



# **Oracle® Communications Tekelec HLR Router**

## **HP Hardware Disaster Recovery Guide**

**Release 4.1**

**E56459, Revision 2.0**

**April 2016**

**Oracle® Communications HLR Router 4.1 Disaster Recovery Guide for HP Hardware**

Copyright © 2011, 2016 Oracle and/or its affiliates. All rights reserved.

This software or hardware and documentation may provide access to or information on 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. 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.

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

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

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

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

This software or hardware and documentation may provide access to or information on 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. 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.

**CAUTION: Before installing any system, please access My Oracle Support (MOS) and review any Technical Service Bulletins (TSBs) that relate to these procedures.**

My Oracle Support (MOS) 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. See **Appendix F** for more information.

# Table of Contents

- 1.0 INTRODUCTION..... 5**
  - 1.1 Purpose and Scope ..... 5
  - 1.2 References..... 5
  - 1.3 Acronyms and Terminology..... 6
  - 1.4 Assumptions ..... 6
  - 1.5 How to Use This Document..... 6
- 2.0 DISASTER RECOVERY SCENARIOS..... 7**
  - 2.1 Complete Connectivity Loss of Primary NOAM Servers ..... 7
    - 2.1.1 Pre-Condition ..... 7
    - 2.1.2 Recovery Steps ..... 7
    - 2.1.3 Post Condition ..... 9
  - 2.2 Replacement of MP Server..... 10
    - 2.2.1 Pre-Condition ..... 10
    - 2.2.2 Recovery Steps ..... 10
    - 2.2.3 Post Condition ..... 11
  - 2.3 Replacement of a SOAM Server ..... 12
    - 2.3.1 Pre-Condition ..... 12
    - 2.3.2 Recovery Steps ..... 12
    - 2.3.3 Post Condition ..... 13
  - 2.4 Replacement of a Query Server ..... 14
    - 2.4.1 Pre-Condition ..... 14
    - 2.4.2 Recovery Steps ..... 14
    - 2.4.3 Post Condition ..... 15
  - 2.5 Replacement of a NOAM-A Server ..... 16
    - 2.5.1 Pre-Condition ..... 16
    - 2.5.2 Recovery Steps ..... 16
    - 2.5.3 Post Condition ..... 18
  - 2.6 Replacement of a NOAM-B Server ..... 19
    - 2.6.1 Pre-Condition ..... 19
    - 2.6.2 Recovery Steps ..... 19
    - 2.6.3 Post Condition ..... 21
  - 2.7 Replacement of NOAM Server Pair..... 22
    - 2.7.1 Pre-Condition ..... 22
    - 2.7.2 Recovery Steps ..... 22
    - 2.7.3 Post Condition ..... 23
  - 2.8 Replacement of SOAM Server Pair ..... 24
    - 2.8.1 Pre-Condition ..... 24
    - 2.8.2 Recovery Steps ..... 24
    - 2.8.3 Post Condition ..... 26
  - 2.9 Replacement of DR NOAM Server Pair ..... 27
    - 2.9.1 Pre-Condition ..... 27
    - 2.9.2 Recovery Steps ..... 27
    - 2.9.3 Post Condition ..... 28
  - 2.10 Replacement of Cisco 4948E-F Aggregation Switch..... 29
    - 2.10.1 Pre-Condition ..... 29
    - 2.10.2 Recovery Steps ..... 29
    - 2.10.3 Post Condition ..... 29
  - 2.11 Replacement of Independent NOAM Frame ..... 30
    - 2.11.1 Pre-Condition ..... 30
    - 2.11.2 Recovery Steps ..... 30
    - 2.11.3 Post Condition ..... 30

2.12 Replacement of Independent SOAM Frame ..... 31

    2.12.1 Pre-Condition ..... 31

    2.12.2 Recovery Steps ..... 31

    2.12.3 Post Condition ..... 31

2.13 Replacement of the Combined NOAM+SOAM Frame ..... 32

    2.13.1 Pre-Condition ..... 32

    2.13.2 Recovery Steps ..... 32

    2.13.3 Post Condition ..... 32

**APPENDIX A. RESTORING SOAM CONFIGURATION DATABASE (SS7/TRANSPORT) FROM THE  
BACKUP FILE..... 33**

**APPENDIX B. CORRECTING SOAM CONFIGURATION DATABASE (SS7/TRANSPORT)..... 36**

**APPENDIX C. RESTORING NOAM PROVISIONING DATABASE (PDB) FROM THE BACKUP FILE..... 38**

**APPENDIX D. DIVERTING SIGNALING TRAFFIC AWAY FROM THE MP SERVER..... 40**

**APPENDIX E. BRINGING SIGNALING TRAFFIC BACK TO THE MP SERVER..... 41**

**APPENDIX F. MY ORACLE SUPPORT (MOS)..... 42**

**List of Tables**

Table 1: Acronyms .....6

## 1.0 INTRODUCTION

### 1.1 Purpose and Scope

This document describes disaster recovery procedures used during disaster scenarios of Oracle's Tekelec HLR Router 4.1 product running on HP DL360 (Gen6) and DL380 (Gen9) hardware.

The disaster scenarios covered in this document are:

1. Connectivity loss to primary NOAM servers and DR NOAM activation.
2. A defective MP server.
3. A defective Query server. *(Note: This configuration is optional)*
4. A defective SOAM server.
5. A defective NOAM server.
6. A defective NOAM-A server.
7. A defective NOAM-B server.
8. A defective NOAM server pair.
9. A defective SOAM server pair.
10. A defective Cisco 4948E switch.
11. Total loss of the independent NOAM frame.
12. Total loss of the independent SOAM frame
13. Total loss of the combined NOAM + SOAM frame.

This document is intended for execution by Customer Service team on the fielded Oracle's Tekelec HLR Router 4.1 systems. It also could be used at Oracle's PV and development teams.

### 1.2 References

External references (*customer facing*):

- [1] HLR Router 4.1 Initial Installation and Configuration Guide, E56461-02
- [2] Eagle STP Commands Manual, 910-5544-001
- [3] Tekelec Platform 7.0.x Configuration Guide, E53486-04
- [4] TPD Initial Product Manufacture, 909-2130-001
- [5] Cabinet Assembly Instructions, 910-6083-001
- [6] Database Management: Backup and System Restoration, UG005196
- [7] HLR Router 4.1 Software Upgrade Procedure, E74583-01
- [8] HP Solutions Firmware Upgrade Pack Release Notes, Release 2.x.x, (Min 2.2.9)
- [9] HP Solutions Firmware Upgrade Pack Upgrade Guide, Release 2.x.x, (Min 2.2.9)

Internal references (*for Oracle personnel only*):

- [10] *Network Interconnect for HP Hardware: Tekelec HLR Router 4.1, E74584-01*

## 1.3 Acronyms and Terminology

**Table 1: Acronyms**

Acronym	Meaning
DR	Disaster Recovery
IMI	Internal Management Interface
ISL	Inter-Switch-Link
NE	Network Element
NOAM	Network Operations, Administration, Maintenance & Provisioning
iLO	HP Integrated Lights-Out
Management Server	HP ProLiant DL 360 or DL380 server used to host PM&C application in a virtual machine, to configure Cisco 4948E switches and to serve other configuration purpose. This server is deployed with a serial card and is connected to both switches.
PM&C	Platform Management & Configuration
PM&C Application	PM&C is an application that provides platform-level management functionality for HP G6 of G9 system, such as the capability to manage and provision platform components of the system so it can host applications.
RMS	Rack Mount Server
SOAM	Systems Operations, Administration & Maintenance
TPD	Tekelec Platform Distribution (Linux OS)
TVOE	Tekelec Virtual Operating Environment
VIP	Virtual IP
VM	Virtual Machine
XMI	External Management Interface

## 1.4 Assumptions

This disaster recovery procedure assumes the following:

- The user conceptually knows and understands HLRR 4.1 topology and network configuration as described in the [10] Network Interconnect for HP Hardware: Tekelec HLR Router 4.1.
- The user has at least an intermediate skill set with command prompt activities on an Open Systems computing environment such as Linux or TPD.

## 1.5 How to Use This Document

When executing this document, understanding the following helps to ensure that the user understands the manual's intent:

- Before beginning a procedure, completely read the instructional text (it appears immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.
- Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS and/or NOTES.

If a procedural STEP fails to execute successfully, please STOP and contact MOS Oracle's Customer Care (See Appendix F) for assistance before attempting to continue.

## 2.0 DISASTER RECOVERY SCENARIOS

### 2.1 Complete Connectivity Loss of Primary NOAM Servers

#### 2.1.1 Pre-Condition

- Primary NOAM GUI is not accessible
- DR NOAM GUI is accessible
- Provisioning clients are disconnected from the Primary NOAM
- PDB database provisioning has stopped

#### 2.1.2 Recovery Steps

To quickly make NOAM GUI accessible and provisioning to continue, DR NOAM servers are activated and made to serve as Primary NOAM servers via following steps:

<p>1. <input type="checkbox"/></p>	<p>Disable the application on DR NOAM servers.</p>	<p>This step ensures that DR NOAM assumes Primary NOAM status in a controlled fashion. Disabling the application inhibits provisioning and can be started after successful validation.</p> <ol style="list-style-type: none"> <li>1. Log in to the DR NOAM GUI via the VIP address as the admin user.</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → Server]</li> <li>3. Select the row that has active DR NOAM server. It will highlight ‘Stop’ button at the bottom.</li> <li>4. Click ‘Stop’ and then click ‘OK’ At this time, HA switch over causes an automatic logout.</li> <li>5. Login to DR NOAM GUI as admin user</li> <li>6. Repeat steps 3 and 4 for the new active DR NOAM server.</li> <li>7. Verify that ‘Proc’ column on both DR NOAM servers shows ‘Man’ indicating that application is manually stopped.</li> </ol>
<p>2. <input type="checkbox"/></p>	<p>SSH to VIP address of the DR NOAM as ‘admusr’ user and make it Primary NOAM</p>	<ol style="list-style-type: none"> <li>1. Login via SSH to VIP IP of DR NOAM server as admusr user.</li> <li>2. Execute this command: <b>sudo top.setPrimary</b> This step makes the DR NOAM to take over as new Primary NOAM</li> <li>3. System generates several replication and collection alarms as replication/collection links to/from former primary NOAM servers becomes inactive.</li> </ol>
<p>3. <input type="checkbox"/></p>	<p>Clear any persistent alarms</p>	<ol style="list-style-type: none"> <li>1. Wait at least 5 minutes for replication to re-sync (“inetmerge” or “inetrep” alarms may remain present).</li> <li>2. If inetmerge or inetrep alarms persist beyond 5 minutes, then on the new primary NOAM server, restart the corresponding processes: <b>sudo pm.kill inetmerge</b> <b>sudo m.kill inetrep</b></li> <li>3. Monitor alarms until they are all cleared</li> </ol>
<p>4. <input type="checkbox"/></p>	<p>Verify replication</p>	<ol style="list-style-type: none"> <li>1. Monitor [Main Menu: Status &amp; Manage → Server] screen at new-Primary NOAM.  <i>Note:</i> It may take several minutes for replication, afterwards the “DB” and “Reporting Status” columns should show ‘Normal’</li> </ol>

<p>5. <input type="checkbox"/></p>	<p>Re-enable the application on the now-Primary NOAM using the Active new-Primary NOAM GUI.</p>	<ol style="list-style-type: none"> <li>2. Login to new-Primary NOAM GUI as admin user</li> <li>3. Navigate to GUI page [Main Menu: Status &amp; Manage → Server]</li> <li>4. Select the active new-Primary NOAM server. This action highlights the ‘Restart’ button at the bottom.</li> <li>5. Click ‘Restart’ and then click ‘OK’</li> <li>6. Verify that ‘PROC’ column now shows ‘Norm’.</li> <li>7. Repeat steps 3 to 5 for standby new-Primary NOAM server.</li> <li>8. PDB provisioning can now resume to the VIP of the new-Primary NOAM.</li> </ol>
<p>6. <input type="checkbox"/></p>	<p>Decrease the durability admin status and then reconfigure and reconnect the customer’s provisioning clients.</p>	<ol style="list-style-type: none"> <li>1. Lower the durability admin status to (NO pair) to exclude the former-primary NOAM servers from the provisioning database durability. If a value other than 1 has been configured for “cm.idb.durableAdminState”, change the value to 1.</li> <li>2. Login to new NOAM GUI as admin user.</li> <li>3. Navigate to GUI page [Main Menu: Administration → General Options]</li> <li>4. Set <b>cm.idb.durableAdminState</b> to 1 (NO pair).</li> <li>5. Click the ‘OK’ button to update.</li> <li>6. Have customer reconfigure provisioning clients to connect to XMI VIP of the newly activated NOAM servers.</li> <li>7. Navigate to GUI page [Main menu: Eagle XG Database → Maintenance → PDBI → Command Log]</li> <li>8. Verify that provisioning from clients have started. Check that new PDB commands have been executed</li> </ol>
<p>At this point, HLRR provisioning is fully functioning. The remaining steps will bring the old Primary NOAM site back into service as the new DR NOAM site.</p>		
<p>7. <input type="checkbox"/></p>	<p>Bring former-Primary NOAM back to service.</p>	<ol style="list-style-type: none"> <li>1. Determine what has happened to former-Primary NOAM site:                      NOAM frame defective _____                      NOAM servers defective _____                      Networking outage _____                      Cisco switch defective _____</li> <li>2. Based on the above disaster recovery scenario, execute procedure from this document to return the former-Primary NOAM servers and its site back to the service</li> </ol>
<p>8. <input type="checkbox"/></p>	<p>Convert former-Primary NOAM servers to new DR NOAM</p>	<ol style="list-style-type: none"> <li>1. Login via SSH to active former-Primary NOAM server as ‘root’ user.</li> <li>2. Execute this command <b>top.setSecondary</b></li> <li>3. This step allows the formerly Primary NOAM to become the DR NOAM.</li> <li>4. Monitor [Main Menu: Status &amp; Manage → Server] screen at new DR NOAM GUI.</li> </ol> <p><i>Note:</i> It may take several minutes for replication, afterward the ‘DB’ and ‘Reporting Status’ columns should show ‘Normal’</p>



<p>9. <input type="checkbox"/></p>	<p>Stop Non-Service processes on DR NOAM</p>	<ol style="list-style-type: none"> <li>1. Navigate to GUI page [Main Menu: Status &amp; Manage → Server] and select the new active DR NOAM server.</li> <li>2. Press the ‘Stop’ button for new active DR NOAM server (stops <i>all</i> processes) then press the ‘OK’ button to confirm.</li> <li>3. On this GUI page [Main Menu: Status &amp; Manage → Server] select new active DR NOAM server.</li> <li>4. Press the ‘Restart’ button for new DR NOAM server (starts <i>only</i> Service processes) then press the ‘OK’ button to confirm.</li> <li>5. Monitor this GUI page [Main Menu: Status &amp; Manage → Server] for new active DR NOAM server on GUI.</li> <li>6. It may take a few seconds, but afterward the Application State should be ‘Enabled’ and the Alarm and Process Status columns should show ‘Normal’</li> <li>7. Repeat steps 1 to 6 for new standby DR NOAM server.</li> </ol>
<p>10. <input type="checkbox"/></p>	<p>Re-exchange SSH keys for PDB Import, PDB Export, PDE, and Data Export (APDE) features</p>	<ol style="list-style-type: none"> <li>1. Login to Primary NOAM GUI as admin user.</li> <li>2. Re-exchange SSH keys for <b>PDB Export</b> using this GUI page [Main Menu: EAGLE XG Database → Configuration → PDBI → Options]</li> <li>3. Re-exchange SSH keys for <b>PDB Import</b> using this GUI page [Main Menu: EAGLE XG Database → Configuration → PDBI → Options]</li> <li>4. Re-exchange SSH keys for <b>PDE</b> using this GUI page [Main Menu: EAGLE XG HLR Router → PDE → Options]</li> <li>5. Re-exchange SSH keys for <b>Data Export (APDE)</b> using this GUI page [Main Menu: Administration → Remote Servers → Data Export]</li> </ol> <p><i>Note:</i> See the Online Help for each GUI to re-exchange keys or contact MOS - My Oracle Support for more assistance (See Appendix F).</p>
<p>11. <input type="checkbox"/></p>	<p>(optional) Clear alarm #14201 on DR-NOAM site</p>	<p>If alarm 14201 was raised before by former Primary NOAM and now is shown on DR-NOAM site, then manually clear this alarm.</p> <ol style="list-style-type: none"> <li>1. SSH to DR-NOAM server where alarm 14201 is still active.</li> <li>2. Execute this command to clear the alarm: <b>alarm.put -e 14201 -s 5 -i PdeAgent</b></li> </ol>

**2.1.3 Post Condition**

- GUI on the new Primary NOAM is accessible
- Provisioning clients are connected to the new Primary NOAM
- Database provisioning resumes
- New DR NOAM GUI is accessible
- Replication and collection alarms have cleared
- NOTE: To swap new Primary NOAM and new DR NOAM back to their original roles, run procedure 2.1.2 over again

## 2.2 Replacement of MP Server

### 2.2.1 Pre-Condition

- MP server has stopped processing traffic
- It has been determined to replace the defective MP server.
- A new replacement for defective MP server is available
- Primary NOAM GUI is accessible.

### 2.2.2 Recovery Steps

1. <input type="checkbox"/>	Prepare for server replacement.	Identify the defective MP server that needs replacement Hostname _____
2. <input type="checkbox"/>	Divert signaling traffic away from defective MP server	Follow steps in Appendix D to divert signaling traffic away from the defective MP to avoid any message loss during the maintenance window activity.
3. <input type="checkbox"/>	Verify that no signaling traffic is processed at defective MP server.	<ol style="list-style-type: none"> <li>1. Login to the SOAM GUI for the site where defective MP server is located.</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → KPIs] and select ‘EXHR’ tab.</li> <li>3. Verify following KPIs are now showing ‘0’ for MP server: <ul style="list-style-type: none"> <li>• <b>ExhrGttPerformed</b></li> <li>• <b>ExhrGttExceptionRouting</b></li> <li>• <b>ExhrMlrPerformed</b></li> </ul> </li> </ol>
4. <input type="checkbox"/>	Stop application software on MP server.	<ol style="list-style-type: none"> <li>1. Navigate to GUI page [Main Menu: Status &amp; Manage → Server] and select defective MP server by its hostname.</li> <li>2. Click ‘Stop’ button followed by ‘OK’ on confirmation screen.</li> </ol>
5. <input type="checkbox"/>	Replace MP server	<ol style="list-style-type: none"> <li>1. Power down the defective MP server.</li> <li>2. Label all cables connected to the defective MP server.</li> <li>3. Disconnect all cables so the defective MP server, and physically remove this server from the enclosure frame for the replacement.</li> <li>4. Prepare and configure the new DL360 MP server by instructions in Appendix B from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>5. Prepare and configure the new DL380 MP server by instructions in Appendix G and H from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>6. Wire in the new MP server according to the cables you labeled and removed from the old MP server.</li> <li>7. Verify all cables are properly reconnected as per reference [10] for physical installation.</li> <li>8. Power up the new MP server</li> </ol>

6. <input type="checkbox"/>	Install the new MP server and wait for it to complete the replication sync.	<ol style="list-style-type: none"> <li>1. Wait for ~10 min until PM&amp;C re-discovers the newly added MP server.</li> <li>2. Execute procedure 10 (Installing TVOE on all RMS) from reference [1] on the new MP.</li> <li>3. Execute procedure 11 (Configuring TVOE host network on all RMS) from reference [1] on the new MP.</li> <li>4. Execute procedure 12 (Create, IPM and Application on all VMs) from reference [1] on the new MP.</li> <li>5. Execute procedure 14, (Configuring Remaining HLRR Servers) steps 19 through 36 (Applying TKLCConfigData.sh configuration file on the new MP server) from reference [1].</li> <li>6. Execute procedure 18, step 21 through 23 (Restarting application on new MP server) from reference [1].</li> </ol>
7. <input type="checkbox"/>	Enable SS7 SCTP associations on newly installed MP server.	<ol style="list-style-type: none"> <li>1. Login to SOAM GUI as admin user.</li> <li>2. Navigate to GUI page [Main Menu: Transport Manager → Maintenance → Transport] and enable SCTP associations for the MP server.</li> </ol>
8. <input type="checkbox"/>	Verify SS7 Link status and enable links.	<ol style="list-style-type: none"> <li>1. Navigate to GUI page [Main Menu: SS7 / Sigtran → Maintenance → Links] and verify that links are all enabled on the MP server using SOAM GUI. <b>Enabled Down Association Down</b></li> <li>2. Enable links for the newly added MP server.</li> </ol>
9. <input type="checkbox"/>	Bring signaling traffic back to MP server.	Follow Appendix E and bring traffic back to MP.
10. <input type="checkbox"/>	Verify SS7 link status and traffic.	<ol style="list-style-type: none"> <li>1. Navigate to GUI page [Main menu: SS7 / Sigtran → Maintenance → Links] and verify that all links are enabled and normal on the MP. <b>Enabled Up Normal</b></li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → KPIs], the select 'EXHR' tab and verify that 'ExhrGttPerformed' KPI is showing non-zero value for the MP's hostname.</li> </ol>

### 2.2.3 Post Condition

- MP server is processing the signaling traffic

## 2.3 Replacement of a SOAM Server

### 2.3.1 Pre-Condition

- SOAM server has stopped functioning.
- It has been determined to replace the defective SOAM server.
- A new SOAM server replacement is available.
- Primary NOAM GUI is accessible.

### 2.3.2 Recovery Steps

1. <input type="checkbox"/>	Prepare for server replacement.	Identify the defective SOAM server that needs replacement Hostname _____
2. <input type="checkbox"/>	Make SOAM server “Standby” so it does not become active.	<ol style="list-style-type: none"> <li>1. Log in to the NOAM GUI via the VIP address as the admin user.</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → HA]</li> <li>3. Click “Edit” button</li> <li>4. Change “Max Allowed HA Role” of SOAM server to “Standby”</li> <li>5. Click “Ok” button.</li> </ol>
3. <input type="checkbox"/>	Remove defective SOAM from the server group.	<ol style="list-style-type: none"> <li>1. Select [Main Menu: Configuration → Server Groups] screen.</li> <li>2. Select server group of SOAM server.</li> <li>3. Click “Edit” button.</li> <li>4. Under ‘SG Inclusion’ uncheck SOAM server</li> <li>5. Click “Ok” button</li> </ol>
4. <input type="checkbox"/>	Power down and replace SOAM server	<ol style="list-style-type: none"> <li>1. Power down the defective SOAM server.</li> <li>2. Label all cables connected to this defective SOAM server.</li> <li>3. Disconnect all cables, and physically remove this server from the enclosure frame for the replacement.</li> <li>4. Prepare and configure the new DL360 SOAM server by instructions in Appendix B from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>5. Prepare and configure the new DL380 SOAM server by instructions in Appendix G and H from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>6. Wire in the new SOAM server according to the cables you labeled and removed from the old defective SOAM server.</li> <li>7. Verify all cables are properly reconnected as per reference [10] for physical installation.</li> <li>8. Power up the new SOAM server.</li> </ol>

5. <input type="checkbox"/>	Install and configure the new SOAM server	<ol style="list-style-type: none"> <li>1. Wait for ~10 min until PM&amp;C re-discovers the newly added SOAM server.</li> <li>2. Execute procedure 10 (Installing TVOE on all RMS) from reference [1] on the new SOAM.</li> <li>3. Execute procedure 11 (Configuring TVOE host network on all RMS) from reference [1] on the new SOAM.</li> <li>4. Execute procedure 12 (Create, IPM and Application on all VMs) from reference [1] on the new SOAM.</li> <li>5. Execute procedure 14, (Configuring Remaining HLRR Servers) steps 19 through 36 (Applying TKLCCConfigData.sh configuration file on the new SOAM server) from reference [1].</li> </ol>
6. <input type="checkbox"/>	Inhibit DB replication for all MP servers associated with the SOAM NE.	<ol style="list-style-type: none"> <li>1. Log in to the NOAM GUI via the VIP address as the admin user.</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>3. Filter on the SOAM Network Element.</li> <li>4. Record the MP server hostnames (Role: MP).</li> <li>5. Click on “Inhibit Replication” button for each MP server until replications on all MP servers associated with the SOAM Network Element have been inhibited.</li> </ol>
7. <input type="checkbox"/>	Add new SOAM server to the server group, make it “Active”, and restart the application.	<ol style="list-style-type: none"> <li>1. Execute procedure 17 (OAM Pairing for SOAM or DR NOAM sites), steps 14 through 16 (Adding new SOAM server back to server group) from reference [1]</li> <li>2. Execute procedure 17 (OAM Pairing for SOAM or DR NOAM sites), steps 19 through 25 (Changing HA role of new SOAM server from “Standby” to “Active”) from reference [1]</li> <li>3. Execute procedure 17 (OAM Pairing for SOAM or DR NOAM sites), steps 26 through 29 (Restarting application on new SOAM server) from reference [1]</li> </ol>
8. <input type="checkbox"/>	Allow DB replication for all MP servers associated with SOAM Network Element.	<ol style="list-style-type: none"> <li>1. Log in to the NOAM GUI as admin user.</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>3. Filter by SOAM network element scope and MP role.</li> <li>4. Click on “Allow Replication” button for each MP until replications on all MP servers associated with the SOAM Network Element have been allowed.</li> </ol>
9. <input type="checkbox"/>	Re-exchange SSH keys for PDE feature	<ol style="list-style-type: none"> <li>1. Login to Primary NOAM GUI as admin user.</li> <li>2. Perform SSH key exchange for <b>PDE</b> using this GUI page [Main Menu: EAGLE XG HLR Router → PDE → Options]</li> </ol> <p><i>Note:</i> See the Online Help for GUI to re-exchange keys or contact MOS - My Oracle Support for more assistance (See Appendix F).</p>

### 2.3.3 Post Condition

- SOAM server is back in the service

## 2.4 Replacement of a Query Server

### 2.4.1 Pre-Condition

- Query server has stopped functioning
- It has been determined to replace the defective Query server.
- A new replacement for Query server is available
- Primary NOAM GUI is accessible

### 2.4.2 Recovery Steps

1. <input type="checkbox"/>	Prepare for server replacement.	Identify defective Query server that needs replacement Hostname _____
2. <input type="checkbox"/>	Remove defective Query server from the NOAM server group.	<ol style="list-style-type: none"> <li>1. Login to Primary NOAM GUI as admin user.</li> <li>2. Navigate to GUI page [Main Menu: Configuration → Server Groups]</li> <li>3. Select NOAM’s server group containing the defective Query Server.</li> <li>4. Click “Edit” button.</li> <li>5. Under ‘SG Inclusion’ uncheck the defective Query Server</li> <li>6. Click “Ok” button</li> </ol>
3. <input type="checkbox"/>	Power down and replace defective Query server	<ol style="list-style-type: none"> <li>1. Power down the defective Query server</li> <li>2. Disconnect all cables, and physically remove this server from the enclosure frame for the replacement.</li> <li>3. Prepare and configure the new DL360 Query Server by instructions in Appendix B from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>4. Prepare and configure the new DL380 Query Server by instructions in Appendix G and H from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>5. Wire in the new Query server according to the cables you labeled and removed from the old defective Query server.</li> <li>6. Verify all cables are properly reconnected as per reference [10] for physical installation.</li> <li>7. Power up the new Query server</li> </ol>
4. <input type="checkbox"/>	Install and configure new Query server	<ol style="list-style-type: none"> <li>1. Wait for ~10 min until PM&amp;C re-discovers the newly added Query server.</li> <li>2. Execute procedure 10 (Installing TVOE on all RMS) from reference [1] on the new Query Server.</li> <li>3. Execute procedure 11 (Configuring TVOE host network on all RMS) from reference [1] on the new Query Server.</li> <li>4. Execute procedure 12 (Create, IPM and Application on all VMs) from reference [1] on the new Query Server.</li> <li>5. Execute procedure 14, (Configuring Remaining HLRR Servers) steps 19 through 36 (Applying TKLCCConfigData.sh configuration file on the new Query Server) from reference [1].</li> </ol>

5. <input type="checkbox"/>	Add Query server to NOAM server group. Restart application on Query server	<ol style="list-style-type: none"><li>1. Execute procedure 15 (OAM Pairing for the Primary NOAM Servers), steps 16 through 18 (Adding Query server to NOAM server group) from the reference [1]</li><li>2. Execute procedure 15 (OAM Pairing for the Primary NOAM Servers), steps 29 through 31 (Set HA level on Query Server) from the reference [1]</li><li>3. Execute procedure 15 (OAM Pairing for the Primary NOAM Servers), step 34 (Restarting application on Query Server) from the reference [1]</li></ol>
--------------------------------	---	---

### 2.4.3 Post Condition

- Query server is back in service

## 2.5 Replacement of a NOAM-A Server

### 2.5.1 Pre-Condition

- The NOAM-A server has stopped functioning.
- NOAM-A server was a VM guest hosted on the Management Server.
- It has been determined to replace defective NOAM-A server.
- The new NOAM-A server replacement is available.
- Primary NOAM GUI is accessible

### 2.5.2 Recovery Steps

<p>1. <input type="checkbox"/></p>	<p>Prepare for server replacement.</p>	<p>Identify the defective NOAM-A server that needs to be replaced. Hostname _____</p>
<p>2. <input type="checkbox"/></p>	<p>Make NOAM-A server “Standby” so it does not become active.</p>	<ol style="list-style-type: none"> <li>1. Login to the NOAM GUI as admin user using VIP address.</li> <li>2. Select [Main Menu: Status &amp; Manage → HA] screen.</li> <li>3. Click ‘Edit’ button.</li> <li>4. Change “Max Allowed HA Role” of NOAM-A server to ‘Standby’.</li> <li>5. Click OK button.</li> </ol>
<p>3. <input type="checkbox"/></p>	<p>Remove NOAM-A from the server group.</p>	<ol style="list-style-type: none"> <li>1. Select [Main Menu: Configuration → Server Groups] screen.</li> <li>2. Select NOAM’s server group.</li> <li>3. Click “Edit” button.</li> <li>4. Under ‘SG Inclusion’, uncheck the defective NOAM-A server.</li> <li>5. Click “Ok” button.</li> </ol>
<p>4. <input type="checkbox"/></p>	<p>Power down and replace NOAM-A server</p>	<ol style="list-style-type: none"> <li>1. Power down the defective NOAM-A server.</li> <li>2. Label all cables connected to defective NOAM-A server.</li> <li>3. Disconnect all cables, and physically remove this server from the enclosure frame for the replacement.</li> <li>4. Prepare and configure the new DL360 Query Server by instructions in Appendix B from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>5. Prepare and configure the new DL380 Query Server by instructions in Appendix G and H from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>6. Wire in the new NOAM-A server according to the cables you labeled and removed from the old NOAM server.</li> <li>7. Verify all cables are properly reconnected as per reference [10] for physical installation.</li> </ol>



<p>5. <input type="checkbox"/></p>	<p>Configure the Management Server, deploy PM&amp;C on Management server, and update PM&amp;C inventory</p>	<ol style="list-style-type: none"> <li>1. Execute procedure 2 (Install TVOE on First RMS) from reference [1].</li> <li>2. Execute procedure 3 (Configure Management Server Network) from reference [1].</li> <li>3. Execute procedure 4 (Deploy PM&amp;C on Management Server) from reference [1].</li> <li>4. Execute procedure 5 (Configure PM&amp;C application) from reference [1]</li> <li>5. Execute procedure 6 (Add Cabinet to PM&amp;C System Inventory) from reference [1].</li> <li>6. Execute procedure 7 (Add Rack Mount Server to PM&amp;C System Inventory) from reference [1].</li> <li>7. Execute procedure 8 (Add Software Image to PM&amp;C Server) from reference [1].</li> <li>8. Execute procedure 9, steps 1 through 22 (Configure Cisco 4948E-F Aggregation Switches using netConfig) from reference [1].</li> </ol>
<p>6. <input type="checkbox"/></p>	<p>Prepare the new NOAM-A server</p>	<ol style="list-style-type: none"> <li>1. Execute procedure 12 (Create, IPM and Install Application on all Virtual Machines) from reference [1] for NOAM-A.</li> <li>2. Execute procedure 13 (Configuring HLRR NOAM-A Server) from reference [1].</li> </ol>
<p>7. <input type="checkbox"/></p>	<p>Inhibit DB replication for all MP servers network wide.</p>	<ol style="list-style-type: none"> <li>1. Login to Primary NOAM GUI as admin user.</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>3. Click on “Inhibit Replication” button for each MP server (Role: MP) until all MP servers at each Network Element have been inhibited</li> </ol>
<p>8. <input type="checkbox"/></p>	<p>Inhibit DB replication for all Query servers network wide.</p>	<ol style="list-style-type: none"> <li>1. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>2. Click on “Inhibit Replication” button for each Query Server (Role: QUERY SERVER) until all Query Servers have been inhibited.</li> </ol>
<p>9. <input type="checkbox"/></p>	<p>Inhibit DB replication for all OAM servers network wide.</p>	<ol style="list-style-type: none"> <li>1. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>2. With the exception of the remaining NOAM-B server, click on “Inhibit Replication” button for each OAM server (Roles: NETWORK OAM&amp;P, and SYSTEM OAM) until all OAM servers at each Network Element have been inhibited.</li> </ol>
<p>10. <input type="checkbox"/></p>	<p>Add NOAM-A server to NOAM server group, make it active, and restart the application on NOAM-A server</p>	<ol style="list-style-type: none"> <li>1. Execute procedure 16 (OAM Pairing for the Primary NOAM Servers), steps 16 through 18 plus 21 and 22. (Adding NOAM-A server to NOAM server group) from the reference [1] for NOAM-A.</li> <li>2. Execute procedure 16 (OAM Pairing for the Primary NOAM Servers), steps 27 through 31 (Changing HA role of new NOAM-A server to “Active”) from reference [1] for NOAM-A</li> <li>3. Execute procedure 16 (OAM Pairing for the Primary NOAM Servers), steps 32 through 35 (Restarting application on NOAM-A server) from the reference [1] for NOAM-A.</li> </ol>
<p>11. <input type="checkbox"/></p>	<p>Allow DB replication for all OAM servers network wide.</p>	<ol style="list-style-type: none"> <li>1. Login to Primary NOAM GUI as admin user.</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>3. Click on “Allow Replication” button for each OAM server (Roles: NETWORK OAM&amp;P, and SYSTEM OAM) until all OAM servers at each Network Element have been allowed.</li> </ol>

12. <input type="checkbox"/>	Allow DB replication for all MP servers network wide.	<ol style="list-style-type: none"> <li>Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>Click on “Allow Replication” button for each MP server (Role: MP) until all MP servers at each Network Element have been allowed.</li> </ol>
13. <input type="checkbox"/>	Allow DB replication for all Query servers network wide.	<ol style="list-style-type: none"> <li>Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>Click on “Allow Replication” button for each Query server (Role: QUERY SERVER) until all query servers have been Allowed.</li> </ol>
14. <input type="checkbox"/>	Re-exchange SSH keys for PDB Import, PDB Export, PDE, and Data Export (APDE) features	<ol style="list-style-type: none"> <li>Login to Primary NOAM GUI as admin user.</li> <li>Perform SSH key exchange for <b>PDB Export</b> using this screen [Main Menu: EAGLE XG Database → Configuration → PDBI → Options]</li> <li>Perform SSH key exchange for <b>PDB Import</b> using this screen [Main Menu: EAGLE XG Database → Configuration → PDBI → Options]</li> <li>Perform SSH key exchange for <b>PDE</b> using this screen [Main Menu: EAGLE XG HLR Router → PDE → Options]</li> <li>Perform SSH key exchange for <b>Data Export (APDE)</b> using this screen [Main Menu: Administration → Remote Servers → Data Export]</li> </ol> <p><b>Note:</b> See the Online Help for each GUI to re-exchange keys or contact MOS - My Oracle Support for more assistance (See Appendix F).</p>

### 2.5.3 Post Condition

- NOAM-A server is back in the service

## 2.6 Replacement of a NOAM-B Server

### 2.6.1 Pre-Condition

- NOAM-B server has stopped functioning
- It has been determined to replace defective NOAM-B server.
- The new replacement for NOAM-B server is available
- Primary NOAM GUI is accessible

### 2.6.2 Recovery Steps

<p>1. <input type="checkbox"/></p>	<p>Prepare for server replacement.</p>	<p>Identify defective NOAM-B server that needs replacement                      Hostname _____</p>
<p>2. <input type="checkbox"/></p>	<p>Make NOAM-B server “Forced Standby” so it does not become active.</p>	<ol style="list-style-type: none"> <li>1. Login to the NOAM GUI as admin user using VIP address.</li> <li>2. Select [Main Menu: Status &amp; Manage → HA] screen</li> <li>3. Click ‘Edit’ button</li> <li>4. Change “Max Allowed HA Role” of NOAM-B server to ‘Standby’</li> <li>5. Click “OK” button</li> </ol>
<p>3. <input type="checkbox"/></p>	<p>Remove NOAM-B from the server group.</p>	<ol style="list-style-type: none"> <li>1. Select [Main Menu: Configuration → Server Groups] screen.</li> <li>2. Select NOAM’s server group.</li> <li>3. Click “Edit” button.</li> <li>4. Under ‘SG Inclusion’ uncheck the defective NOAM-B server</li> <li>5. Click “Ok” button</li> </ol>
<p>4. <input type="checkbox"/></p>	<p>Power down and replace NOAM-B Server</p>	<ol style="list-style-type: none"> <li>1. Power down the defective NOAM-B server.</li> <li>2. Label all cables connected to defective NOAM-B server.</li> <li>3. Disconnect all cables, and physically remove this server from the enclosure frame for the replacement.</li> <li>4. Prepare and configure the new DL360 Query Server by instructions in Appendix B from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>5. Prepare and configure the new DL380 Query Server by instructions in Appendix G and H from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>6. Wire in the new NOAM-B server according to the cables you labeled and removed from the old NOAM server.</li> <li>7. Verify all cables are properly reconnected as per reference [10] for physical installation.</li> </ol>

<p>5. <input type="checkbox"/></p>	<p>Prepare the new NOAM-B server</p>	<ol style="list-style-type: none"> <li>1. Wait for ~10 min until PM&amp;C re-discovers the newly added NOAM-B server.</li> <li>2. Execute procedure 10 (Installing TVOE on all RMS) from reference [1] on the new NOAM-B.</li> <li>3. Execute procedure 11 (Configuring TVOE host network on all RMS) from reference [1] on the new NOAM-B.</li> <li>4. Execute procedure 12 (Create, IPM and Application on all VMs) from reference [1] on the new NOAM-B.</li> <li>5. Execute procedure 14, (Configuring Remaining HLRR Servers) steps 19 through 36 (Applying TKLCCfgData.sh configuration file on the new NOAM-B server) from reference [1].</li> </ol>
<p>6. <input type="checkbox"/></p>	<p>Inhibit DB Replication for all MP servers network wide.</p>	<ol style="list-style-type: none"> <li>1. Go to the NOAM GUI.</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>3. Inhibit replication for each MP server until all MP servers (Role: MP) at each Network Element have been Inhibited.</li> </ol>
<p>7. <input type="checkbox"/></p>	<p>Inhibit DB Replication for all Query servers network wide.</p>	<ol style="list-style-type: none"> <li>1. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>2. Inhibit replication for each Query Server (Role: QUERY SERVER) until all Query Servers have been Inhibited.</li> </ol>
<p>8. <input type="checkbox"/></p>	<p>Inhibit DB Replication for all SOAM servers network wide.</p>	<ol style="list-style-type: none"> <li>1. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>2. With the exception of the remaining NOAM server, inhibit replication for each SOAM server (Role: SYSTEM OAM) until all SOAM servers at each Network Element have been Inhibited.</li> </ol>
<p>9. <input type="checkbox"/></p>	<p>Add NOAM-B server to NOAM server group, make it active, and restart the application on NOAM-B server</p>	<ol style="list-style-type: none"> <li>1. Execute procedure 16 (OAM Pairing for the Primary NOAM Servers), steps 16 through 18 plus 21 and 22. (Adding NOAM-B server to NOAM server group) from the reference [1] for NOAM-B.</li> <li>2. Execute procedure 16 (OAM Pairing for the Primary NOAM Servers), steps 27 through 31 (Changing HA role of new NOAM-B server to “Active”) from reference [1] for NOAM-B.</li> <li>3. Execute procedure 16 (OAM Pairing for the Primary NOAM Servers), steps 32 through 35 (Restarting application on NOAM-B server) from the reference [1] for NOAM-B.</li> </ol>
<p>10. <input type="checkbox"/></p>	<p>Allow DB Replication for all SOAM servers network wide.</p>	<ol style="list-style-type: none"> <li>1. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>2. Allow replication for each SOAM server (Role: SYSTEM OAM) until all SOAM servers at each Network Element have been Allowed.</li> </ol>
<p>11. <input type="checkbox"/></p>	<p>Allow DB Replication for all MP servers network wide.</p>	<ol style="list-style-type: none"> <li>1. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>2. Allow replication for each MP server (Role: MP) until all MP servers at each Network Element have been Allowed.</li> </ol>
<p>12. <input type="checkbox"/></p>	<p>Allow DB Replication for all Query servers network wide.</p>	<ol style="list-style-type: none"> <li>1. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>2. Allow replication for each Query Server (Role: QUERY SERVER) until all Query Servers have been Allowed.</li> </ol>

<p>13. <input type="checkbox"/></p>	<p>Re-exchange SSH keys for PDB Import, PDB Export, PDE, and Data Export (APDE) features</p>	<ol style="list-style-type: none"> <li>1. Login to Primary NOAM GUI as admin user.</li> <li>2. Perform SSH key exchange for <b>PDB Export</b> using this screen [Main Menu: EAGLE XG Database → Configuration → PDBI → Options]</li> <li>3. Perform SSH key exchange for <b>PDB Import</b> using this screen [Main Menu: EAGLE XG Database → Configuration → PDBI → Options]</li> <li>4. Perform SSH key exchange for <b>PDE</b> using this screen [Main Menu: EAGLE XG HLR Router → PDE → Options]</li> <li>5. Perform SSH key exchange for <b>Data Export (APDE)</b> using this screen [Main Menu: Administration → Remote Servers → Data Export]</li> </ol> <p><i>Note:</i> See the Online Help for each GUI to re-exchange keys or contact MOS - My Oracle Support for more assistance (See Appendix F).</p>
---	--	--

**2.6.3 Post Condition**

- NOAM-B server is back in service

## 2.7 Replacement of NOAM Server Pair

### 2.7.1 Pre-Condition

- Both active and standby NOAM servers have stopped functioning.
- DR NOAM servers are not available or are not installed.
- It has been determined to replace both defective NOAM servers.
- New NOAM servers for replacement are available.
- A recent backup archive file containing NOAM Configuration and Provisioning data is available.

### 2.7.2 Recovery Steps

1. <input type="checkbox"/>	Determine NOAM backup archive	Make sure that you have access to the customer’s NOAM backup archive files that contains both Provisioning and Configuration data.  This backup archive file should be in uncompressed format.
2. <input type="checkbox"/>	Power down and remove both old NOAM-A and NOAM-B servers. Replace them with new NOAM servers.	<ol style="list-style-type: none"> <li>1. Power down NOAM-A server.</li> <li>2. Power down the defective NOAM-A server.</li> <li>3. Label all cables connected to defective NOAM-A server.</li> <li>4. Disconnect all cables, and physically remove this server from the enclosure frame for the replacement.</li> <li>5. Prepare and configure the new DL360 Query Server by instructions in Appendix B from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>6. Prepare and configure the new DL380 Query Server by instructions in Appendix G and H from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>7. Wire in the new NOAM-A server according to the cables you labeled and removed from the old NOAM server.</li> <li>8. Verify all cables are properly reconnected as per reference [10] for physical installation.</li> <li>9. Power down the defective NOAM-B server.</li> <li>10. Label all cables connected to defective NOAM-B server.</li> <li>11. Disconnect all cables, and physically remove this server from the enclosure frame for the replacement.</li> <li>12. Prepare and configure the new DL360 Query Server by instructions in Appendix B from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>13. Prepare and configure the new DL380 Query Server by instructions in Appendix G and H from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>14. Wire in the new NOAM-B server according to the cables you labeled and removed from the old NOAM server.</li> <li>15. Verify all cables are properly reconnected as per reference [10] for physical installation.</li> <li>16. Power up new NOAM-A server only. Don’t power up new NOAM-B yet!</li> </ol>

<p>3. <input type="checkbox"/></p>	<p>Configure the Management Server, deploy PM&amp;C on Management server, and update PM&amp;C inventory</p>	<ol style="list-style-type: none"> <li>1. Execute procedure 2 (Install TVOE on First RMS) from reference [1].</li> <li>2. Execute procedure 3 (Configure Management Server Network) from reference [1].</li> <li>3. Execute procedure 4 (Deploy PM&amp;C on Management Server) from reference [1].</li> <li>4. Execute procedure 5 (Configure PM&amp;C application) from reference [1]</li> <li>5. Execute procedure 6 (Add Cabinet to PM&amp;C System Inventory) from reference [1].</li> <li>6. Execute procedure 7 (Add Rack Mount Server to PM&amp;C System Inventory) from reference [1].</li> <li>7. Execute procedure 8 (Add Software Image to PM&amp;C Server) from reference [1].</li> <li>8. Execute procedure 9, steps 1 through 22 (Configure Cisco 4948E-F Aggregation Switches using netConfig) from reference [1].</li> </ol>
<p>4. <input type="checkbox"/></p>	<p>Prepare the new NOAM-A server</p>	<ol style="list-style-type: none"> <li>1. Execute procedure 12 (Create, IPM and Install Application on all Virtual Machines) from reference [1] for NOAM-A.</li> <li>2. Execute procedure 13 (Configuring HLRR NOAM-A Server) from reference [1].</li> </ol>
<p>5. <input type="checkbox"/></p>	<p>Copy NOAM backup archive to new NOAM-A server, and perform DB restore from backup file.</p>	<ol style="list-style-type: none"> <li>1. Login via SSH to the console of new NOAM-A server.</li> <li>2. Copy the uncompressed backup archive identified in step 1 to newly installed first NOAM-A server at this location: <b>/var/TKLC/db/filemgmt</b></li> <li>3. Execute this command to stop running applications and leave database running: <b>prod.stop</b></li> <li>4. Restore configuration and provisioning database by executing this command: <b>idb.restore -n -t /var/TKLC/db/filemgmt -v &lt;archive file&gt;</b></li> <li>5. NOAM database is now restored</li> <li>6. Start the application by executing this command. <b>prod.start</b></li> </ol>
<p>6. <input type="checkbox"/></p>	<p>Install the new second NOAM-B server in the frame.</p>	<ol style="list-style-type: none"> <li>1. Power up the new NOAM-B server</li> <li>2. Follow all recovery steps 5 through 13 from section 2.6.2 of this document to restore the second NOAM-B server.</li> </ol>

### 2.7.3 Post Condition

- Both NOAM-A and NOAM-B servers are back in service
- Provisioning clients are connected to NOAM VIP address
- Provisioning continues

## 2.8 Replacement of SOAM Server Pair

### 2.8.1 Pre-Condition

- Both active and standby SOAM servers have stopped functioning
- It has been determined to replace both SOAM servers
- New replacements for SOAM servers are available
- Access to Primary NOAM GUI is available
- MPs are not receiving provisioning database updates.

### 2.8.2 Recovery Steps

<p>1. <input type="checkbox"/></p>	<p>Determine if MPs should carry traffic during this procedure and divert signaling traffic away from MPs at this SOAM site</p>	<ol style="list-style-type: none"> <li>1. Identify all MPs at the SOAM site.</li> <li>2. In absence of SOAMs, MPs will not get provisioning database updates. Poll customer to determine if traffic needs to be diverted away from these MPs.</li> <li>3. Divert traffic away from the MPs by applying Appendix D on each MP.</li> </ol>
<p>2. <input type="checkbox"/></p>	<p>Determine SOAM backup archive</p>	<p>Make sure that you have access to SOAMP backup archive file that contains only the Configuration data. This SOAM backup archive file should be in uncompressed format.</p>
<p>3. <input type="checkbox"/></p>	<p>Prepare for server replacement.</p>	<p>Identify the SOAM servers that needs replacement                      Hostname of first SOAM-A server _____                      Hostname of second SOAM-B server _____</p>
<p>4. <input type="checkbox"/></p>	<p>Place first SOAM-A server in Forced Standby.</p>	<ol style="list-style-type: none"> <li>1. Log in to the NOAM GUI via the VIP address as the admin user.</li> <li>2. Select [Main Menu: Status &amp; Manage → HA] screen.</li> <li>3. Click “Edit” button</li> <li>4. Change ‘Max Allowed HA Role’ of SOAM-A server to ‘Standby’</li> <li>5. Click “OK” button</li> </ol>
<p>5. <input type="checkbox"/></p>	<p>Remove first SOAM-A server from the Server Group.</p>	<ol style="list-style-type: none"> <li>1. Select [Main Menu: Configuration → Server Groups] screen.</li> <li>2. Select SOAM’s server group.</li> <li>3. Click “Edit” button.</li> <li>4. Under ‘SG Inclusion’ uncheck the first SOAM-A server</li> <li>5. Click “Ok” button</li> </ol>



<p>6. <input type="checkbox"/></p>	<p>Power down and remove first SOAM-A and second SOAM-B servers from the frame.  Replace them with new SOAM-A and SOAM-B servers.</p>	<p>Perform following steps for the first SOAM-A server</p> <ol style="list-style-type: none"> <li>1. Power down the defective SOAM server.</li> <li>2. Label all cables connected to this defective SOAM server.</li> <li>3. Disconnect all cables, and physically remove this server from the enclosure frame for the replacement.</li> <li>4. Prepare and configure the new DL360 SOAM server by instructions in Appendix B from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>5. Prepare and configure the new DL380 SOAM server by instructions in Appendix G and H from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]).</li> <li>6. Wire in the new SOAM server according to the cables you labeled and removed from the old defective SOAM server.</li> <li>7. Verify all cables are properly reconnected as per reference [10] for physical installation.</li> <li>8. Power up the new SOAM server.</li> <li>9. Repeat all above steps for the second SOAM-B server</li> </ol>
<p>7. <input type="checkbox"/></p>	<p>Install and configure software on first SOAM-A and second SOAM-B servers in the frame.</p>	<p>Perform following steps on the first SOAM-A server.</p> <ol style="list-style-type: none"> <li>1. Wait for ~10 min until PM&amp;C re-discovers the newly added SOAM server.</li> <li>2. Execute procedure 10 (Installing TVOE on all RMS) from reference [1] on the new SOAM.</li> <li>3. Execute procedure 11 (Configuring TVOE host network on all RMS) from reference [1] on the new SOAM.</li> <li>4. Execute procedure 12 (Create, IPM and Application on all VMs) from reference [1] on the new SOAM.</li> <li>5. Execute procedure 14, (Configuring Remaining HLRR Servers) steps 19 through 36 (Applying TKLCConfigData.sh configuration file on the new SOAM server) from reference [1].</li> <li>6. Repeat all above steps on the second SOAM-B server.</li> </ol>
<p>8. <input type="checkbox"/></p>	<p>Add SOAM-A server back to SOAM server group and restart the application on SOAM-A server</p>	<ol style="list-style-type: none"> <li>1. Execute procedure 17 (OAM Pairing for SOAM or DR NOAM sites), steps 14 through 16 (Adding new SOAM-A server back to server group) from reference [1]</li> <li>2. Execute procedure 17 (OAM Pairing for SOAM or DR NOAM sites), steps 19 through 25 (Changing HA role of new SOAM-A server from “Standby” to “Active”) from reference [1]</li> <li>3. Execute procedure 17 (OAM Pairing for SOAM or DR NOAM sites), steps 26 through 29 (Restarting application on new SOAM-A server) from reference [1]</li> </ol>
<p>9. <input type="checkbox"/></p>	<p>Place second SOAM-B server in Standby</p>	<ol style="list-style-type: none"> <li>1. Log in to the NOAM GUI via the VIP address as the admin user.</li> <li>2. Select [Main Menu: Status &amp; Manage → HA] screen.</li> <li>3. Click “Edit” button</li> <li>4. Change ‘Max Allowed HA Role’ of SOAM-B server to ‘Standby’</li> <li>5. Click “OK” button</li> </ol>

10. <input type="checkbox"/>	Remove second SOAM-B server from the Server Group.	<ol style="list-style-type: none"> <li>1. Select [Main Menu: Configuration → Server Groups] screen.</li> <li>2. Select SOAM's server group.</li> <li>3. Click "Edit" button.</li> <li>4. Under 'SG Inclusion' uncheck SOAM-B server</li> <li>5. Click "Ok" button</li> </ol>
11. <input type="checkbox"/>	Inhibit database replication for all MP servers associated with the NE.	<ol style="list-style-type: none"> <li>1. Go to the NOAM GUI.</li> <li>2. Select [Main Menu: Status &amp; Manage → Database] screen</li> <li>3. Filter on the SOAM Network Element.</li> <li>4. Record the MP server hostnames (Role: MP).</li> <li>5. Click "Inhibit Replication" button for each MP until all MP servers associated with the SOAM Network Element have been Inhibited.</li> </ol>
12. <input type="checkbox"/>	Add second SOAM-B server back to the SOAM server group and restart application on the second SOAM-B server	<ol style="list-style-type: none"> <li>1. Execute procedure 17 (OAM Pairing for SOAM or DR NOAM sites), steps 14 through 16 (Adding new SOAM-B server back to server group) from reference [1]</li> <li>2. Execute procedure 17 (OAM Pairing for SOAM or DR NOAM sites), steps 19 through 25 (Changing HA role of new SOAM-B server from "Standby" to "Active") from reference [1]</li> <li>3. Execute procedure 17 (OAM Pairing for SOAM or DR NOAM sites), steps 26 through 29 (Restarting application on new SOAM-B server) from reference [1]</li> </ol>
13. <input type="checkbox"/>	Verify that SOAM servers have received all NOAM provisioning and configuration data from NOAM.	<ol style="list-style-type: none"> <li>1. Login to active SOAM GUI using VIP address.</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → Servers]</li> <li>3. Make sure that newly replaced SOAM-A and SOAM-B servers show 'Norm' for replication, collections and application status.</li> </ol>
14. <input type="checkbox"/>	Restore the Configuration database on SOAM	Follow Appendix A to restore SOAM configuration data.
15. <input type="checkbox"/>	Allow database replication for all MP servers associated with the NE.	<ol style="list-style-type: none"> <li>1. Go to the NOAM GUI.</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>3. Filter on the SOAM Network Element.</li> <li>4. Record the MP server hostnames (Role: MP).</li> <li>5. Click on "Allow Replication" button for each MP until replications on all MP servers associated with the SOAM Network Element have been allowed.</li> </ol>
16. <input type="checkbox"/>	Bring traffic back on to the MPs	If traffic was diverted away in step 1, follow Appendix E to bring signaling traffic back to all MPs at the SOAM site.

### 2.8.3 Post Condition

- Both SOAM-A and SOAM-B servers are back in service
- SOAM configuration changes can be made from the SOAM GUI
- MP servers are now receiving provisioning database updates.

## 2.9 Replacement of DR NOAM Server Pair

### 2.9.1 Pre-Condition

- Both active and standby DR-NOAM servers have stopped functioning.
- It has been determined to replace the both DR-NOAM servers.
- New DR NOAM servers for replacement are available.
- Access to Primary NOAM GUI is functional.

### 2.9.2 Recovery Steps

1. <input type="checkbox"/>	Prepare for server replacement.	Identify the DR NOAM servers that needs replacement Hostname of first DR NOAM-A server _____ Hostname of second DR NOAM-B server _____
2. <input type="checkbox"/>	Place DR NOAM servers in Forced Standby	Log in to the NOAM GUI via the VIP address as the admin user. Perform following steps for the first DR NOAM-A server: 1. Select [Main Menu: Status & Manage → HA] screen 2. Click ‘Edit’ button 3. For first DR NOAM server, change its “Max Allowed HA Role” to “Standby” 4. Click “OK” button Repeat all above steps for the second DR NOAM-B server
3. <input type="checkbox"/>	Remove DR NOAM servers from the server group.	Perform following steps for the first DR NOAM-A server: 1. Select [Main Menu: Configuration → Server Groups] screen 2. Select DR NOAM’s server group 3. Click “Edit” 4. Under ‘SG Inclusion’ uncheck the first DR NOAM-A server 5. Click “Ok” button Repeat all above steps for the second DR NOAM-B server.
4. <input type="checkbox"/>	Power down and remove old DR NOAM servers. Replace with new DR NOAM servers	Perform following steps for the first DR NOAM-A server 1. Power down the defective DR NOAM server. 2. Label all cables connected to this defective DR NOAM server. 3. Disconnect all cables, and physically remove this server from the enclosure frame for the replacement. 4. Prepare and configure the new DL360 DR NOAM server by instructions in Appendix B from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]). 5. Prepare and configure the new DL380 DR NOAM server by instructions in Appendix G and H from reference [1] (BIOS and iLO setup), firmware upgrade should be in accordance with reference [8] and [9]). 6. Wire in the new DR NOAM server according to the cables you labeled and removed from the old defective DR NOAM server. 7. Verify all cables are properly reconnected as per reference [10] for physical installation. Repeat all above steps for the second DR NOAM-B server

<p>5. <input type="checkbox"/></p>	<p>Install software on DR NOAM-A servers in the frame.</p>	<p>Perform following steps for the first DR NOAM-A server</p> <ol style="list-style-type: none"> <li>1. Execute procedure 2 (Install TVOE on First RMS) from reference [1].</li> <li>2. Execute procedure 3 (Configure Management Server Network) from reference [1].</li> <li>3. Execute procedure 4 (Deploy PM&amp;C on Management Server) from reference [1].</li> <li>4. Execute procedure 5 (Configure PM&amp;C application) from reference [1]</li> <li>5. Execute procedure 6 (Add Cabinet to PM&amp;C System Inventory) from reference [1].</li> <li>6. Execute procedure 7 (Add Rack Mount Server to PM&amp;C System Inventory) from reference [1].</li> <li>7. Execute procedure 8 (Add Software Image to PM&amp;C Server) from reference [1].</li> <li>8. Execute procedure 9, steps 1 through 22 (Configure Cisco 4948E-F Aggregation Switches using netConfig) from reference [1].</li> </ol>
<p>6. <input type="checkbox"/></p>	<p>Prepare the new DR NOAM-A server.</p>	<ol style="list-style-type: none"> <li>1. Execute procedure 12 (Create, IPM and Install Application on all Virtual Machines) from reference [1] for DR NOAM-A.</li> <li>2. Execute procedure 13 (Configuring HLRR NOAM-A Server) from reference [1] on DR NOAM-A.</li> </ol>
<p>7. <input type="checkbox"/></p>	<p>Install software on DR NOAM-B servers in the frame.</p>	<ol style="list-style-type: none"> <li>1. Wait for ~10 min until PM&amp;C re-discovers the newly added DR NOAM-B server.</li> <li>2. Execute procedure 10 (Installing TVOE on all RMS) from reference [1] on the new DR NOAM-B.</li> <li>3. Execute procedure 11 (Configuring TVOE host network on all RMS) from reference [1] on the new DR NOAM-B.</li> <li>4. Execute procedure 12 (Create, IPM and Application on all VMs) from reference [1] on the new DR NOAM-B.</li> <li>5. Execute procedure 14, (Configuring Remaining HLRR Servers) steps 19 through 36 (Applying TKLCCConfigData.sh configuration file on the new DR NOAM-B server) from reference [1].</li> </ol>
<p>8. <input type="checkbox"/></p>	<p>Add new DR NOAM-A and B servers to the DR NOAM server group, make it “Active”, and restart the application.</p>	<ol style="list-style-type: none"> <li>1. Execute procedure 17 (OAM Pairing for SOAM or DR NOAM sites), steps 14 through 16 plus 19 and 20 (Adding new DR-NOAM-A and B servers back to DR NOAM server group) from reference [1].</li> <li>2. Execute procedure 17 (OAM Pairing for SOAM or DR NOAM sites), steps 21 through 25 (Changing HA role of new DR-NOAM-A and B servers from “Standby” to “Active”) from reference [1].</li> <li>3. Execute procedure 17 (OAM Pairing for SOAM or DR NOAM sites), steps 26 through 31 (Restarting application on new DR-NOAM-A and B servers) from reference [1].</li> </ol>

**2.9.3 Post Condition**

- Both DR NOAM servers are back in service

## 2.10 Replacement of Cisco 4948E-F Aggregation Switch

### 2.10.1 Pre-Condition

- A Cisco 4948E-F aggregation switch has been identified to be defective.
- A new replacement for Cisco 4948E-F aggregation switch is available.
- A backup of Cisco 4948E-F aggregation switch configuration was successfully performed and the archive file is available (see Section 3.2.5 of reference [3])
- OAM servers at the site are accessible

### 2.10.2 Recovery Steps

1. <input type="checkbox"/>	Prepare for switch replacement.	<ol style="list-style-type: none"> <li>1. Identify which Cisco 4948E-F Aggregation Switch that needs replacement.</li> <li>2. Determine if it is switch1A or switch1B at the HLRR site.</li> </ol>
2. <input type="checkbox"/>	Replace switch.	<ol style="list-style-type: none"> <li>1. Power down the faulty Cisco switch.</li> <li>2. Replace switch and re-attach cables to new switch.</li> <li>3. Power up the new Cisco switch.</li> </ol>
3. <input type="checkbox"/>	Initialize and Configure new switch.	<ol style="list-style-type: none"> <li>1. Initialize and configure the new switch by executing procedure 9, steps 22 through 43 (Configure Cisco 4948E-F Aggregation Switches using netConfig) from reference [1] for the switch that was replaced.</li> </ol>

### 2.10.3 Post Condition

- Cisco switch is back in service

## 2.11 Replacement of Independent NOAM Frame

### 2.11.1 Pre-Condition

- NOAM frame is destroyed
- A replacement NOAM frame with 2 NOAM servers and a Query Server (optional) is available
- DR-NOAM servers are available
- User can access GUI of the DR-NOAM

### 2.11.2 Recovery Steps

1. <input type="checkbox"/>	Determine NOAM site and status of provisioning	If NOAM frame is the Primary NOAM frame, then execute procedure from section 2.1 to activate DR-NOAM site in order to make it as Primary NOAM site.  This allows provisioning to continue and makes the defective frame a defective DR-NOAM frame.
2. <input type="checkbox"/>	Install new replacement frame	Follow procedures in reference [4] to install the new NOAM frame.
3. <input type="checkbox"/>	Recover NOAM-A server	Follow recovery steps from Section 2.5.
4. <input type="checkbox"/>	Configure switch1A	Follow recovery steps from Section 2.10.
5. <input type="checkbox"/>	Configure switch1B	Follow recovery steps from Section 2.10.
6. <input type="checkbox"/>	Recover NOAM-B server	Follow recovery steps from Section 2.6.
7. <input type="checkbox"/>	Recover Query server	Follow recovery steps from Section 2.4.

### 2.11.3 Post Condition

- NOAM frame is back in service and now serves as DR-NOAM frame

## 2.12 Replacement of Independent SOAM Frame

### 2.12.1 Pre-Condition

- SOAM frame is destroyed
- A replacement SOAM frame with 2 SOAM servers and MP servers is available

### 2.12.2 Recovery Steps

1. <input type="checkbox"/>	Install new SOAM frame.	Follow procedure in reference [4] to install new SOAM frame.
2. <input type="checkbox"/>	Recover SOAM server pair.	Follow recovery steps from Section 2.8.
3. <input type="checkbox"/>	Recover MP servers.	For each MP server, follow recovery steps from Section 2.2.

### 2.12.3 Post Condition

- SOAM frame is back in service

## 2.13 Replacement of the Combined NOAM+SOAM Frame

### 2.13.1 Pre-Condition

- A combined NOAM+SOAM frame is destroyed
- A replacement NOAM frame with 2 NOAM servers, 1 Query Server (optional), 2 SOAM servers and MP servers is available
- DR NOAM servers and GUI are available

### 2.13.2 Recovery Steps

1. <input type="checkbox"/>	Determine NOAM+SOAM site and status of provisioning	If NOAM + SOAM frame is the primary NOAM+SOAM frame, execute procedure from section 2.1 to activate DR NOAM site.  This allows provisioning to continue and makes the defective frame a defective DR NOAM frame.
2. <input type="checkbox"/>	Install new replacement frame	Follow procedures in reference [4] to install the new NOAM+SOAM frame.
3. <input type="checkbox"/>	Recover NOAM-A server	Follow recovery steps from Section 2.5.
4. <input type="checkbox"/>	Configure switch1A	Follow recovery steps from Section 2.10.
5. <input type="checkbox"/>	Configure switch1B	Follow recovery steps from Section 2.10.
6. <input type="checkbox"/>	Recover NOAM-B server	Follow recovery steps from Section 2.6.
7. <input type="checkbox"/>	Recover Query server	Follow recovery steps from Section 2.4.
8. <input type="checkbox"/>	Recover SOAM server pair	Follow recovery steps from Section 2.8.
9. <input type="checkbox"/>	Recover MP servers	For each MP server, follow recovery steps from section 2.2

### 2.13.3 Post Condition

- NOAM+SOAM frame is back in service




## APPENDIX A. RESTORING SOAM CONFIGURATION DATABASE (SS7/TRANSPORT) FROM THE BACKUP FILE

Use these instructions to restore the SOAM Configuration Database (SS7/Transport) at HLRR system.

The SS7/Transport Configuration Database consists of Adjacent Nodes, Transports, Adjacent Server Groups, Local Signaling Points, Local SCCP Users, Remote Signaling Points, Remote MTP3 Users, Link Sets, Links, and Routes configured via SOAM GUI and/or command line interface.

<p>1. <input type="checkbox"/></p>	<p>Determine the impact of restored data on signaling traffic running on MP</p>	<ol style="list-style-type: none"> <li>1. Evaluate the impact of the restored data on MP server(s) on SOAM site.</li> <li>2. It is advisable to divert traffic away from MP server(s) using <b>Appendix D</b> when performing the restore of database.</li> </ol>
<p>2. <input type="checkbox"/></p>	<p>On the SOAM GUI, perform the actions to upload SS7/Transport backup archive file and verify it was uploaded successfully.</p>	<ol style="list-style-type: none"> <li>1. Login to the SOAM GUI via VIP address.</li> <li>2. Identify the hostname of the active SOAM server Hostname = _____</li> <li>3. Navigate to GUI page [Main Menu: Status &amp; Manage → Files]</li> <li>4. Select the active SOAM server tab.</li> <li>5. Click on the 'Upload' button.</li> <li>6. Use 'Browse' button to select the backup archive containing SS7/Transport configuration database.</li> <li>7. Click on the 'Upload' button to upload the backup archive file to the active SOAM server.</li> <li>8. Verify that upload is complete and the backup archive file now shows up in the file list.</li> <li>9. If not already done so, create the directory /var/TKLC/db/filemgmt/backup and set its owner and permissions with the following commands: <ul style="list-style-type: none"> <li>• sudo mkdir /var/TKLC/db/filemgmt/backup</li> <li>• sudo chmod 775 /var/TKLC/db/filemgmt/backup</li> <li>• sudo chown awadmin:awadm /var/TKLC/db/filemgmt/backup</li> </ul> </li> <li>10. Move the backup archive file from the /var/TKLC/db/filemgmt directory to the /var/TKLC/db/filemgmt/backup directory and change the file permissions to rw-rw-rw- with the following commands: <ul style="list-style-type: none"> <li>• sudo mv /var/TKLC/db/filemgmt/&lt;backup archive name&gt; /var/TKLC/db/filemgmt/backup/&lt;backup archive name&gt;</li> <li>• sudo chmod 666 /var/TKLC/db/filemgmt/backup/&lt;backup archive name&gt;</li> </ul> </li> <li>11. Verify that the backup archive file is now in the backup directory with the correct file permissions.</li> </ol>

<p>3. <input type="checkbox"/></p>	<p>Execute a restore of SOAM configuration database.</p>	<ol style="list-style-type: none"> <li>1. Login to SOAM GUI via VIP address.</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>3. Select the active SOAM server. Server is now highlighted.</li> <li>4. Click ‘Restore’ button and select the backup archive file.</li> <li>5. GUI will display compatibility information. If databases are not compatible, then call Oracle’s Customer Care Center before selecting a ‘force’ option. If ‘force’ option is used, then SS7/Transport configuration data needs manual modifications.</li> <li>6. If the databases are compatible, then click ‘OK’ to continue with SS7/Transport database restoration.</li> <li>7. If databases are shown as incompatible, then review and record incompatibility information. If ‘server id’ within topology check are shown to be incompatible, check ‘force’ option then click ‘OK’ to continue with DB restoration.</li> <li>8. Wait for 5 minutes. There will be HA switch over for SOAM servers and you will have to log back in the SOAM GUI via VIP address again. Make sure that you are logging in to the same active server identified in Step 1 above.</li> </ol>
<p>4. <input type="checkbox"/></p>	<p>Check the status of SOAM database restore and rectify the SS7/Transport data if needed.</p>	<ol style="list-style-type: none"> <li>1. Login to SOAM GUI via VIP address.</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>3. Click on “Info” button to verify that database restore has completed. </li> <li>4. If ‘force’ option was used in step 3 above, then follow <b>Appendix B</b> to correct SS7 configuration data.</li> </ol>
<p>5. <input type="checkbox"/></p>	<p>Plan and replicate database down to MPs in controlled manner.</p>	<ol style="list-style-type: none"> <li>1. Login to NOAM GUI via VIP address</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>3. Allow replication to servers within SOAM site in following order:             <ol style="list-style-type: none"> <li>a. Select the ‘Standby’ SOAM server and click ‘Allow replication’</li> <li>b. Select the first MP server at the same SOAM network element and click ‘Allow replication’.</li> <li>c. Verify the functionality of first MP server and decide to roll out the restored data to all MP servers.</li> <li>d. Click ‘Allow Replication’ for all MPs.</li> <li>e. Select the active SOAM server and click ‘Allow Replication’.</li> </ol> </li> <li>4. Enable site provisioning on SOAM site             <ol style="list-style-type: none"> <li>a. Log in to SOAM GUI via VIP address</li> <li>b. Navigate to GUI page [Main Menu: Status &amp; Manage → Database].</li> <li>c. Click ‘Enable Site Provisioning’ button.</li> </ol> </li> <li>5. Login to NOAM GUI via VIP address</li> <li>6. Navigate to GUI page [Main Menu: Status &amp; Manage → HA]</li> <li>7. For the standby SOAM server             <ol style="list-style-type: none"> <li>a. Click “Edit” button</li> <li>b. Change ‘Max Allowed HA Role’ of standby SOAM server to ‘Active’</li> <li>c. Click “OK” button</li> </ol> </li> <li>8. SOAM configuration database restoration is complete.</li> </ol>

6. <input type="checkbox"/>	Restart MP application and bring traffic back to MP.	<ol style="list-style-type: none"><li>1. If MP traffic was diverted away in step 1, then for each MP at SOAM site do the following:<ol style="list-style-type: none"><li>a. Restart MP application on each MP at the SOAM site.<ol style="list-style-type: none"><li>i. On active NOAM GUI select [Main Menu: Status &amp; Manage → Server] screen</li><li>ii. Select MP server</li><li>iii. Click 'Restart' button</li></ol></li><li>b. Follow <b>Appendix E</b> to bring traffic back on the MP.</li></ol></li><li>2. Repeat above actions for next MPs</li></ol>
--------------------------------	--	---

### APPENDIX B. CORRECTING SOAM CONFIGURATION DATABASE (SS7/TRANSPORT)


When a SOAM backup performed in past is restored to newly recovered SOAM site, the Server ID mismatch could occur. In this situation a user could use ‘force’ option to restore SOAM configuration data and execute following procedure to correct SS7 configuration data.

<p>1. <input type="checkbox"/></p>	<p>Login to active SOAM server, and identify all MP servers enclosed in SOAM Network Element</p>	<p>1. Identify the hostname of active SOAM server                      Hostname _____</p> <p>2. Find the network element ID of the SOAM server:  <b>iqt -z -f_h_NE_ID Server where "Hostname = '&lt;SOAM Hostname&gt;'"</b></p> <p>3. Identify MP servers by this network element ID:  <b>iqt -z -fHostname -f_h_Server_ID Server where "_h_NE_ID = &lt;NEId&gt; and Role = 'MP'"</b></p> <p>4. Complete this list for each MP server on SOAM site:</p> <table border="1" data-bbox="535 745 1079 945"> <thead> <tr> <th>Server</th> <th>Hostname</th> <th>Server ID</th> </tr> </thead> <tbody> <tr> <td>MP 1</td> <td></td> <td></td> </tr> <tr> <td>MP 2</td> <td></td> <td></td> </tr> <tr> <td>...</td> <td></td> <td></td> </tr> <tr> <td>MP N</td> <td></td> <td></td> </tr> </tbody> </table>	Server	Hostname	Server ID	MP 1			MP 2			...			MP N		
Server	Hostname	Server ID															
MP 1																	
MP 2																	
...																	
MP N																	
<p>2. <input type="checkbox"/></p>	<p>Execute Step 3 through 6 for each of MP servers.</p>	<p>For each MP server defined in the above list, execute steps 3, 4 and 5 listed below</p>															
<p>3. <input type="checkbox"/></p>	<p>Find MP’s server group ID</p>	<p>1. Find ServerGroup ID for the MP  <b>iqt -z -f_h_SG_ID Server2SG where "_h_Server_ID = &lt;ServerId of MP&gt;"</b></p>															
<p>4. <input type="checkbox"/></p>	<p>Verify that Local Signaling Point code (LSP) assigned to MP has the same server ID.</p>	<p>1. Find the LSP ID for MP’s LSP from LocalSP table.  <b>iqt LocalSP</b>  <i>Note:</i> The LSP ID is stored under “_h_LSP_ID” column/field name</p> <p>2. Find the server group ID matching to MP’s LSP ID.  <b>iqt -p -z -f_h_SG_ID LSP2SG where "_h_LSP_ID = &lt;LSPId of LSP thatshould belong to this MP&gt;"</b></p> <p>3. Verify that the server group ID of this LSP must match to the server group ID of this MP. If server group ID does not match, then correct the server group ID in “LSP2SG” table.  <b>ivi LSP2SG</b>  <i>Note:</i> The server group ID is stored under “_h_SG_ID” column/field name</p>															
<p>5. <input type="checkbox"/></p>	<p>Verify that transports hosted on this MP server have the same server ID.</p>	<p>1. For Local Associations that does not match the server IDs of local MP server, update server ID for that record.  <b>ivi Transports</b>  <i>Note:</i> Server IDs are stored under “_h_Server_ID” column/field name.</p>															

<p>6. <input type="checkbox"/></p>	<p>Login to SOAM GUI and execute the backup of SS7/Transport configuration database</p>	<ol style="list-style-type: none"> <li>1. Log into SOAM GUI via VIP address.</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>3. Select the active SOAM server.</li> <li>4. Click on 'Backup' button The "Database Backup" page appears.</li> <li>5. Select the data to be backed up as "Configuration"</li> <li>6. Select the backup archive compression algorithm as "none"</li> <li>7. Choose a name of the backup that will exclusively identify the backup.</li> <li>8. Enter a comment in the Comment field to identify the backup file.</li> <li>9. Click on 'Ok' button.</li> <li>10. Wait for at least 5 minutes.</li> <li>11. Navigate to GUI page [Main Menu: Status &amp; Manage → Database].</li> <li>12. Click on 'Info' button and make sure the backup was successfully completed</li> <li>13. Navigate to GUI page [Main Menu: Status &amp; Manage → Files]</li> <li>14. Under the active SOAM server tab, select the newly created backup file</li> <li>15. Click "Download" button</li> <li>16. A pop-up window appears</li> <li>17. Click "Save As" button to offload the backup file to a secure location.</li> </ol>
--	---	---

### APPENDIX C. RESTORING NOAM PROVISIONING DATABASE (PDB) FROM THE BACKUP FILE

Use these instructions to restore NOAM Provisioning Database (PDB) at HLRR system. The Provisioning Database consists of DNs, IMSIs and Network Entities configured via PDBI and/or NOAM GUI.

<p>1. <input type="checkbox"/></p>	<p>Identify hostname of active Primary NOAM server</p>	<p>1. Determine the hostname of the active Primary NOAM Server                  Hostname _____</p>
<p>2. <input type="checkbox"/></p>	<p>Identify and copy the backup archive to the active Primary NOAM server.</p>	<p>1. Identify and locate NOAM provisioning database backup archive file stored in the uncompressed format.                  2. Use <b>scp</b> or <b>sftp</b> to copy the backup archive file to the following directory on active Primary NOAM server:  <b>/var/TKLC/db/filegmt</b></p>
<p>3. <input type="checkbox"/></p>	<p>Execute a restore of NOAM provisioning database.</p>	<p>1. Login to NOAM GUI via VIP address.                  2. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]                  3. Select the active NOAM server. Server is now highlighted.                  4. Click ‘Restore’ button                  5. Select the desired provisioning database backup archive file                  6. GUI displays compatibility information. If databases are not compatible, then stop and call My Oracle’s Support (See Appendix F) before selecting a ‘force’ option.                  7. If the databases are compatible, click ‘OK’ to continue with database restoration.                  8. Wait for ~5 minutes until database restore is complete.  <b>Note:</b> Database restore process could be a long operation. There will be HA switchover for NOAM servers and you will have to log back in the NOAM GUI via VIP address again. Make sure that you are logging in to the same active server identified in Step 1 above. During the database restoration, provisioning from GUI or via PDBI remains disabled. Replication of data down to SOAM sites is also disabled.</p>
<p>4. <input type="checkbox"/></p>	<p>Check database restore completion and start PDBI provisioning</p>	<p>1. Log back in to NOAM GUI via VIP address.                  2. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]                  3. Click on the “Info” button to verify that database restore has completed successfully.                    4. Click ‘Enable site provisioning’ button to enable site provisioning.  <b>Note:</b> External provisioning clients can now connect via PDBI and start updates to provision HLRR database.</p>

<p>5. <input type="checkbox"/></p>	<p>Plan and replicate database to rest of the servers including Signaling NEs in controlled manner.</p>	<ol style="list-style-type: none"> <li>1. Log in to NOAM GUI via VIP address.</li> <li>2. Navigate to GUI page [Main Menu: Status &amp; Manage → Database]</li> <li>3. Select active NOAM server.             <ol style="list-style-type: none"> <li>a. Click ‘Allow Replication’.</li> <li>b. Click ‘OK’.</li> </ol> </li> <li>4. Select first SOAM site to replicate newly restored provisioning database.             <ol style="list-style-type: none"> <li>a. Select the standby SOAM server                 <ol style="list-style-type: none"> <li>i. Click ‘Allow Replication’</li> <li>ii. Click ‘OK’</li> </ol> </li> <li>b. Select the first MP server at the same SOAM network element                 <ol style="list-style-type: none"> <li>i. Click ‘Allow Replication’</li> <li>ii. Click ‘OK’</li> </ol> </li> <li>c. Verify the functionality of first MP server and decide to roll out the restored data to all MP servers.</li> <li>d. Repeat (b) and (c) for all MPs.</li> <li>e. Select the active SOAM server                 <ol style="list-style-type: none"> <li>i. Click ‘Allow Replication’</li> <li>ii. Click ‘OK’.</li> </ol> </li> </ol> </li> <li>5. Verify that first SOAM site is processing traffic with new provisioning database correctly.</li> <li>6. Repeat step 2 for each remaining SOAM sites.</li> <li>7. Select ‘standby’ NOAM server             <ol style="list-style-type: none"> <li>a. Click ‘Allow replication’</li> <li>b. Click ‘OK’.</li> </ol> </li> <li>8. Select Query Server             <ol style="list-style-type: none"> <li>a. Click ‘Allow replication’</li> <li>b. Click ‘OK’.</li> </ol> </li> <li>9. Select DR NOAM servers one at a time (active 1<sup>st</sup>, then standby 2<sup>nd</sup>)             <ol style="list-style-type: none"> <li>a. Click ‘Allow replication’</li> <li>b. Click ‘OK’.</li> </ol> </li> <li>10. Navigate to GUI page [Main Menu: Status &amp; Manage → HA]</li> <li>11. For the standby NOAM server             <ol style="list-style-type: none"> <li>a. Click “Edit” button</li> <li>b. Change ‘Max Allowed HA Role’ of standby NOAM server to ‘Active’</li> <li>c. Click “OK” button</li> </ol> </li> <li>12. NOAM provisioning database restoration now is complete.</li> </ol>
--	---	---

### APPENDIX D. DIVERTING SIGNALING TRAFFIC AWAY FROM THE MP SERVER

When doing maintenance activity on affected MP server, it is recommended to divert the signaling traffic away from the affected MP server until the maintenance activity is complete. This is to eliminate traffic loss at the affected MP server.

<p>1. <input type="checkbox"/></p>	<p>Identify the hostname of the affected MP server</p>	<p>1. Identify the hostname of the affected MP server Hostname _____</p>
<p>2. <input type="checkbox"/></p>	<p>Determine True Point Code (TPC) and Capability Point Code (CPC) of the affected MP server.</p>	<p>1. Login to the SOAM GUI via VIP address for the site where the affected MP is located. 2. Navigate to GUI page [Main Menu: Configuration → Server Groups] and determine MP server’s group name. 3. Navigate to GUI page [Main Menu: SS7 / Sigtran → Configuration → Local Signaling Points] and determine True Point Code (TPC) and Capability Point Code (CPC) for this MP server group: MP server’s TPC = _____ MP server’s CPC = _____</p>
<p>3. <input type="checkbox"/></p>	<p>Identify Eagle STPs that are connected to the affected MP server, and determine their Point Codes.</p>	<p>1. Navigate to GUI page [Main Menu: Transport Manager → Configuration → Transport] 2. Set the filter to MP’s hostname, and determine ‘Adjacent Node’ names of Eagle STPs. 3. Cross reference the ‘Adjacent Node’ names of Eagle STPs with [Main Menu: SS7/Sigtran → Configuration → Adjacent Server Groups] screen and determine ‘Adjacent Server Group’ names of Eagle STP. 4. Cross reference the ‘Adjacent Server Group’ name with [Main Menu: SS7/Sigtran → Configuration → Remote Signaling Points] screen and determine MTP Point Codes of Eagle STPs connected to this MP server: Eagle STP-1 MTP Point Code = _____ Eagle STP-2 MTP Point Code = _____ ... Eagle STP-N MTP Point Code = _____</p>
<p>4. <input type="checkbox"/></p>	<p>Divert signaling traffic away from the affected MP server at the Eagle STP. Execute these steps at each Eagle STP connected to this MP server.</p>	<p>The signaling traffic to the affected MP server can be diverted away in 2 steps: 1. Increase the relative cost of the link set to MP server’s True Point Code (TPC) for route to MP’s Capability Point Code (CPC) by issuing this command on Eagle STP terminal: <b>chg-rte</b> 2. Wait for ~30 seconds and then disable the link going to MP server’s True Point Code (TPC) by issuing this command on Eagle STP terminal: <b>dact-slk</b> <i>Note:</i> For more info, see “Eagle STP Commands Manual” [2]</p>



### APPENDIX E. BRINGING SIGNALING TRAFFIC BACK TO THE MP SERVER

After the maintenance activity on the affected MP server is completed, the signaling traffic can be brought back to the affected MP server by using the following steps.

<p>1. <input type="checkbox"/></p>	<p>Identify the hostname of the affected MP server.</p>	<p>1. Identify the hostname of the affected MP server Hostname _____</p>
<p>2. <input type="checkbox"/></p>	<p>Determine True Point Code (TPC) and Capability Point Code (CPC) of the affected MP server.</p>	<p>1. Login to the SOAM GUI via VIP address for the site where the affected MP is located. 2. Navigate to GUI page [Main Menu: Configuration → Server Groups] and determine MP server’s group name. 3. Navigate to GUI page [Main Menu: SS7/Sigtran → Configuration → Local Signaling Points] and determine True Point Code (TPC) and Capability Point Code (CPC) for the MP server group: MP server’s TPC = _____ MP server’s CPC = _____</p>
<p>3. <input type="checkbox"/></p>	<p>Identify Eagle STPs that are connected to the affected MP server, and determine their Point Codes.</p>	<p>1. Navigate to GUI page [Main Menu: Transport Manager → Configuration → Transport]. 2. Set the filter to MP’s hostname, and determine ‘Adjacent Node’ names of Eagle STPs. 3. Cross reference the ‘Adjacent Node’ names of Eagle STPs with [Main Menu: SS7/Sigtran → Configuration → Adjacent Server Groups] screen and determine ‘Adjacent Server Group’ names of Eagle STP. 4. Cross reference the ‘Adjacent Server Group’ name with [Main Menu: SS7/Sigtran → Configuration → Remote Signaling Points] screen and determine MTP Point Codes of Eagle STPs connected to this MP server: Eagle STP-1 MTP Point Code = _____ Eagle STP-2 MTP Point Code = _____ ... Eagle STP-N MTP Point Code = _____</p>
<p>4. <input type="checkbox"/></p>	<p>Bring signaling traffic back to the affected MP server at the Eagle STP. Execute these steps at each Eagle STP connected to this MP server.</p>	<p>The signaling traffic to the affected MP server can be brought back in 2 steps: 1. Reduce the relative cost (to pre-maintenance value) of link set to MP server’s TPC for route to MP’s Capability Point Code (CPC) by issuing this command on Eagle STP terminal: <b>chg-rte</b> 2. Wait for ~30 seconds and then enable the link going to MP server’s True Point Code (TPC) by issuing this command on Eagle STP terminal: <b>act-slk</b> <i>Note:</i> For more info, see “Eagle STP Commands Manual” [2]</p>

## APPENDIX F. 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 2 for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS. MOS is available 24 hours a day, 7 days a week, 365 days a year.

### **Emergency Response**

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at **1-800-223-1711** (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

### **Locating Product Documentation on the Oracle Help Center Site**

Oracle customer documentation is available on the web at the Oracle Help Center (OHC) site, <http://docs.oracle.com>. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at <http://www.adobe.com>.

1. Access the OHC site at <http://docs.oracle.com>.
2. Click Industries.
3. Under the Oracle Communications subheading, click the Oracle Communications documentation link.
4. The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."

5. Click the Product and then the Release Number. A list of the entire documentation set for the selected product and release appears.
6. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser), and save to a local folder.