
   "connectionMode": "Server",
   "connectionType": "N3ua",
   "localHostName": "AUTLocalHost1",
   "name": "AUTLinkTestConn1",
   "remoteHostName": "AUTRemoteHost1"
   },
   { 
   "configurationLevel": "14",
   "conftCfgSetName": "Default",
   "connectionMode": "Server",
   "connectionType": "N2pa",
   "localHostName": "AUTLocalHost2",
   "name": "AUTLinkTestConn2",
   "remoteHostName": "AUTRemoteHost1"
   }
   ],
   "links": {},
   "messages": [],
   "status": true
}
```
<table>
<thead>
<tr>
<th></th>
<th><strong>MP Servers:</strong> Disable SCTP Auth Flag</th>
<th>For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [1]. Execute this procedure on all Failed MP Servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>49.</td>
<td>SOAM VIP GUI: Enable Connections if needed</td>
<td>Navigate to <strong>Main Menu-&gt;Diameter-&gt;Maintenance-&gt;Connections</strong> Select each connection and click on the <strong>Enable</strong> button. Alternatively you can enable all the connections by selecting the <strong>EnableAll</strong> button. Verify that the Operational State is Available. <strong>Note:</strong> 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</td>
</tr>
<tr>
<td>50.</td>
<td>SOAM VIP GUI: Enable Optional Features</td>
<td>Navigate to <strong>Main Menu -&gt; Diameter -&gt; Maintenance -&gt; Applications</strong> Select the optional feature application configured before. Click the <strong>Enable</strong> button.</td>
</tr>
<tr>
<td></td>
<td>SOAM VIP GUI: Re-enable Transports if Needed [Applicable when MAP-IWF application is activated]</td>
<td>Navigate to Main Menu-&gt;Transport Manager -&gt; Maintenance -&gt; Transport</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>52.</td>
<td></td>
<td>Select each transport and click on the <strong>Enable</strong> button</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="enable.png" alt="Enable" /> <img src="disable.png" alt="Disable" /> <img src="block.png" alt="Block" /></td>
</tr>
<tr>
<td>53.</td>
<td>SOAM VIP GUI: Re-enable MAPIWF application if needed [Applicable when MAP-IWF application is activated]</td>
<td>Navigate to Main Menu-&gt;SS7/Sigtran-&gt;Maintenance-&gt;Local SCCP Users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select each transport and click on the <strong>Enable</strong> button</td>
</tr>
<tr>
<td>54.</td>
<td>SOAM VIP GUI: Re-enable links if needed [Applicable when MAP-IWF application is activated]</td>
<td>Navigate to Main Menu-&gt;SS7/Sigtran-&gt;Maintenance-&gt;Links</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select each transport and click on the <strong>Enable</strong> button</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="enable.png" alt="Enable" /> <img src="disable.png" alt="Disable" /></td>
</tr>
<tr>
<td>55. SOAM VIP GUI: Examine All Alarms</td>
<td>Navigate to Main Menu-&gt;Alarms &amp; Events-&gt;View Active</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Alarms &amp; Events" /></td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="View Active" /></td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="View History" /></td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="View Trap Log" /></td>
<td></td>
</tr>
<tr>
<td>Examine all active alarms and refer to the on-line help on how to address them. If needed contact Appendix G. My Oracle Support (MOS).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>56. NOAM VIP GUI: Examine All Alarms</th>
<th>Login to the NOAM VIP if not already logged in. Navigate to Main Menu-&gt;Alarms &amp; Events-&gt;View Active</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="#" alt="Alarms &amp; Events" /></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="View Active" /></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="View History" /></td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="View Trap Log" /></td>
</tr>
<tr>
<td>Examine all active alarms and refer to the on-line help on how to address them. If needed contact Appendix G. My Oracle Support (MOS)</td>
<td></td>
</tr>
</tbody>
</table>

| 57. Restore GUI Usernames and Passwords | If applicable, Execute steps in Section 6.0 to recover the user and group information restored. |

| 58. Backup and Archive All the Databases from the Recovered System | Execute Appendix A. DSR Database Backup to back up the Configuration databases: |
5.1.2 Recovery Scenario 2 (Partial Server Outage with one NOAM server intact and both 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

This procedure performs recovery if at least 1 NOAM server is available but all SOAM servers in a site have failed. This includes any SOAM server that is in another location.

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

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

<table>
<thead>
<tr>
<th>STE P #</th>
<th>Workarounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Refer to <strong>Appendix F. Workarounds for Issues not fixed in this Release</strong> to understand any workarounds required during this procedure.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STE P #</th>
<th>Gather Required Materials</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Gather the documents and required materials listed in <strong>Section 3.1 Required Materials</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STE P #</th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th></th>
<th>Active NOAM: Set Failed Servers to OOS</th>
<th>Navigate to Main Menu -&gt; Status &amp; Manage -&gt; HA</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td><strong>Active NOAM:</strong></td>
<td><strong>Navigate to Main Menu -&gt; Status &amp; Manage -&gt; HA</strong></td>
</tr>
<tr>
<td></td>
<td>Set Failed Servers to OOS</td>
<td><strong>Navigate to Main Menu -&gt; Status &amp; Manage -&gt; HA</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Set Failed</strong></td>
<td><strong>Select Edit</strong></td>
</tr>
<tr>
<td></td>
<td>Servers to OOS</td>
<td><strong>Set the Max Allowed HA Role drop down box to OOS for the failed servers.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Select Ok</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Select Ok</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Select Ok</strong></td>
</tr>
</tbody>
</table>
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| 5. | Create VMs 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 [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing 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 [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing 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" [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]  
   b. Procedure 5 (KVM/Openstack): "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" [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]  
   b. Procedure 6 (KVM/Openstack): "Configure Remaining DSR guests based on resource profile"  
For OVM-S/OVM-M based deployments:  
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 [Note: While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs)]
| 6. | Repeat for Remaining Failed Servers | If necessary, repeat step 5 for all remaining failed servers. |
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Login</th>
<th>Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td></td>
<td><img src="image" alt="Oracle System Login" /></td>
</tr>
<tr>
<td></td>
<td>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</td>
<td>Login as the <em>guiadmin</em> user:</td>
</tr>
</tbody>
</table>

**Note:** If Topology or nodeld alarms are persistent after the database restore, refer to Appendix F. Workarounds for Issues not fixed in this Release or the next step below.

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Recover Standby NOAM</th>
<th>Install the second NOAM server by executing procedures from reference [1]:</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td></td>
<td>Procedure 11 &quot;Configure the Second NOAM Server&quot; steps 1, 3-7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Procedure 12 &quot;Complete Configuring the NOAM Server Group&quot; Step 4</td>
</tr>
</tbody>
</table>

[1]: Reference URL
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th></th>
<th><strong>NOAM VIP GUI:</strong></th>
<th><strong>Navigate to</strong></th>
<th><strong>Action</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td>Restart DSR application</td>
<td>Main Menu-&gt;Status &amp; Manage-&gt;Server,</td>
<td>Restart NOAM server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Status &amp; Manage</td>
<td>Stop, Restart, Reboot, NTP Sync, Report</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>10.</th>
<th><strong>NOAM VIP GUI:</strong></th>
<th><strong>Navigate to</strong></th>
<th><strong>Action</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set HA on Standby NOAM</td>
<td>Status &amp; Manage -&gt; HA</td>
<td>Edit</td>
</tr>
</tbody>
</table>

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

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

Press **OK**
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>No.</th>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.</td>
<td>NOAM VIP GUI:</td>
<td>Inhibit Replication to the working C Level Servers which belong to the same site as the failed SOAM servers, as the recovery of Active SOAM will cause the database wipeout in the C level servers because of the replication</td>
</tr>
<tr>
<td></td>
<td>NOAM VIP GUI:</td>
<td><strong>Stop Replication to the C-Level Servers of this Site.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>If the spare SOAM is also present in the site and lost:</strong></td>
<td>Appendix D. Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are lost)</td>
</tr>
<tr>
<td></td>
<td><strong>If the spare SOAM is NOT deployed in the site:</strong></td>
<td>Execute Appendix B. Inhibit A and B Level Replication on C-Level Servers</td>
</tr>
</tbody>
</table>
| 12. | NOAM VIP GUI:                             | Install the SOAM servers by executing procedure from reference [1]:  
Procedure 18 "Configure the SOAM Servers", steps 1, 3-7                                                                                 |
|     | NOAM VIP GUI:                             | **Recover Active SOAM Server**                                                                                                                                                                       |
|     | **NOTE:**                                | Wait for server to reboot before continuing.                                                                                                                                                    |
| 13. | NOAM VIP GUI:                             | Navigate to **Status & Manage -> HA**                                                                                                                                                              |
|     | **Set HA on Active SOAM**                 | **Click on Edit at the bottom of the screen**                                                                                                                                                    |
|     |                                           | **Select the Active SOAM server, set it to **Active**                                                                                                                                             |
|     |                                           | **Press OK**                                                                                                                                                                                                 |
## Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>14.</th>
<th><strong>NOAM VIP GUI:</strong> Restart DSR application</th>
</tr>
</thead>
</table>

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

Select the recovered Active SOAM server and click on **Restart**.
Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>NOAM VIP GUI:</th>
<th>Navigate to Main Menu-&gt;Status &amp; Manage-&gt;Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload the backed up SOAM Database file</td>
<td>Select the Active SOAM server. The following screen will appear:</td>
</tr>
</tbody>
</table>

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

![Image of Main Menu with Status & Manage and Files options]

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

- Click on **Browse** and locate the backup file
- Check **This is a backup file** Box
- Click on **Open** as shown below.

![Image of Upload dialog box]

Click on the **Upload** button.

The file will take a few seconds to upload depending on the size of the backup data. The file will be visible on the list of entries after the upload is complete.
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th></th>
<th>Recovered SOAM GUI: Login</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>16.</td>
<td><strong>Recovered SOAM GUI:</strong> Login</td>
<td>Establish a GUI session on the recovered SOAM server. Open the web browser and enter a URL of:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>http://&lt;Recovered_SOAM_IP_Address&gt;</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Login as the <code>guiadmin</code> user:</td>
</tr>
</tbody>
</table>

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

17. Recovered SOAM GUI: Verify the Archive Contents and Database Compatibility

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

   Select the Active SOAM server and click on the Compare.

   The following screen is displayed; click the button for the restored database file that was uploaded as a part of Step 15 of this procedure.

   **Database Compare**

   ![Database Compare](image)

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

   **Note:** You will get a database mismatch regarding the NodeIDs of the VMs. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix G. My Oracle Support (MOS).

   **Database Archive Compare**

   ![Database Archive Compare](image)

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

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

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

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

   **Note:** We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility. If the verification is successful, Click BACK button and continue to next step in this procedure.
## Procedure 2: Recovery Scenario 2

**18. Recovered SOAM GUI:**

- **Restore the Database**

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

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

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

  ![Database Compare](image)

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

  Note: You will get a database mismatch regarding the NodeIDs of the servers. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix G. My Oracle Support (MOS).

  Select the **Force** checkbox as shown above and Click **OK** to proceed with the DB restore.

  ![Database Restore Confirm](image)

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

**19. Recovered SOAM GUI:**

- **Monitor and Confirm database restore**

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

  Monitor the Info tab for **“Success”**. This will indicate that the backup 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 will be in the same state it was backed up during initial backup.
### Procedure 2: Recovery Scenario 2

| NOAM VIP GUI: Recover remaining SOAM Server | Install the SOAM servers by executing procedure from reference [1]: Procedure 18 "Configure the SOAM Servers", steps 1, 3-6  

**NOTE:** Wait for server to reboot before continuing. |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------|
| NOAM VIP GUI: Start replication on the recovered SOAMs | Un-Inhibit *(Start)* Replication to the recovered SOAM servers  

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

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

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

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

#### 22. Recovered Server: Sync NTP

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

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

Select the Recovered server and click NTP Sync button

![Start NTP Sync.](image)

Click **Ok**

**Are you sure you wish to force an NTP Sync on the following server(s)?**

**SOAM2**

![OK, Cancel buttons](image)

#### 23. NOAM VIP GUI: Set HA on SOAM Servers

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

![Snapshot](image)

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

For each SOAM server whose Max Allowed HA Role is set to Standby, set it to **Active**

Press **OK**
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.</td>
<td>NOAM VIP GUI: Restart DSR application</td>
<td>Navigate to <strong>Main Menu-&gt;Status &amp; Manage-&gt;Server</strong>. Select the recovered server and click on <strong>Restart</strong>.</td>
</tr>
<tr>
<td></td>
<td>SOAM GUI: Enable Provisioning</td>
<td>Click on <strong>Main Menu-&gt;Status &amp; Manage-&gt;Database</strong>. Enable Provisioning by clicking on <strong>Enable Site Provisioning</strong> button at the bottom of the screen as shown below. A confirmation window will appear, press <strong>OK</strong> to enable Provisioning.</td>
</tr>
</tbody>
</table>
Procedure 2: Recovery Scenario 2

26. 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>
<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>

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

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

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

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

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

- Active NOAM Server
- Standby NOAM Server
- Active SOAM Server
- Standby SOAM Server
- Spare SOAM Server (if applicable)
- 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 that the replication on all the working servers is allowed. This can be done by examining the Repl Status table as seen below:
## Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>27.</th>
<th><strong>NOAM VIP GUI:</strong> Recover the C-Level Server (DA-MP, SBRs, IPFE, SS7-MP, vSTP-MP)</th>
</tr>
</thead>
</table>

Establish a SSH session to the C Level server being recovered, login as **admusr**.

Execute following command to set shared memory to unlimited:

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

Execute the following procedures from [1] **FOR EACH** server that has been recovered:

Procedure 21 “Configure the MP Virtual Machines”, Steps 1, 8-14 (& 15 if required).
Procedure 2: Recovery Scenario 2

28. NOAM VIP GUI:
Start replication on ALL C-Level Servers

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

Navigate to Status & Manage -> Database

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

- 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)

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

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

If applicable, the Spare SOAM Server and MP/IPFE Servers would be added to the list as well.
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 29.  | **NOAM VIP GUI:** Set HA on all C-Level Servers  
Navigate to Status & Manage -> HA  
Click on Edit at the bottom of the screen  
For each server whose Max Allowed HA Role is set to Standby, set it to Active  
Press OK |
| 30.  | **ACTIVE NOAM:** Perform key exchange between the active-NOAM and recovered servers.  
Establish an SSH session to the Active NOAM, login as admusr.  
Execute the following command to perform a keyexchange from the active NOAM to each recovered server:  
\[ \$ \text{keyexchange admusr@<Recovered Server Hostname>} \]  
**Note:** If an export server is configured, perform this step. |
| 31.  | **ACTIVE NOAM:** Activate Optional Features  
Establish an SSH session to the active NOAM, login as admusr.  
**Note for PCA Feature Activation:**  
If you have PCA installed in the system being recovered, execute the procedure “PCA Activation on Standby NOAM server” on recovered NOAM Server and procedure “PCA Activation on Stand By SOAM server” on recovered Standby SOAM from [3] to re-activate PCA  
**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 1.5 Optional Features to activate any features that were previously activated. |
Procedure 2: Recovery Scenario 2

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

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

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

Select the **active NOAM** server and click on the **Report** button at the bottom of the page. The following screen is displayed:

<table>
<thead>
<tr>
<th>Table Name</th>
<th>Row Size</th>
<th>Avg</th>
<th>Max</th>
<th>Used</th>
<th>Alloc</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoPsw</td>
<td>44</td>
<td>1</td>
<td>44</td>
<td>44</td>
<td>44</td>
</tr>
<tr>
<td>CoPswInfo</td>
<td>64</td>
<td>1</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>CoPswLoco</td>
<td>36</td>
<td>1</td>
<td>36</td>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td>CountryCode</td>
<td>24</td>
<td>206</td>
<td>7344</td>
<td>7344</td>
<td>7344</td>
</tr>
<tr>
<td>OCMconfig</td>
<td>52</td>
<td>104</td>
<td>104</td>
<td>104</td>
<td>104</td>
</tr>
<tr>
<td>NocRuc</td>
<td>40</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NocRucAdd</td>
<td>52</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NocRucAdd</td>
<td>60</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NocRucAdd</td>
<td>72</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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

33. **ACTIVE NOAM:**
    - Verify Replication Between Servers.

    Login to the Active NOAM via SSH terminal as `admusr` user.
    Execute the following command:

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

    Output like below shall be generated:

    ```
    -- Policy 0 ActStb [DbReplication] -------------------------------
    -- Policy 0 ActStb [DbReplication] -------------------------------
    RDU06-MP1 -- Stby
    BC From RDU06-S01 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-S01 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-S01 -- Active
    AB To RDU06-S01 Active 0 0.50 1%R 0.03%cpu 21B/s
    RDU06-S01 -- 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

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

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

35. **NOAM VIP GUI: Verify the HA Status**
   - Click on Main Menu->Status and Manage->HA
   - Select the row for all of the servers
   - Verify that the “HA Role” is either “Active” or “Standby”.

36. **SOAM VIP GUI: Verify the Local Node Info**
   - Navigate to Main Menu->Diameter->Configuration->Local Node
   - Verify that all the local nodes are shown.
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Number</th>
<th>Task Description</th>
<th>Navigation Path</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>37.</td>
<td>SOAM VIP GUI: Verify the Peer Node Info</td>
<td>Navigate to Main Menu-&gt;Diameter-&gt;Configuration-&gt;Peer Node</td>
<td>Verify that all the peer nodes are shown.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>38.</td>
<td>SOAM VIP GUI: Verify the Connections Info</td>
<td>Navigate to Main Menu-&gt;Diameter-&gt;Configuration-&gt;Connections</td>
<td>Verify that all the connections are shown.</td>
</tr>
</tbody>
</table>
### Procedure 2: Recovery Scenario 2

**39. For vSTP Only:**

**SOAM VIP Server Console (Optional):**
Verify the local nodes info

To verify the vSTP MP Local nodes info:

1. Login to the SOAM VIP Server console as **admusr**
2. Execute the following command
   ```bash
   [admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts
   ``
3. Verify the output similar to the below output

   ```json
   {
     "data": [
       {
         "configurationLevel": "10",
         "localHostName": "AUTLocalHost1",
         "localHostPort": 4444,
         "localHostPriIPAddress": "145.168.100.2",
         "localHostSecIPAddress": "145.168.111.1"
       },
       {
         "configurationLevel": "11",
         "localHostName": "AUTLocalHost2",
         "localHostPort": 4445,
         "localHostPriIPAddress": "145.168.100.2",
         "localHostSecIPAddress": "145.168.111.1"
       }
     ],
     "links": {},
     "messages": [],
     "status": true
   }
   ```

**40. For vSTP Only:**

**SOAM VIP Server Console (Optional):**
Verify the remote nodes info

To verify the vSTP MP Remote nodes info:

1. Login to the SOAM VIP Server console as **admusr**
2. Execute the following command
   ```bash
   [admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts
   ``
3. Verify the output similar to the below output

   ```json
   {
     "data": [
       {
         "configurationLevel": "12",
         "remoteHostName": "AUTRemoteHost1",
         "remoteHostPort": 4444,
         "remoteHostPriIPAddress": "1.1.1.6",
         "remoteHostSecIPAddress": "1.1.1.7"
       }
     ],
     "links": {},
     "messages": [],
     "status": true
   }
   ```
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
</table>
| 41.  | For vSTP Only- SOAM VIP Server Console (Optional): Verify the Connections info | 1. Login to the SOAM VIP Server console as admusr  
2. Execute the following command  
   [admusr@SOAM1 ~]$ mmiclient.py/vstp/connections  
3. Verify the output similar to the below output |
| 42.  | MP Servers: Disable SCTP Auth Flag | For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS procedure from reference [1].  
Execute this procedure on all Failed MP Servers. |
## Procedure 2: Recovery Scenario 2

### 43. SOAM VIP GUI: Enable Connections if needed

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

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

Verify that the Operational State is Available.

### 44. SOAM VIP GUI: Enable Optional Features

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

Select the optional feature application configured in **step 29**.

Click the **Enable** button.
## Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>45.</td>
<td><strong>SOAM VIP GUI:</strong> Re-enable Transports if Needed&lt;br&gt;<strong>Navigate to</strong> Main Menu-&gt;Transport Manager -&gt; Maintenance -&gt; Transport&lt;br&gt;<strong>Select each transport and click on the Enable button</strong>&lt;br&gt;<strong>Verify that the Operational Status for each transport is Up.</strong></td>
</tr>
<tr>
<td>46.</td>
<td><strong>SOAM VIP GUI:</strong> Re-enable MAPIWF application if needed&lt;br&gt;<strong>Navigate to</strong> Main Menu-&gt;SS7/Sigtran-&gt;Maintenance-&gt;Local SCCP Users&lt;br&gt;<strong>Click on the Enable button corresponding to MAPIWF Application Name.</strong>&lt;br&gt;<strong>Verify that the SSN Status is Enabled.</strong></td>
</tr>
</tbody>
</table>
### Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>47.</td>
<td><strong>SOAM VIP GUI:</strong> Re-enable links if needed</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;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 Poi</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>Click on <strong>Enable</strong> button for each link.</td>
</tr>
<tr>
<td></td>
<td>Verify that the Operational Status for each link is Up.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>48.</td>
<td><strong>SOAM VIP GUI:</strong> Examine All Alarms</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;Alarms &amp; Events-&gt;View Active</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Alarms &amp; Events</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>View Active</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>View History</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>View Trap Log</strong></td>
</tr>
<tr>
<td></td>
<td>Examine all active alarms and refer to the on-line help on how to address them.</td>
</tr>
<tr>
<td></td>
<td>If needed contact Appendix G. My Oracle Support (MOS)</td>
</tr>
</tbody>
</table>
## Procedure 2: Recovery Scenario 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 49.  | **SOAM VIP GUI:** Perform Key exchange with Export Server  
      Navigate to **Main Menu -> Administration -> Remote Servers -> Data Export**  
      Navigate to **Administration**  
      **General Options**  
      **Access Control**  
      **Software Management**  
      **Remote Servers**  
      **LDAP Authentication**  
      **SNMP Trapping**  
      **Data Export**  
      **DNS Configuration**  
      Click on **Key Exchange** at the bottom of the screen  
      Enter the Password and press **OK** |
| 50.  | **NOAM VIP GUI:** Examine All Alarms  
      Login to the NOAM VIP if not already logged in.  
      Navigate to **Main Menu -> Alarms & Events -> View Active**  
      Examine all active alarms and refer to the on-line help on how to address them.  
      If needed contact Appendix G. My Oracle Support (MOS). |
| 51.  | **Backup and Archive All the Databases from the Recovered System**  
      Execute Appendix A. DSR Database Backup to back up the Configuration databases: |
5.1.3 Recovery Scenario 3 (Partial Server Outage with all NOAM servers failed and one SOAM server intact)

For a partial server outage with an SOAM server intact and available; NOAM servers are recovered using recovery procedures 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 Standby 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>Workarounds</th>
<th>1. Refer to Appendix F. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Gather Required Materials</td>
<td>Gather the documents and required materials listed in Section 3.1 Required Materials</td>
</tr>
</tbody>
</table>

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

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

If this procedure fails, contact Appendix G. My Oracle Support (MOS), and ask for assistance.
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</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 [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing 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 [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing 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 [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing 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" [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]
   b. Procedure 5 (KVM/Openstack). "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" [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]
   b. Procedure 6 (KVM/Openstack). "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" [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]
   b. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests based on resource profile"

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

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

**Note:** While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs)
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
</table>
| 4.   | **Obtain Latest Database Backup and Network Configuration Data.**  
      | Obtain the most recent database backup file from external backup sources (e.g., file servers) or tape backup sources.  
      | 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 networking data for Network Elements  
      | **Note:** Use the backup copy of network configuration data and site surveys (Step 2)  
      | **Execute** installation procedures for the first NOAM server from reference [1]:  
      | Procedure 9 “Configure the First NOAM NE and Server” and  
      | Procedure 10 “Configure the NOAM Server Group”. |
| 6.   | **NOAM GUI: Login**  
      | Login to 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 | **Browse to Main Menu->Status & Manage->Files** |

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

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

![Main Menu Screen](image)

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

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

![Browse Screen](image)

Click on the **Upload** button.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td><strong>NOAM GUI:</strong> Disable Provisioning</td>
</tr>
</tbody>
</table>

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

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

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

![Disable Provisioning Button](image)

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

![Confirmation Window](image)

The message “Warning Code 002” will appear.
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td><strong>NOAM GUI:</strong> Verify the Archive Contents and Database Compatibility</td>
</tr>
</tbody>
</table>

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

The following screen is displayed; click the button for the restored database file that was uploaded as a part of **Step 7** of this procedure.

Verify that the output window matches the screen below.

**Note:** You will get a database mismatch regarding the NodeIDs of the VMs. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix G. My Oracle Support (MOS)

**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 NOAM:

**Topology Compatibility**

THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.</td>
<td><strong>ACTIVE NOAM:</strong> Restore the Database</td>
</tr>
</tbody>
</table>

- Click on **Main Menu->Status & Manage->Database**
- Select the **Active NOAM** server, and click on **Restore** as shown below.
- The following screen will be displayed. Select the proper back up provisioning and configuration file.
- Click **OK** Button. The following confirmation screen will be displayed.

**Note:** You will get a database mismatch regarding the NodeIDs of the servers. That is expected. If that is the only mismatch, proceed, otherwise stop and contact Appendix G. My Oracle Support (MOS)

- Select the **Force** checkbox as shown above and Click **OK** to proceed with the DB restore.

**Database Restore Confirm**

- The selected database came from ZombieNOAM1.

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

**Confirm archive "backup/Backup.dsr.ZombieNOAM1.Configur**

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **11.** | **NOAM VIP GUI: Login**  
Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  
http://<Primary_NOAM_VIP_IP_Address>  
Login as the guiadmin user: |
| | ![Oracle System Login](image) |
| **12.** | **NOAM VIP GUI: Monitor and Confirm database restoral**  
Wait for 5-10 minutes for the System to stabilize with the new topology:  
Monitor the Info tab for “Success”. This will indicate that the backup is complete and the system is stabilized.  
Following alarms **must** be ignored for NOAM and MP Servers until all the Servers are configured:  
Alarms with Type Column as “REPL”, “COLL”, “HA” (with mate NOAM), “DB” (about Provisioning Manually Disabled)  
**Note:** Do not pay attention to alarms until all the servers in the system are completely restored.  
**Note:** The Configuration and Maintenance information will be in the same state it was backed up during initial backup. |
| **13.** | **ACTIVE NOAM: Login**  
Login to the recovered Active NOAM via SSH terminal as admusr user. |
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
</table>
| 14.  | **NOAM VIP GUI:** Re-enable Provisioning | Navigate to **Main Menu->Status & Manage->Database**  

![Enable Provisioning](image)  

Click on the **Enable Provisioning**. A pop-up window will appear to confirm as shown below, press **OK**. |
| 15.  | **NOAM VIP GUI:** Recover Standby NOAM | Install the second NOAM server by executing procedures from reference [1]:  
Procedure 11 “Configure the Second NOAM Server” steps 1, 3-7 |
| 16.  | **NOAM VIP GUI:** Recover Standby NOAM | Navigate to **Main Menu->Status & Manage->Server** and select the second NOAM server.  

![Status & Manage](image)  

Click **Restart**.  

![Restart](image)  

Click **OK** on the confirmation screen.  

**Note:** If Topology or nodeld alarms are persistent after the database restore, refer to Appendix F. Workarounds for Issues not fixed in this Release or the next step below. |
| 17.  | **NOAM VIP GUI:** Recover remaining failed SOAM Servers | Recover the **remaining** SOAM servers **(standby, spare)** by repeating the **following steps** for each SOAM server:  

1. Install the remaining SOAM servers by executing Procedure 18 “Configure the SOAM Servers”, steps 1, 3-7 from reference [1].  

**NOTE:** Wait for server to reboot before continuing. |
## Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>No.</th>
<th>Task Description</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.</td>
<td>NOAM VIP GUI: Restart DSR application</td>
<td>Navigate to <strong>Main Menu-&gt;Status &amp; Manage-&gt;Server</strong>, select the recovered server and click on <strong>Restart</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stop Restart Reboot NTP Sync Report</td>
</tr>
<tr>
<td>19.</td>
<td>NOAM VIP GUI: Set HA on all C-Level Servers</td>
<td>Navigate to <strong>Status &amp; Manage -&gt; HA</strong>, click <strong>Edit</strong> at the bottom of the screen. For each server whose Max Allowed HA Role is not <strong>Active</strong>, set it to <strong>Active</strong>. Press <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.</td>
<td><strong>NOAM VIP GUI:</strong> Restart DSR application  &lt;br&gt; Navigate to <strong>Main Menu-&gt;Status &amp; Manage-&gt;Server,</strong>  &lt;br&gt; Select each recovered server and click on <strong>Restart.</strong></td>
</tr>
<tr>
<td>21.</td>
<td><strong>ACTIVE NOAM:</strong> Perform key exchange between the active-NOAM and recovered servers.  &lt;br&gt; Establish an SSH session to the Active NOAM, login as <strong>admusr.</strong>  &lt;br&gt; Execute the following command to perform a keyexchange from the active NOAM to each recovered server:  &lt;br&gt; $ keyexchange admusr@&lt;Recovered Server Hostname&gt;  &lt;br&gt; <strong>Note:</strong> If an export server is configured, perform this step.</td>
</tr>
<tr>
<td>22.</td>
<td><strong>ACTIVE NOAM:</strong> Activate Optional Features  &lt;br&gt; Establish an SSH session to the active NOAM, login as <strong>admusr.</strong>  &lt;br&gt; <strong>Note for PCA Feature Activation:</strong>  &lt;br&gt; If you have PCA installed in the system being recovered, execute the procedure “PCA Activation on Active NOAM server” on recovered Active NOAM Server and procedure “PCA Activation on Stand By SOAM server” on recovered Standby SOAM from [3] to re-activate PCA  &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; iload#31000{S/W Fault}  &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 <strong>section 1.5 Optional Features</strong> to activate any features that were previously activated.</td>
</tr>
</tbody>
</table>
NOAM VIP GUI: 
Fetch and Store the database Report for the Newly Restored Data and Save it

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

Select the active NOAM server and click on the Report button at the bottom of the page. The following screen is displayed:

[Database Report Screen]

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

24. **ACTIVE NOAM:** Verify Replication Between Servers.

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

   Execute the following command:

   ```
   $ sudo irepstat -m
   ```

   Output like below shall be generated:

   ```
   -- 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%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 0.08%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

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

   Verify that the “OAM Max HA Role” is either “Active” or “Standby” for NOAM and SOAM and “Application Max HA Role” for MPs is “Active”, and that the status is “Normal” as shown below:
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th></th>
<th>NOAM VIP GUI: Verify the HA Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>26.</td>
<td>Click on <strong>Main Menu-&gt;Status and Manage-&gt;HA</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image1" alt="Status &amp; Manage menu" /></td>
</tr>
<tr>
<td></td>
<td>Select the row for all of the servers</td>
</tr>
<tr>
<td></td>
<td>Verify that the “HA Role” is either &quot;Active&quot; or “Standby”.</td>
</tr>
</tbody>
</table>

27. **SOAM VIP GUI: Verify the Local Node Info**

    ![Configuration menu](image2)

    Navigate to **Main Menu->Diameter->Configuration->Local Node**

    Verify that all the local nodes are shown.
### Procedure 3: Recovery Scenario 3

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>28.</strong></td>
<td>SOAM VIP GUI: Verify the Peer Node Info</td>
<td>Navigate to Main Menu-&gt;Diameter-&gt;Configuration-&gt;Peer Node Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify that all the peer nodes are shown.</td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>29.</strong></td>
<td>SOAM VIP GUI: Verify the Connections Info</td>
<td>Navigate to Main Menu-&gt;Diameter-&gt;Configuration-&gt;Connections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify that all the connections are shown.</td>
</tr>
</tbody>
</table>
### Procedure 3: Recovery Scenario 3

#### 30. For vSTP Only- SOAM VIP Server Console (Optional): Verify the local nodes info

To verify the vSTP MP Local nodes info:

1. Login to the SOAM VIP Server console as `admusr`
2. Execute the following command:
   
   ```bash
   [admusr@SOAM ~]$ mmiclient.py /vstp/localhosts
   ```
3. Verify the output similar to the below output
   
   ```json
   {  
   "data": [  
   {  
   "configurationLevel": "10",  
   "localHostName": "AUTLocalHost1",  
   "localHostPort": 4444,  
   "localHostPriIPAddress": "145.168.100.2",  
   "localHostSecIPAddress": "145.168.111.1"
   },  
   {  
   "configurationLevel": "11",  
   "localHostName": "AUTLocalHost2",  
   "localHostPort": 4445,  
   "localHostPriIPAddress": "145.168.100.2",  
   "localHostSecIPAddress": "145.168.111.1"
   }
   ],  
   "links": {},  
   "messages": [],  
   "status": true
   }
   ```

#### 31. For vSTP Only- SOAM VIP Server Console (Optional): Verify the remote nodes info

To verify the vSTP MP Remote nodes info:

1. Login to the SOAM VIP Server console as `admusr`
2. Execute the following command:
   
   ```bash
   [admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts
   ```
3. Verify the output similar to the below output
   
   ```json
   {  
   "data": [  
   {  
   "configurationLevel": "12",  
   "remoteHostName": "AUTRemoteHost1",  
   "remoteHostPort": 4444,  
   "remoteHostPriIPAddress": "1.1.1.4",  
   "remoteHostSecIPAddress": "1.1.1.7"
   }
   ],  
   "links": {},  
   "messages": [],  
   "status": true
   }
   ```
Procedure 3: Recovery Scenario 3

32. **For vSTP Only-**

   **SOAM VIP Server Console (Optional):**

   Verify the Connections info

   To verify the vSTP MP **Connections** info:

   1. Login to 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 the below output

   ```json
   {
     "data": [
       {
         "configurationLevel": "13",
         "connCfgSetName": "Default",
         "connectionMode": "Server",
         "connectionType": "MSua",
         "localHostName": "AUTLocalHost1",
         "name": "AUTLinkTestConn1",
         "remoteHostName": "AUTRemoteHost1"
       },
       {
         "configurationLevel": "11",
         "connCfgSetName": "Default",
         "connectionMode": "Server",
         "connectionType": "M2pa",
         "localHostName": "AUTLocalHost2",
         "name": "AUTLinkTestConn2",
         "remoteHostName": "AUTRemoteHost1"
       }
     ],
     "links": {},
     "messages": [],
     "status": true
   }
   ```

33. **SOAM VIP GUI:**

   Enable Connections if needed

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

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

   Verify that the Operational State is Available.
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>34.</td>
<td>SOAM VIP GUI: Enable Optional Features</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu -&gt; Diameter -&gt; Maintenance -&gt; Applications</strong></td>
</tr>
<tr>
<td></td>
<td>Select the optional feature application configured in <strong>step 31</strong></td>
</tr>
<tr>
<td></td>
<td>Click the <strong>Enable</strong> button.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>35.</td>
<td>SOAM VIP GUI: Re-enable Transports if Needed</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;Transport Manager -&gt; Maintenance -&gt; Transport</strong></td>
</tr>
<tr>
<td></td>
<td>Select each transport and click on the <strong>Enable</strong> button</td>
</tr>
<tr>
<td></td>
<td>Verify that the Operational Status for each transport is Up.</td>
</tr>
</tbody>
</table>
### Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 36.  | **SOAM VIP GUI:** Re-enable MAPIWF application if needed  
  Navigate to **Main Menu->SS7/Sigtran->Maintenance->Local SCCP Users**  
  Click on the **Enable** button corresponding to MAPIWF Application Name.  
  Verify that the SSN Status is Enabled. |
| 37.  | **SOAM VIP GUI:** Re-enable links if needed  
  Navigate to **Main Menu->SS7/Sigtran->Maintenance->Links**  
  Click on **Enable** button for each link.  
  Verify that the Operational Status for each link is Up. |
| 38.  | **SOAM VIP GUI:** Examine All Alarms  
  Navigate to **Main Menu->Alarms & Events->View Active**  
  Examine all active alarms and refer to the on-line help on how to address them.  
  If needed contact Appendix G. My Oracle Support (MOS) |
## Procedure 3: Recovery Scenario 3

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 39.  | **NOAM VIP GUI:** Perform Keyexchange with Export Server  

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

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

Enter the Password and press **OK** |
| 40.  | **NOAM VIP GUI:** Examine All Alarms  

Login to the NOAM VIP if not already logged in.  

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

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

If needed contact Appendix G. My Oracle Support (MOS). |
| 41.  | **Restore GUI Usernames and Passwords**  

If applicable, Execute steps in **Section 6.0** to recover the user and group information restored. |
| 42.  | **Backup and Archive All the Databases from the Recovered System**  

Execute **Appendix A. DSR Database Backup** to back up the Configuration databases: |
5.1.4 Recovery Scenario 4 (Partial Server Outage with one NOAM server and one SOAM server intact)

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

Recover Standby NOAM server by recovering 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 VM is an MP.
Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step #</th>
<th>Workarounds</th>
<th>Gather Required Materials</th>
<th>NOAM VIP GUI: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. □</td>
<td>Refer to Appendix F. Workarounds for Issues not fixed in this Release to understand/apply any workarounds required during this procedure.</td>
<td>Gather the documents and required materials listed in Section 3.1 Required Materials</td>
<td>Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:</td>
</tr>
<tr>
<td>2. □</td>
<td></td>
<td></td>
<td>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</td>
</tr>
<tr>
<td>3. □</td>
<td></td>
<td></td>
<td>Login as the <strong>guiadmin</strong> user:</td>
</tr>
</tbody>
</table>

This procedure performs recovery if at least 1 NOAM server is intact and available and 1 SOAM server is intact and available.

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

If this procedure fails, contact Appendix G. My Oracle Support (MOS), and ask for assistance.
## Procedure 4: Recovery Scenario 4

| 4. | Active NOAM:  
|    | Set Failed  
|    | Servers to OOS  |

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

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

Select **Edit**

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

Select **Ok**
**Procedure 4: Recovery Scenario 4**

<table>
<thead>
<tr>
<th>5.</th>
<th><strong>Recover the Failed Software</strong></th>
<th>For VMware based deployments:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1. For NOAMs execute the following procedures from reference [1]:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Procedure 1 (VMware). Import DSR OVA [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]</td>
</tr>
<tr>
<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>2. For SOAMs execute the following procedures from reference [1]:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Procedure 1 (VMware). Import DSR OVA [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]</td>
</tr>
<tr>
<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>3. For failed MPs execute the following procedures from reference [1]:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Procedure 1 (VMware). Import DSR OVA [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. 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" [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] |
|    |                                 | b. Procedure 5 (KVM/Openstack). "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" [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] |
|    |                                 | b. Procedure 6 (KVM/Openstack). "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" [Note: If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA] |
|    |                                 | b. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests based on resource profile" |

For OVM-S/OVM-M based deployments:

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 |
|    |                                 | Note: While executing Procedure 8, configure the required failed VMs only (NOAMs/NOAMs/MPs) |
### Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>Repeat for Remaining Failed Servers</td>
<td>If necessary, repeat 5 for all remaining failed servers.</td>
</tr>
</tbody>
</table>
| 7.   | NOAM VIP GUI: Login | Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  

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

Login as the `guiadmin` user: |
| 8.   | NOAM VIP GUI: Recover Standby NOAM if needed | Install the second NOAM server by executing procedures from reference [1]:  

Procedure 11 “Configure the Second NOAM Server” steps 1, 3-7  
Procedure 12 “Complete Configuring the NOAM Server Group” Step 4  

**Note:** If Topology or nodeld alarms are persistent after the database restore, refer to Appendix F. Workarounds for Issues not fixed in this Release, or the next step below. |
Procedure 4: Recovery Scenario 4

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 9. | **(OPTIONAL) NOAM VIP GUI:** Recover the Failed SOAM Servers if needed | If the failed server is an SOAM, recover the remaining SOAM servers (standby, spare) by repeating the following steps for each SOAM server:  
1. Install the remaining SOAM servers by executing Procedure 18 “Configure the SOAM Servers”, steps 1, 3–7 from reference [1]. |
|   |   | **NOTE:** Wait for server to reboot before continuing. |
| 10. | **Recovered Server:** Login | Establish an SSH to the recovered server’s XMI address: |
| 11. | **Recovered Server:** Sync NTP | Navigate to **Status & Manage -> Server**  
1. Status & Manage  
   - Network Elements  
   - Server  
   - HA  
   - Database  
   - KPIs  
   - Processes  
   - Tasks  
   - Files  
2. Select the Recovered server and click NTP Sync button  
   - Stop  
   - Restart  
   - Reboot  
   - NTP Sync  
   - Report  
3. Start NTP Sync.  
4. Click **Ok**  
5. Are you sure you wish to force an NTP Sync on the following server(s)?  
   - SOAM2  
6. Click **OK**  
   - **Cancel** |
**Procedure 4: Recovery Scenario 4**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.</td>
<td><strong>(OPTIONAL) NOAM VIP GUI:</strong> Set HA on Recovered Servers</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Status &amp; Manage -&gt; HA</strong></td>
</tr>
<tr>
<td></td>
<td>Click on <strong>Edit</strong> at the bottom of the screen</td>
</tr>
<tr>
<td></td>
<td>For each server whose Max Allowed HA Role is set to Standby, set it to <strong>Active</strong></td>
</tr>
<tr>
<td></td>
<td>Press <strong>OK</strong></td>
</tr>
<tr>
<td>13.</td>
<td><strong>NOAM VIP GUI:</strong> Restart DSR application</td>
</tr>
<tr>
<td></td>
<td>Navigate to <strong>Main Menu-&gt;Status &amp; Manage-&gt;Server</strong>,</td>
</tr>
<tr>
<td></td>
<td>Select the recovered server and click on <strong>Restart</strong>.</td>
</tr>
<tr>
<td>14.</td>
<td><strong>NOAM VIP GUI:</strong> Recover the C-Level Server (DA-MP, SBRs, IPFE, SS7-MP, vSTP-MP)</td>
</tr>
<tr>
<td></td>
<td>Establish a SSH session to the C Level server being recovered, login as <strong>admusr</strong>.</td>
</tr>
<tr>
<td></td>
<td>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>Execute the following procedures from [1] <strong>FOR EACH</strong> server that has been recovered:</td>
</tr>
<tr>
<td></td>
<td>Procedure 21 “Configure the MP Virtual Machines”, Steps 1, 8-14 (&amp; 15 if required).</td>
</tr>
</tbody>
</table>
Procedure 4: Recovery Scenario 4

15. NOAM VIP GUI: Restart DSR Application on recovered C-Level Servers.
   Navigate to Main Menu->Status & Manage->Server
   Select the recovered servers and click on Restart.

16. NOAM VIP GUI: Set HA on all C-Level Servers
   Navigate to Status & Manage -> HA
   Click on Edit at the bottom of the screen
   For each server whose Max Allowed HA Role is set to Standby, set it to Active
   Press OK

17. ACTIVE NOAM: Login
   Login to the recovered Active NOAM via SSH terminal as admusr user.

18. ACTIVE NOAM: Perform key exchange between the active-NOAM and recovered servers.
   Establish an SSH session to the Active NOAM, login as admusr.
   Execute the following command to perform a key exchange from the active NOAM to each recovered server:
   
   $ keyexchange admusr@<Recovered Server Hostname>
### Procedure 4: Recovery Scenario 4

| 19. ACTIVE NOAM: Activate Optional Features | Establish an SSH session to the active NOAM, login as *admusr.*

**Note For PCA Activation:**
If you have PCA installed in the system being recovered, execute the procedure “PCA Activation on Stand By NOAM server” on recovered StandBy NOAM Server and procedure “PCA Activation on Stand By SOAM server” on recovered StandBy SOAM Server from [3] to re-activate PCA.

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

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

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

**Note:** If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.
Procedure 4: Recovery Scenario 4

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

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

Select the active NOAM server and click on the Report button at the bottom of the page. The following screen is displayed:

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

---

### NOAM Database Status Report
---

Report Generated: Tue Oct 09 15:13:39 2018 UTC
From: Active Network (NOAM) on Host blade07
Report Version: 3.0.13-1.0.0:10.13.0
User: quxIain

---

**General**
- Hostname: blade07
- Application Database Version: 3.0.13-1.0.0:10.13.0

**Capacities and Utilization**
- Disk Utilization: 0.6% - 248M used of 416G total, 388G available
- Memory Utilization: 0.6% - 136M used of 2397M total, 2261M available

**Alarms**
- None
- Maintenance in Progress
- Restore operation success

**Service Information**
- Part: A,AppendTable

<table>
<thead>
<tr>
<th>Table Name</th>
<th>Row Size</th>
<th>Avg</th>
<th>Max</th>
<th>Rows</th>
<th>Used</th>
<th>Alloc</th>
<th>Used</th>
<th>Alloc</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoFlush</td>
<td>44</td>
<td>1</td>
<td>44</td>
<td>44</td>
<td>44</td>
<td>B</td>
<td>44</td>
<td>B</td>
</tr>
<tr>
<td>CoGdStats</td>
<td>52</td>
<td>0</td>
<td>52</td>
<td>52</td>
<td>52</td>
<td>B</td>
<td>52</td>
<td>B</td>
</tr>
<tr>
<td>CoGdInfo</td>
<td>64</td>
<td>0</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>B</td>
<td>64</td>
<td>B</td>
</tr>
<tr>
<td>CoGdAlign</td>
<td>36</td>
<td>0</td>
<td>36</td>
<td>36</td>
<td>36</td>
<td>B</td>
<td>36</td>
<td>B</td>
</tr>
<tr>
<td>CountryCode</td>
<td>24</td>
<td>206</td>
<td>734</td>
<td>734</td>
<td>734</td>
<td>B</td>
<td>734</td>
<td>B</td>
</tr>
<tr>
<td>CountryId</td>
<td>67</td>
<td>104</td>
<td>104</td>
<td>104</td>
<td>104</td>
<td>B</td>
<td>104</td>
<td>B</td>
</tr>
<tr>
<td>NcoDec</td>
<td>60</td>
<td>0</td>
<td>60</td>
<td>60</td>
<td>60</td>
<td>B</td>
<td>60</td>
<td>B</td>
</tr>
<tr>
<td>NcoGdAlign</td>
<td>52</td>
<td>0</td>
<td>52</td>
<td>52</td>
<td>52</td>
<td>B</td>
<td>52</td>
<td>B</td>
</tr>
<tr>
<td>NcoErr</td>
<td>60</td>
<td>0</td>
<td>60</td>
<td>60</td>
<td>60</td>
<td>B</td>
<td>60</td>
<td>B</td>
</tr>
<tr>
<td>NcoRdOp</td>
<td>75</td>
<td>0</td>
<td>75</td>
<td>75</td>
<td>75</td>
<td>B</td>
<td>75</td>
<td>B</td>
</tr>
</tbody>
</table>

---

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

#### 21. **ACTIVE NOAM:**
**Verify Replication Between Servers.**

Login to the Active NOAM via SSH terminal as `admusr` user. Execute the following command:

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

Output like below shall be generated:

```
-- 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
```

#### 22. **NOAM VIP GUI:**
**Verify the Database states**

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

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

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

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

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

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

   ![Main Menu: Status & Manage -> HA]

24. **SOAM VIP GUI:** Verify the Local Node Info

   **Navigate to Main Menu->Diameter->Configuration->Local Node**

   ![Diameter]
   - Configuration
     - Capacity Summary
     - Connection Capacity Dashboard
     - Application Ids
     - CBX Parameters
     - Command Codes
   - Configuration Sets
     - Local Nodes
     - Peer Nodes
     - Peer Node Groups
     - Connections
     - Route Groups
     - Route Lists
     - Peer Route Tables
     - Egress Throttle Groups
     - Re-route On Answer
     - Application Route Tables
     - Routing Option Sets
     - Pending Answer Timers
     - Traffic Throttle Points
     - Traffic Throttle Groups
     - RTP Removal Lists
     - System Options
     - DNS Options
   - Peer Discovery

   Verify that all the local nodes are shown.
### 25. SOAM VIP GUI: Verify the Peer Node Info

Navigate to **Main Menu->Diameter->Configuration->Peer Node**

Verify that all the peer nodes are shown.

### 26. SOAM VIP GUI: Verify the Connections Info

Navigate to **Main Menu->Diameter->Configuration->Connections**

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

#### 27. For vSTP Only

**SOAM VIP Server Console (Optional): Verify the local nodes info**

To verify the vSTP MP **Local nodes** info:

1. Login to the SOAM VIP Server console as **admusr**
2. Execute the following command
   
   ```bash
   [admusr@SOAM1 ~]$ mmiclient.py /vstp/localhosts
   ```
3. Verify the output similar to the below output
   ```json
   {
   "data": [
   {
   "configurationLevel": "10",
   "localHostName": "AUTLocalHost1",
   "localHostPort": 4444,
   "localHostPriIPAddress": "145.168.100.2",
   "localHostSecIPAddress": "145.168.111.1"
   },
   {
   "configurationLevel": "11",
   "localHostName": "AUTLocalHost2",
   "localHostPort": 4445,
   "localHostPriIPAddress": "145.168.100.2",
   "localHostSecIPAddress": "145.168.111.1"
   }
   ],
   "links": {},
   "messages": [],
   "status": true
   }
   ```

#### 28. For vSTP Only

**SOAM VIP Server Console (Optional): Verify the remote nodes info**

To verify the vSTP MP **Remote nodes** info:

1. Login to the SOAM VIP Server console as **admusr**
2. Execute the following command
   
   ```bash
   [admusr@SOAM1 ~]$ mmiclient.py /vstp/remotehosts
   ```
3. Verify the output similar to the below output
   ```json
   {
   "data": [
   {
   "configurationLevel": "12",
   "remoteHostName": "AUTRemoteHost1",
   "remoteHostPort": 4444,
   "remoteHostPriIPAddress": "1.1.1.6",
   "remoteHostSecIPAddress": "1.1.1.7"
   }
   ],
   "links": {},
   "messages": [],
   "status": true
   }
   ```
### Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
</table>
| 29. | **For vSTP Only- SOAM VIP Server Console (Optional): Verify the Connections info** | To verify the vSTP MP Connections info:  
1. Login to 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 the below output  
   ```json
   {
   "data": [
   {
   "configurationLevel": "13",
   "connCnfSetName": "Default",
   "connectionMode": "Server",
   "connectionType": "M3ua",
   "localHostName": "AUTLocalHost1",
   "name": "AUTLinkTextConn1",
   "remoteHostName": "AUTRemoteHost1"
   },
   {
   "configurationLevel": "14",
   "connCnfSetName": "Default",
   "connectionMode": "Server",
   "connectionType": "M2pa",
   "localHostName": "AUTLocalHost2",
   "name": "AUTLinkTextConn2",
   "remoteHostName": "AUTRemoteHost1"
   }
   ],
   "links": {},
   "messages": [],
   "status": true
   }
   ``` |
| 30. | **MP Servers: Disable SCTP Auth Flag** | For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [1].  
Execute this procedure on all Failed MP Servers. |
Procedure 4: Recovery Scenario 4

31. **SOAM VIP GUI:** Enable Connections if needed

   Navigate to **Main Menu->Diameter->Maintenance->Connections**
   
   Select each connection and click on the **Enable** button.
   
   Alternatively you can enable all the connections by selecting the **EnableAll** button.
   
   Verify that the Operational State is Available.

32. **SOAM VIP GUI:** Enable Optional Features

   Navigate to **Main Menu -> Diameter -> Maintenance -> Applications**
   
   Select the optional feature application
   
   Click the **Enable** button.
### Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>33.</td>
<td><strong>SOAM VIP GUI:</strong> Re-enable Transports if Needed</td>
<td>Navigate to Main Menu-&gt;Transport Manager -&gt; Maintenance -&gt; Transport &lt;br&gt; Select each transport and click on the <strong>Enable</strong> button. &lt;br&gt; Verify that the Operational Status for each transport is Up.</td>
</tr>
<tr>
<td>34.</td>
<td><strong>SOAM VIP GUI:</strong> Re-enable MAPIWF application if needed</td>
<td>Navigate to Main Menu-&gt;SS7/Sigtran-&gt;Maintenance-&gt;Local SCCP Users &lt;br&gt; Click on the <strong>Enable</strong> button corresponding to MAPIWF Application Name. &lt;br&gt; Verify that the SSN Status is Enabled.</td>
</tr>
</tbody>
</table>
### Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
</table>
| 35.  | **SOAM VIP GUI:** Re-enable links if needed | Navigate to **Main Menu-＞SS7/Sigtran-＞Maintenance-＞Links**  
- Click on **Enable** button for each link.  
- Verify that the Operational Status for each link is Up. |
| 36.  | **SOAM VIP GUI:** Examine All Alarms | Navigate to **Main Menu-＞Alarms & Events-＞View Active**  
- Examine all active alarms and refer to the on-line help on how to address them.  
- If needed contact Appendix G. My Oracle Support (MOS). |
| 37.  | **NOAM VIP GUI:** Examine All Alarms | Login to the NOAM VIP if not already logged in.  
- Navigate to **Main Menu-＞Alarms & Events-＞View Active**  
- Examine all active alarms and refer to the on-line help on how to address them.  
- If needed contact Appendix G. My Oracle Support (MOS). |
## Procedure 4: Recovery Scenario 4

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Note: If alarm “10012: The responder for a monitored table failed to respond to a table change” is raised, the oampAgent needs to be restarted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>38.</td>
<td><strong>Restart oampAgent if Needed</strong></td>
<td>Establish an SSH session to each server that has the alarm. Login as <em>admusr</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Execute the following commands:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ sudo pm.set off oampAgent</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ sudo pm.set on oampAgent</code></td>
</tr>
<tr>
<td>39.</td>
<td><strong>Backup and Archive All the Databases from the Recovered System</strong></td>
<td>Execute <strong>Appendix A. DSR Database Backup</strong> to back up the Configuration databases:</td>
</tr>
</tbody>
</table>
5.1.5 Recovery Scenario 5 (Partial Server Outage with all NOAM servers failed with DR-NOAM available)

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

Switch DR NOAM from secondary to primary

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

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

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Workarounds</td>
<td>Refer to Appendix F. Workarounds for Issues not fixed in this Release to understand any workarounds required during this procedure.</td>
</tr>
<tr>
<td>2</td>
<td>Gather Required Materials</td>
<td>Gather the documents and required materials listed in Section 3.1 Required Materials</td>
</tr>
<tr>
<td>3</td>
<td>Switch DR NOAM to Primary</td>
<td>Refer to DSR / SDS 8.x NOAM Failover User's Guide [2]</td>
</tr>
</tbody>
</table>
Procedure 5: Recovery Scenario 5

<table>
<thead>
<tr>
<th></th>
<th>Recover the Failed Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td></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 \[\textbf{Note}:\text{ If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA}\]
   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 \[\textbf{Note}:\text{ If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA}\]
   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 \[\textbf{Note}:\text{ If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA}\]
   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" \[\textbf{Note}:\text{ If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA}\]
   b. Procedure 5 (KVM/Openstack). "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" \[\textbf{Note}:\text{ If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA}\]
   b. Procedure 6 (KVM/Openstack). "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" \[\textbf{Note}:\text{ If OVA is already imported and present in the Infrastructure Manager, skip this procedure of importing OVA}\]
   b. Procedure 6 (KVM/Openstack). "Configure Remaining DSR guests based on resource profile"

For OVM-S/OVM-M based deployments:

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
   \[\textbf{Note}:\text{ While executing Procedure 8, configure the required failed VMs only (NOAMs/SOAMs/MPs)}\]
### Procedure 5: Recovery Scenario 5

<table>
<thead>
<tr>
<th></th>
<th>Recover Failed SOAMs</th>
<th>DR-NOAM VIP GUI: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>If ALL SOAM servers have failed, execute Procedure 2</td>
<td>Establish a GUI session on the DR-NOAM server by using the VIP IP address of the DR-NOAM server. Open the web browser and enter a URL of:</td>
</tr>
</tbody>
</table>

http://<Primary_DR-NOAM_VIP_IP_Address>

Login as the *guiadmin* user:

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

<table>
<thead>
<tr>
<th>Step</th>
<th>DR-NOAM VIP GUI:</th>
<th>Navigate to Main Menu -&gt; Status &amp; Manage -&gt; HA</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Set Failed NOAM Servers to Standby</td>
<td>Navigate to Main Menu -&gt; Status &amp; Manage -&gt; HA</td>
</tr>
<tr>
<td></td>
<td>GUI:</td>
<td>Status &amp; Manage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network Elements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Database</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KPIs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Files</td>
</tr>
<tr>
<td></td>
<td>Select Edit</td>
<td>Set the Max Allowed HA Role drop down box to <em>Standby</em> for the failed NOAM servers.</td>
</tr>
<tr>
<td></td>
<td>Select Ok</td>
<td>Select Ok</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>DR-NOAM VIP GUI:</th>
<th>Export the Initial Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>GUI: Copy the Initial Configuration File to Failed NOAM Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Navigate to Main Menu -&gt; Configuration -&gt; Servers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>From the GUI screen, select the Failed NOAM server and then select Export to generate the initial configuration data for that server.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>DR-NOAM VIP GUI:</th>
<th>Copy Configuration File to Failed NOAM Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Obtain a terminal session to the DR-NOAM VIP, login as the <em>admusr</em> user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Execute the following command to configure the failed NOAM server:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.&lt;Failed_NOAM_Hostname&gt;.sh admusr@&lt;Failed_NOAM_xmi_IP_address&gt;:/var/tmp/TKLCConfigData.sh</code></td>
<td></td>
</tr>
</tbody>
</table>
### Procedure 5: Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 10   | **Recovered NOAM Server:**  
Verify configuration was called and Reboot the Server  
Establish an SSH session to the Recovered NOAM server  
(Recovered_NOAM_xmi_IP_address)  
Login as the `admusr` user.  
The automatic configuration daemon will look for the file named  
“TKLCCfgData.sh” in the /var/tmp directory, implement the configuration in  
the file, and then prompt the user to reboot the server.  
Verify `awpushcfg` was called by checking the following file  

```
$ sudo cat /var/TKLC/appw/logs/Process/install.log
```

Verify the following message is displayed:  

```
[SUCCESS] script completed successfully!
```

Now Reboot the Server:  

```
$ sudo init 6
```

Wait for the server to reboot  

| 11   | **Recovered NOAM Server:**  
Verify Server Health  
Execute the following command on the failed NOAM server and make sure that  
no errors are returned:  

```
$ sudo syscheck
```

Running modules in class hardware...OK  
Running modules in class disk...OK  
Running modules in class net...OK  
Running modules in class system...OK  
Running modules in class proc...OK  
LOG LOCATION: /var/TKLC/log/syscheck/fail_log  

| 12   | **Repeat for Additional 2nd Failed NOAM**  
Repeat steps 8-11 for the 2nd failed NOAM server. |
### Procedure 5: Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td><strong>Perform Key exchange between Active NOAM and Recovered NOAMs</strong>&lt;br&gt;Perform a key exchange between the newly active NOAM and the recovered NOAM servers:&lt;br&gt;From a terminal window connection on the active NOAM as the <code>admusr</code> user, exchange SSH keys for <code>admusr</code> between the active NOAM and the recovered NOAM servers using the key exchange utility, using the host names of the recovered NOAMs.&lt;br&gt;When prompted for the password, enter the password for the <code>admusr</code> user of the recovered NOAM servers.</td>
</tr>
<tr>
<td>14</td>
<td><strong>NOAM VIP GUI: Set HA on Recovered NOAMs</strong>&lt;br&gt;Navigate to <strong>Status &amp; Manage -&gt; HA</strong>&lt;br&gt;Click on <strong>Edit</strong> at the bottom of the screen&lt;br&gt;For each NOAM server whose Max Allowed HA Role is set to <strong>Standby</strong>, set it to <strong>Active</strong>&lt;br&gt;Press <strong>OK</strong></td>
</tr>
<tr>
<td>15</td>
<td><strong>NOAM VIP GUI: Restart DSR application</strong>&lt;br&gt;Navigate to <strong>Main Menu-&gt;Status &amp; Manage-&gt;Server</strong>&lt;br&gt;Select each recovered NOAM server and click on <strong>Restart</strong>.</td>
</tr>
</tbody>
</table>

```bash
$ keyexchange admusr@<Recovered_NOAM Hostname>
```
### Procedure 5: Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 16   | **Recovered NOAM servers:**
|      | Activate Optional Features |
|      | **Map-Diameter Interworking (MAP-IWF) and/or Policy and Charging Application (PCA) Only** |
|      | Activate the features Map-Diameter Interworking (MAP-IWF) and Policy and Charging Application (PCA) as follows: |
|      | **For PCA:** |
|      | 1. Establish SSH sessions to the all the recovered NOAM servers and login as admusr. Refer [3] and execute procedure “PCA Activation on Standby NOAM server” on all recovered NOAM Servers to re-activate PCA. |
|      | Establish SSH session to the recovered active NOAM, login as admusr. For **MAP-IWF:** |
|      | 1. Establish SSH session to the recovered active NOAM, login as admusr. Refer [4] to activate Map-Diameter Interworking (MAP-IWF) |
|      | **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. |
| 17   | **Switch DR NOAM Back to Secondary** |
|      | Once the system have been recovered: |
|      | Refer to DSR / SDS 8.x NOAM Failover User’s Guide [2] |
### Procedure 5: Recovery Scenario 5

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 18   | **NOAM VIP GUI:** Perform Keyexchange with Export Server  
     | Navigate to Main Menu -> Administration -> Remote Servers -> Data Export  
     | Click on **Key Exchange** at the bottom of the screen  
     | Enter the Password and press **OK** |
| 19   | **Recovered Servers:** Verify Alarms  
     | Navigate to Main Menu -> Alarms & Events -> View Active  
     | Verify the recovered servers are not contributing to any active alarms  
     | (Replication, Topology misconfiguration, database impairments, NTP, etc.) |
| 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 as well as any C-Level servers. |

### 5.1.6 Recovery Scenario 6 (Database Recovery)

#### 5.1.6.1 Recovery Scenario 6: Case 1

For a partial outage with:

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

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

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

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Workarounds</th>
<th>NOAM VIP GUI: Set Failed Servers to OOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Refer to Appendix F. Workarounds for Issues not fixed in this Release to understand/apply any workarounds required during this procedure.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Navigate to Main Menu -&gt; Status &amp; Manage -&gt; HA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the Max Allowed HA Role drop down box to OOS for the failed servers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select Ok</td>
<td></td>
</tr>
</tbody>
</table>

| 3.     | Establish an SSH session to the server in question. Login as admusr user. |
| 4.     | Execute the following command to bring the system to runlevel 3. |

```bash
$ sudo init 3
```
## Procedure 6: Recovery Scenario 6 (Case 1)

<table>
<thead>
<tr>
<th>5.</th>
<th><strong>Server in Question:</strong> Recover System</th>
<th>Execute the following command and follow the instructions appearing the console prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><code>$ sudo /usr/TKLC/appworks/sbin/backout_restore</code></td>
</tr>
<tr>
<td>6.</td>
<td><strong>Server in Question:</strong> Change runlevel to 4</td>
<td>Execute the following command to bring the system back to runlevel 4.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ sudo init 6</code></td>
</tr>
<tr>
<td>7.</td>
<td><strong>Server in Question:</strong> Verify the server</td>
<td>Execute the following command to verify if the processes are up and running</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$ sudo pm.getprocs</code></td>
</tr>
<tr>
<td>8.</td>
<td><strong>NOAM VIP GUI:</strong> Set Failed Servers to Active</td>
<td>Navigate to Status &amp; Manage -&gt; HA</td>
</tr>
</tbody>
</table>
|    |                                        | ![Status & Manage menu with submenus](image)
|    |                                        | Click on **Edit** at the bottom of the screen  |
|    |                                        | For each failed server whose Max Allowed HA Role is set to OOS, set it to **Active**  |
|    |                                        | Press **OK**                                                                    |
| 9. | **Backup and Archive All the Databases from the Recovered System** | Execute **Appendix A. DSR Database Backup** to back up the Configuration databases: |

### 5.1.6.2 Recovery Scenario 6: Case 2

For a partial outage with

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

**Procedure 6: Recovery Scenario 6 (Case 2)**
**Procedure 6: Recovery Scenario 6 (Case 2)**

**Step #** | Description |
--- | --- |
1. | **Workarounds** |
2. | **NOAM VIP GUI:** Set Failed Servers to OOS |
3. | **Server in Question:** Login |
4. | **Server in Question:** Take Server out of Service |
5. | **Server in Question:** Take Server to DbUp State and Start the Application |

This procedure performs recovery if database got corrupted in the system and system is in the state to get replicated.

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

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

1. **Workarounds**
   - Refer to Appendix F. Workarounds for Issues not fixed in this Release to understand/apply any workarounds required during this procedure.

2. **NOAM VIP GUI:** Set Failed Servers to OOS
   - Navigate to **Main Menu -> Status & Manage -> HA**
   - Select **Edit**
   - Set the Max Allowed HA Role drop down box to **OOS** for the failed servers.
   - Select **Ok**

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

4. **Server in Question:** Take Server out of Service
   - Execute the following command to take the server out of service:
   ```bash
   $ sudo bash -l
   $ sudo prod.clobber
   ```

5. **Server in Question:** Take Server to DbUp State and Start the Application
   - Execute the following commands to take the server to Dbup and start the DSR application:
   ```bash
   $ sudo bash -l
   $ sudo prod.start
   ```
### Procedure 6: Recovery Scenario 6 (Case 2)

#### 6. Server in Question: Verify the Server State

*Execute the following commands to verify the processes are up and running:*

```bash
$ sudo pm.getprocs
```

*Execute the following command to verify if replication channels are up and running:*

```bash
$ sudo irepstat
```

*Execute the following command to verify if merging channels are up and running:*

```bash
$ sudo inetmstat
```

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

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

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

#### 8. NOAM VIP GUI: Set Failed Servers to Active

*Navigate to Status & Manage -> HA*

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

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

Press **OK**
Procedure 6: Recovery Scenario 6 (Case 2)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Backup and Archive All the Databases from the Recovered System</td>
<td>Execute Appendix A. DSR Database Backup to back up the Configuration databases:</td>
</tr>
</tbody>
</table>
6.0 Resolving User Credential Issues after Database Restore

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

6.1 Restoring a Deleted User

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

These users were removed prior to creation of the backup and archive file. They will be reintroduced by system restoration of that file.
### 6.2 Keeping a Restored user

**Procedure 7: Keep Restored User**

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

<table>
<thead>
<tr>
<th><strong>STEP #</strong></th>
<th><strong>After Restoration:</strong> Login to the NOAM VIP</th>
</tr>
</thead>
</table>
| 2.         | Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  

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

Login as the *guiadmin* user:

---

**Oracle System Login**

Enter your username and password to log in

- **Username:** guiadmin
- **Password:** ********

- [ ] Change password

[Log In]

Welcome to the Oracle System Login.

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 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.
Procedure 7: Keep Restored User

<table>
<thead>
<tr>
<th>3.</th>
<th>After Restoration: Reset User Passwords</th>
</tr>
</thead>
</table>

3. After Restoration:

1. Reset User Passwords

   Navigate to Administration -> Access Control -> Users

   - Administration
   - General Options
   - Access Control
     - Users
   - Groups

   Select the user

   Click the Change Password button

   Enter a new password

   Enter the new password for **guiadmin** two times:
   - New Password: [enter password]
   - Retype New Password: [re-enter password]

   - Force password change on next login

   Click the Continue button
## 6.3 Removing a Restored User

### Procedure 8: Remove the Restored User

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Perform this procedure to remove users that will be restored by system restoration. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix G. My Oracle Support (MOS), and ask for assistance.</td>
</tr>
</tbody>
</table>

#### 1. After Restoration: Login to the NOAM VIP

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

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

Login as the `guiadmin` user:

![Oracle System Login](image-url)
### Procedure 8: Remove the Restored User

<table>
<thead>
<tr>
<th>Step</th>
<th>After Restoration: Delete user</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td></td>
<td><strong>Navigate to</strong> Administration -&gt; Access Control -&gt; Users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>![Tree Diagram]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click the <strong>Delete</strong> button</td>
</tr>
<tr>
<td></td>
<td></td>
<td>![Delete Selection Prompt]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click the <strong>OK</strong> button to confirm.</td>
</tr>
</tbody>
</table>
6.4 Restoring a Modified User

These users have had a password change prior to creation of the backup and archive file. The will be reverted by system restoration of that file.

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

Before Restoration:

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

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

After Restoration:

Log in and reset the passwords for all users in this category. See the steps in Appendix G. My Oracle Support (MOS) for resetting passwords for a user.
6.5 Restoring an Archive that does not contain a Current User

These users have been created after the creation of the backup and archive file. The will be deleted by system restoration of that file.

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

If the user is no longer desired, do not perform any additional steps. The user is permanently removed.

Procedure 9: Restoring an Archive that does not Contain a Current User

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Perform this procedure to remove users that will be restored by system restoration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
</tr>
<tr>
<td></td>
<td>If this procedure fails, contact Appendix G. My Oracle Support (MOS), and ask for assistance.</td>
</tr>
</tbody>
</table>

1. Before Restoration: Notify Affected Users Before Restoration
   - Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.

2. Before Restoration: Login to the NOAM VIP
   - Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:

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

   Login as the **guiadmin** user:
Procedure 9: Restoring an Archive that does not Contain a Current User

3. Before Restoration: Record user settings

   Navigate to Administration -> Access Control -> Users

   Under each affected user, record the following:
   - Username,
   - Account status
   - Remote Auth
   - Local Auth
   - Concurrent Logins Allowed
   - Inactivity Limit
   - Comment
   - Groups

4. After Restoration: Login

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

   [http://<Primary_NOAM_VIP_IP_Address>]

   Login as the guiadmin user:

   [Oracle System Login]
   [Log In]
   [Username: guiadmin]
   [Password: ********]
   [Change password]
   [Log In]

   Welcome to the Oracle System Login.

   Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 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.
### Procedure 9: Restoring an Archive that does not Contain a Current User

<table>
<thead>
<tr>
<th>Step</th>
<th>After Restoration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td></td>
<td><strong>Restoring an Archive that does not Contain a Current User</strong></td>
</tr>
<tr>
<td></td>
<td><strong>After Restoration:</strong> Recreate affected user and required group</td>
<td>Navigate to <strong>Administration -&gt; Access Control -&gt; Users</strong>. Click <strong>Insert</strong>. Recreate the user using the data collected in <strong>Step 4</strong>. Click <strong>Ok</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Repeat <strong>Step 5</strong> to recreate additional users and groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>After Restoration:</strong> Reset the Passwords</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See 6.2 Keeping a Restored user for resetting passwords for a user.</td>
</tr>
</tbody>
</table>
## 7.0 IDIH Disaster Recovery

### Procedure 10: IDIH Disaster Recovery Preparation

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This procedure performs disaster recovery preparation steps for the IDIH. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix G. My Oracle Support (MOS), and ask for assistance.</td>
</tr>
<tr>
<td>1.</td>
<td><strong>Oracle Guest:</strong> Login</td>
</tr>
</tbody>
</table>


**Procedure 10: IDIH Disaster Recovery Preparation**

1. **Oracle Guest:**
   - Perform Database Health check

   Execute the following command to perform a database health check:
   
   ```sh
   $ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i
   ```

   Output:

   ![Database Health Check Output]

   **NOTE:** If this step fails, a re-installation is necessary by following procedure from reference [1]:
   - For VMware based deployments:
     - Section 4.9 (Procedure 28) : Create iDIH Virtual Machines (VMware)
     - Section 4.12 (Procedure 31 – 34) : Configure iDIH Virtual Machines
   - For KVM/Openstack based deployments:
     - Section 4.10 (Procedure 29) : Create iDIH Virtual Machines (KVM/Openstack)
     - Section 4.12 (Procedure 31 – 34) : Configure iDIH Virtual Machines
   - For OVM-S/OVM-M based deployments:
     - Section 4.11 (Procedure 30) : (OVM-S/OVM-M). Import three IDIH OVA’s and create and configure a VM for each
     - Section 4.12 (Procedure 31 – 34) : Configure iDIH Virtual Machines
Procedure 11: IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

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

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

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

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| 1.     | Create iDIH Application & Mediation VMs | Execute the following procedure from [1] to recover the Application and Mediation VMs:  
- For VMWare based deployments:  
  Procedure 28 *(VMware only) Create iDIH Oracle, Mediation and Application VMs*  
- For KVM / Openstack based deployments:  
  Procedure 29. *(KVM/OpenStack only) Create iDIH Oracle, Mediation and Application VMs (Optional)*  
- For OVM-S / OVM-M based deployments:  
  Procedure 30. *(OVM-S/OVM-M). Import three IDIH OVA’s and create and configure a VM for each* |
| 2.     | Configure iDIH VM Networks | Execute the following procedure from [1] to configure the VM networks on the Application and Mediation VMs only:  
  Procedure 31 “Configure iDIH VM Networks” |
| 3.     | Configure VMs | Execute the following procedure from [1]:  
  Procedure 32 “Run Post Installation scripts on iDIH VMs”, steps 3 - 7 |
| 4.     | Integrate into DSR (Optional) | If integration is needed execute the following procedure from [1]:  
  Procedure 35. Integrate iDIH into DSR |
## Appendix A. DSR Database Backup

### Procedure 12: Back up the provision and configuration data

<table>
<thead>
<tr>
<th><strong>STEP #</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong> NOAM/SOAM VIP: Login</td>
<td>Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server.</td>
</tr>
</tbody>
</table>

Open the web browser and enter a URL of:

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

Login as the `guiadmin` user:

![Oracle System Login](image)

Welcome to the Oracle System Login.

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 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.
### Procedure 12: Back up the provision and configuration data

<table>
<thead>
<tr>
<th>NOAM/SOAM VIP: Backup Configuration Data for the System</th>
<th>Navigate to Main Menu -&gt; Status &amp; Manage -&gt; Database</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>![Main Menu Screenshot]</td>
</tr>
<tr>
<td></td>
<td>Select the Active NOAM Server and Click on <strong>Backup</strong> button</td>
</tr>
</tbody>
</table>

**Select the Active NOAM Server and Click on **Backup** button**

Make sure that the checkboxes next to “Configuration” is checked.

**Database Backup**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server: Hartenque ASI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select data for backup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compression</td>
<td>0: none</td>
<td>Selected the backup archive compression algorithm. The following file suffix will be applied for the selected option:</td>
</tr>
<tr>
<td>ArchName</td>
<td>Backup_Hartenque_ASI_Configuration</td>
<td>Modify archiving name if desired. Do not include the compression type suffix (A value is required)</td>
</tr>
<tr>
<td>Comment</td>
<td></td>
<td>May not contain the following characters: <strong>“/ $</strong></td>
</tr>
</tbody>
</table>

**Enter a filename for the backup and press **OK**
## Procedure 12: Back up the provision and configuration data

### 3. NOAM/NOAM VIP: Verify the backup file existence.

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

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Type</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIW016013955_20150418.au.t</td>
<td>11.4M</td>
<td>LG</td>
<td>2015-04-18 18:42:48</td>
</tr>
<tr>
<td>VIW016013955_20150418.au.t</td>
<td>11.4M</td>
<td>LG</td>
<td>2015-04-18 18:42:48</td>
</tr>
<tr>
<td>VIW016013955_20150418.au.t</td>
<td>11.4M</td>
<td>LG</td>
<td>2015-04-18 18:42:48</td>
</tr>
</tbody>
</table>

Select the Active NOAM or SOAM tab.

The files on this server will be displayed. Verify the existence of the backup file.

### 4. NOAM/NOAM VIP: Download the file to a local machine.

From the previous step, choose the backup file.

Select the **Download** button

Select OK to confirm the download.

### 5. Upload the Image to Secure Location

Transfer the backed up image saved in the previous step to a secure location where the Server Backup files are fetched in case of system disaster recovery.
Procedure 12: Back up the provision and configuration data

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td><strong>Backup Active SOAM</strong></td>
</tr>
<tr>
<td></td>
<td>Repeat <strong>Steps 2 through 5</strong> to back up the Active SOAM</td>
</tr>
</tbody>
</table>
Appendix B. Inhibit A and B Level Replication on C-Level Servers

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

The intent of this procedure is to inhibit A and B level replication on all C Level servers of this site. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

1. **Active NOAM:** Login
   - Login to the Active NOAM server via SSH as **admusr** user.

2. **Active NOAM:** Inhibit replication on all C level Servers
   - Execute the following command:
     ```bash
     $ for i in $(iqt -p -z -h -fhostName NodeInfo where "nodeName='$i'"; done
     
     Note: NE name of the site can be found out by logging into the Active NOAM GUI and going to **Configuration->Server Groups** screen.

     Please see the snapshot below for more details.
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 site e.g. Site SO_HPC03 shall be set as ‘A B’:

Perform the following command:

```
$ sudo iqt NodeInfo
```

Expected output:

<table>
<thead>
<tr>
<th>nodeId</th>
<th>nodeName</th>
<th>hostName</th>
<th>nodeCapability</th>
<th>InhibitRepPlans</th>
<th>siteId</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1386.099</td>
<td>NO1</td>
<td>NO1</td>
<td>Active</td>
<td></td>
<td>NO_HPC03</td>
</tr>
<tr>
<td>B1754.109</td>
<td>SO1</td>
<td>SO1</td>
<td>Active</td>
<td></td>
<td>SO_HPC03</td>
</tr>
<tr>
<td>C2254.131</td>
<td>MP2</td>
<td>MP2</td>
<td>Active</td>
<td>A B</td>
<td>SO_HPC03</td>
</tr>
<tr>
<td>C2254.233</td>
<td>MP1</td>
<td>MP1</td>
<td>Active</td>
<td>A B</td>
<td>SO_HPC03</td>
</tr>
</tbody>
</table>
## Appendix C. Un-Inhibit A and B Level Replication on C-Level Servers

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

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Active NOAM:</strong> Login to the Active NOAM server via SSH as <code>admusr</code> user.</td>
</tr>
</tbody>
</table>
| 2.     | **Active NOAM:** Un-Inhibit replication on all C Level Servers. Execute the following command:  

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

**Note:** NE name of the site can be found out by logging into the Active NOAM GUI and going to Configuration->Server Groups screen.

Please see the snapshot below for more details.

![Snapshot of NOAM Configuration -> Server Groups](image)

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

The intent of this procedure is to inhibit A and B level replication on all C Level servers of this site when Active, Standby and Spare SOAMS are lost.

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

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

3.  
Active NOAM: Login

Login to the Active NOAM server via SSH as admuser user.

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Active NOAM: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Login</td>
</tr>
</tbody>
</table>
Procedure 13: Inhibit A and B Level Replication on C-Level Servers

4.  

**Active NOAM:**
Inhibit replication on all C level Servers

Execute the following command:

```bash
$ for i in $(sudo Imysql.client -B -N -e "
SELECT DISTINCT CS.hostname
FROM appworks.Server CS, appworks.Server PS,
appworks.Server2SG C2SG, appworks.Server2SG P2SG,
appworks.ServerGroup CSG, appworks.ServerGroup PSG,
comcol.ClusterInfo CCI, comcol.ClusterInfo PCI,
comcol.ClusterGroupInfo
WHERE CS._h_Server_ID = C2SG._h_Server_ID
AND C2SG._h_SG_ID = CSG._h_SG_ID
AND CSG.clusterId = CCI.clusterId
AND CCI.groups = comcol.ClusterGroupInfo.groupId
AND comcol.ClusterGroupInfo.parentGroup = PCI.groups
AND PCI.clusterId = PSG.clusterId
AND PSG.ServerGroupName='"<SOAM_SG_NAME>"");
do iset -finhibitRepPlans='A B' NodeInfo where
"nodeName='$i'"; done
```

**Note:** SOAM_SG_NAME name of the Server Group can be found out by logging into the Active NOAM GUI and going to **Configuration->Server Groups** screen.

Please see the snapshot below for more details.
Procedure 13: Inhibit A and B Level Replication on C-Level Servers

<table>
<thead>
<tr>
<th>3</th>
<th>Active NOAM:</th>
<th>Verify Replication has been Inhibited.</th>
</tr>
</thead>
</table>

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 e.g. Server group SO_SG shall be set as 'A B'.

Perform the following command:

```
$ sudo iqt NodeInfo
```

**Expected output:**

<table>
<thead>
<tr>
<th>nodeId</th>
<th>nodeName</th>
<th>hostName</th>
<th>nodeCap</th>
<th>inhibitRepPlans</th>
<th>siteId</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1386.099</td>
<td>NO1</td>
<td>NO1</td>
<td>Active</td>
<td></td>
<td>NO_HPC03</td>
</tr>
<tr>
<td>B1754.109</td>
<td>SO1</td>
<td>SO1</td>
<td>Active</td>
<td>A B</td>
<td>SO_HPC03</td>
</tr>
<tr>
<td>C2254.131</td>
<td>MP2</td>
<td>MP2</td>
<td>Active</td>
<td>A B</td>
<td>SO_HPC03</td>
</tr>
<tr>
<td>C2254.233</td>
<td>MP1</td>
<td>MP1</td>
<td>Active</td>
<td>A B</td>
<td>SO_HPC03</td>
</tr>
</tbody>
</table>

Appendix E. 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

**STEPS**

4. Active NOAM: Login

The intent of this procedure is to Un-inhibit A and B level replication on all C Level servers of this site when Active, Standby and Spare SOAMS are lost.

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

If this procedure fails, contact Appendix G. My Oracle Support (MOS), and ask for assistance.
Procedure 14: Un-Inhibit A and B Level Replication on C-Level Servers

5. Active NOAM: Un-Inhibit replication on all C level Servers

Execute the following command:

```
$ for i in $(sudo Imysql.client -B -N -e "
SELECT DISTINCT CS.hostname
 FROM appworks.Server CS, appworks.Server PS,
 appworks.Server2SG C2SG, appworks.Server2SG P2SG,
 appworks.ServerGroup CSG, appworks.ServerGroup PSG,
 comcol.ClusterInfo CCI, comcol.ClusterInfo PCI,
 comcol.ClusterGroupInfo
 WHERE CS._h_Server_ID = C2SG._h_Server_ID
   AND C2SG._h_SG_ID = CSG._h_SG_ID
   AND CSG.clusterId = CCI.clusterId
   AND CCI.groups = comcol.ClusterGroupInfo.groupId
   AND comcol.ClusterGroupInfo.parentGroup = PCI.groups
   AND PCI.clusterId = PSG.clusterId
   AND PSG.ServerGroupName='\<SOA\_SG\_NAME>'
"); do iset -finhibitRepPlans='' NodeInfo where
 "nodeName='$i'"; done
```

Note: **SOA\_SG\_NAME** name of the site can be found out by logging into the Active NOAM GUI and going to Configuration->Server Groups screen.

Please see the snapshot below for more details.
Procedure 14: Un-Inhibit A and B Level Replication on C-Level Servers

Active NOAM:
Verify Replication has been un-Inhibited.

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

Verification of replication un-inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected server group e.g. Server group SO_SG shall be set as ‘’:

Perform the following command:

```
$ sudo iqt NodeInfo
```

Expected output:

```
Expected output:
nodeId   nodeName  hostName  nodeCapability inhibitRepPlans  siteId  excludeTables
A1386.099 NO1        NO1      Active                                        NO_HPC03
B1754.109 SO1        SO1      Active                                        SO_HPC03
C2254.131 MP2        MP2      Active                                        SO_HPC03
C2254.233 MP1        MP1      Active                                        SO_HPC03
```
Appendix F. Workarounds for Issues not fixed in this Release

Appendix G. My Oracle Support (MOS)

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

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