

# **Oracle® Communications**

## **Diameter Signaling Router**

Rack Mount Server Disaster Recovery Guide

Release 8.5

F34928-01

October 2020

**ORACLE®**

### Oracle Communications DSR Rack Mount Server Disaster Recovery User's Guide, Release 8.5

Copyright © 2020 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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

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

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

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

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates is not responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.



**CAUTION:** Use only the Upgrade procedure included in the Upgrade Kit.

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

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

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

See more information My Oracle Support (MOS).

## Table of Contents

<b>1. Introduction.....</b>	<b>6</b>
1.1 References .....	6
1.2 Acronyms.....	6
1.3 Terminology.....	7
1.4 How to Use this Document.....	8
1.5 Optional Features .....	8
<b>2. General Description .....</b>	<b>9</b>
2.1 Complete Server Outage (All Servers).....	10
2.2 Partial Server Outage with One NOAM Server Intact and Both SOAMs Failed .....	10
2.3 Partial Server Outage with Both NOAM Servers Failed and One SOAM Server Intact.....	10
2.4 Partial Server Outage with NOAM and One SOAM Server Intact .....	11
2.5 Partial Server Outage with Both NOAMs Failed and DR-NOAM Available .....	11
2.6 Partial Service Outage with Corrupt Database .....	11
<b>3. Procedure Overview .....</b>	<b>11</b>
3.1 Required Materials .....	11
3.2 Disaster Recovery Strategy.....	12
<b>4. Disaster Recovery Procedure .....</b>	<b>14</b>
4.1 Recovery Scenario 1 (Complete Server Outage).....	14
4.2 Recovery Scenario 2 (Partial Server Outage with One NOAM Server Intact and ALL SOAMs Failed) .....	56
4.3 Recovery Scenario 3 (Partial Server Outage with All NOAM Servers Failed and One SOAM Server Intact) .....	90
4.4 Recovery Scenario 4 (Partial Server Outage with One NOAM Server and One SOAM Server Intact) .....	123
4.5 Recovery Scenario 5 (Both NOAM Servers Failed with DR-NOAM Available).....	147
4.6 Recovery Scenario 6 (Database Recovery) .....	152
4.6.1 Recovery Scenario 6: Case 1 .....	152
4.6.2 Recovery Scenario 6: Case 2 .....	158
<b>5. Resolve User Credential Issues after Database Restore .....</b>	<b>163</b>
5.1 Restore a Deleted User .....	163
5.2 Keep a Restored User .....	163
5.3 Remove a Restored User.....	165
5.4 Restore a Modified User.....	166
5.5 Restore an Archive that Does Not Contain a Current User .....	166
<b>6. IDIH Disaster Recovery .....</b>	<b>171</b>
<b>Appendix A. DSR Database Backup .....</b>	<b>177</b>

<b>Appendix B. Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only).....</b>	<b>181</b>
<b>Appendix C. Inhibit A and B Level Replication on C-level Servers .....</b>	<b>183</b>
<b>Appendix D. Un-Inhibit A and B Level Replication on C-level Servers .....</b>	<b>184</b>
<b>Appendix E. Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost).....</b>	<b>185</b>
<b>Appendix F. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost) .....</b>	<b>187</b>
<b>Appendix G. Restore TVOE Configuration from Backup Media.....</b>	<b>189</b>
<b>Appendix H. Restore PMAC from Backup .....</b>	<b>197</b>
<b>Appendix I. Restore Provisioning Database .....</b>	<b>206</b>
<b>Appendix J. Recover PDB Relay .....</b>	<b>210</b>
<b>Appendix K. SNMP Configuration .....</b>	<b>211</b>
<b>Appendix L. Backup Directory .....</b>	<b>214</b>
<b>Appendix M. netConfig backupConfiguration/restoreConfiguration/upgradeFirmware with TPD cipher change .....</b>	<b>216</b>
<b>Appendix N. My Oracle Support (MOS) .....</b>	<b>218</b>

## List of Tables

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

## List of Figures

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

## List of Procedures

Procedure 1. Recovery Scenario 1 .....	15
Procedure 2. Recovery Scenario 2 .....	57
Procedure 3. Recovery Scenario 3 .....	91
Procedure 4. Recovery Scenario 4 .....	124
Procedure 5. Recovery Scenario 5 .....	147
Procedure 6. Recovery Scenario 6 (Case 1) .....	152
Procedure 7. Recovery Scenario 6 (Case 2) .....	158

Procedure 8. Keep Restored User .....	163
Procedure 9. Remove the Restored User .....	165
Procedure 10. Restore an Archive That Does Not Contain a Current User .....	167
Procedure 11. IDIH Disaster Recovery Preparation .....	172
Procedure 12. IDIH Disaster Recovery (Re-Install Mediation and Application Servers) .....	174
Procedure 13. DSR Database Backup .....	177
Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F) (HP DL380 Gen 9 Only) .....	181
Procedure 15. Inhibit A and B Level Replication on C-level Servers .....	183
Procedure 16. Un-Inhibit A and B Level Replication on C-level Servers .....	184
Procedure 17. Inhibit A and B Level Replication on C-level Servers .....	185
Procedure 18. Un-Inhibit A and B Level Replication on C-Level Servers .....	187
Procedure 19. Restore TVOE Configuration from Backup Media .....	189
Procedure 20. Restore PMAC from Backup Media .....	197
Procedure 21. Restore PMAC from Backup Server .....	200
Procedure 22. Restore Provisioning Database .....	206
Procedure 23. Recover PDB Relay .....	210
Procedure 24. Configure SNMP .....	211
Procedure 25. Backup Directory .....	214
Procedure 26. Turn off cipher list before backupConfiguration/restoreConfiguration/upgradeFirmware command .....	216
Procedure 27. Resume cipher list after backupConfiguration/restoreConfiguration/upgradeFirmware command .....	217

## 1. Introduction

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

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

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

### 1.1 References

- [1] TPD Initial Product Manufacture
- [2] Platform 7.2 Configuration Procedure Reference
- [3] DSR FABR Feature Activation Procedure
- [4] DSR RBAR Feature Activation Procedure
- [5] DSR MAP-Diameter Feature Activation Procedure
- [6] PM&C Disaster Recovery Guide
- [7] DSR PCA Activation Guide
- [8] DSR Rack Mount Server Installation Guide
- [9] DSR Hardware and Software Installation Procedure 1/2
- [10] DCA Framework and Application Activation and Deactivation Guide
- [11] DSR Security Guide
- [12] DSR DTLS Feature Activation Procedure
- [13] DSR/SDS NOAM Failover User's Guide

### 1.2 Acronyms

An alphabetized list of acronyms used in the document.

**Table 1. Acronyms**

Acronym	Definition
BIOS	Basic Input Output System
CD	Compact Disk
DSR	Diameter Signaling Router
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
FRU	Field Replaceable Unit
IDIH	Integrated Diameter Intelligence Hub

Acronym	Definition
iLO	Integrated Lights Out manager
IPFE	IP Front End
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
MSA	Modular Smart Array
NB	NetBackup
OA	HP Onboard Administrator
OS	Operating System (e.g. TPD)
PCA	Policy and Charging Application
PMAC	Platform Management & Configuration
RMS	Rack Mounted Server
SAN	Storage Area Network
SDS	Subscriber Database Server
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtual Operating Environment
VM	Virtual Machine

### 1.3 Terminology

An alphabetized list of terms used in the document.

**Table 2. Terminology**

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

## 1.4 How to Use this Document

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

1. Before beginning a procedure, completely read the instructional text (it displays immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.
2. Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.
3. If a procedural STEP fails to execute successfully or fails to receive the desired output, STOP the procedure. It is recommended to contact My Oracle Support (MOS) for assistance, as described in Appendix N before attempting to continue.

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

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

	Title/Instructions	Directive/Result Steps
1. <input type="checkbox"/>	Change directory	Change to the backout directory. <code>\$ cd /var/TKLC/backout</code>
2. <input type="checkbox"/>	Verify Network Element data	View the Network Elements configuration data; verify the data; save and print report. 1. Select <b>Configuration &gt; Network Elements</b> to view Network Elements Configuration screen.

Figure 1. Example Procedure Steps Used in This Document

## 1.5 Optional Features

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

Table 3. Optional Features

Feature	Document
Diameter Custom Applications (DCA)	DCA Framework and Application Activation and Deactivation Guide
Diameter Mediation	DSR Meta Administration Feature Activation Procedure
Full Address Based Resolution (FABR)	DSR FABR Feature Activation Procedure
Gateway Location Application (GLA)	DSR GLA Feature Activation Procedure



Feature	Document
Host Intrusion Detection System (HIDS)	DSR Security Guide (Section 3.2)
Map-Diameter Interworking (MAP-IWF)	DSR MAP-Diameter IWF Feature Activation Procedure
Policy and Charging Application (PCA)	DSR PCA Activation Guide
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation Procedure

## 2. General Description

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

**Table 4. Recovery Scenarios**

Procedure	State of NOAM and/or SOAM server(s)
Recovery of the entire network from a total outage Recovery Scenario 1 (Complete Server Outage)	<ul style="list-style-type: none"> <li>All NOAM servers failed.</li> <li>All SOAM servers failed.</li> <li>MP servers may or may not have failed.</li> </ul>
Recovery of one or more servers with at least one NOAM server intact Recovery Scenario 2 (Partial Server Outage with One NOAM Server Intact and ALL SOAMs Failed)	<ul style="list-style-type: none"> <li>At least 1 NOAM server is intact and available.</li> <li>All SOAM servers failed.</li> <li>MP servers may or may not have failed.</li> </ul>
Recovery of the NOAM pair with one or more SOAM servers intact Recovery Scenario 3 (Partial Server Outage with All NOAM Servers Failed and One SOAM Server Intact)	<ul style="list-style-type: none"> <li>All NOAM servers failed.</li> <li>At least 1 SOAM server out of active, standby, spare is intact and available.</li> <li>MP servers may or may not have failed.</li> </ul>
Recovery of one or more server with at least one NOAM and one SOAM server intact Recovery Scenario 4 (Partial Server Outage with One NOAM Server and One SOAM Server Intact)	<ul style="list-style-type: none"> <li>At least 1 NOAM server is intact and available.</li> <li>At least 1 SOAM server out of active, standby, spare is intact and available.</li> <li>1 or more MP servers have failed.</li> </ul>
Recovery Scenario 5 (Both NOAM Servers Failed with DR-NOAM Available)	<ul style="list-style-type: none"> <li>Both NOAM servers failed.</li> <li>DR NOAM is available</li> <li>SOAM servers may or may not be failed.</li> <li>MP servers may or may not be failed.</li> </ul>
Section Recovery Scenario 6 (Database Recovery) Recovery of one or more server with corrupt databases that cannot be restored using replication from the active parent node.	<ul style="list-style-type: none"> <li>Server is intact</li> <li>Database gets corrupted on the server</li> <li>Latest database backup of the corrupt server is present</li> <li>Replication is inhibited (either manually or because of Comcol upgrade barrier)</li> </ul>

Procedure	State of NOAM and/or SOAM server(s)
Section Recovery Scenario 6: Case 1	<ul style="list-style-type: none"> <li>• Server is intact</li> <li>• Database gets corrupted on the server</li> <li>• Replication is occurring to the server with corrupted database</li> </ul>
Section Recovery Scenario 6: Case 2	<ul style="list-style-type: none"> <li>• Server is intact</li> <li>• Database gets corrupted on the server</li> <li>• Latest Database backup of the corrupt server is NOT present</li> <li>• Replication is inhibited (either manually or because of Comcol upgrade barrier)</li> </ul>

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

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

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

## 2.1 Complete Server Outage (All Servers)

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

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

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

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

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

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

## 2.4 Partial Server Outage with NOAM and One SOAM Server Intact

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

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

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

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

## 2.6 Partial Service Outage with Corrupt Database

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

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

## 3. Procedure Overview

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

### 3.1 Required Materials

The following items are needed for disaster recovery:

1. A hardcopy of this document and hardcopies of all documents in the reference list.
2. Hardcopy of all NAPD performed at the initial installation and network configuration of this customer's site. If the NAPD cannot be found, escalate this issue within My Oracle Support (MOS) until the NAPD documents can be located.
3. DSR recent backup files: electronic backup file (preferred) or hardcopy of all DSR configuration and provisioning data.
4. Latest Network Element report: Electronic file or hardcopy of Network Element report.
5. The XML configuration files used to configure the Cisco 4948 aggregation switches, available on the PMAC Server (or PMAC backup).
6. The switch backup files taken after the switch is configured, available on the PMAC server (or PMAC backup).
7. The network element XML file used for the initial configuration.
8. Firmware files as provide by hardware vendor.
9. NetBackup files if they exist. This may require the assistance of the customer's NetBackup administrator.
10. PMAC and TVOE backups (if available).
11. One (1) target release DSR media or a target-release ISO.
12. One (1) target release SDS Media or a target-release ISO (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only).
13. Three (3) target release iDIH Media or target-release ISOs.

14. Site specific VM Placement and Socket Pinning workbook used during deployment (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 only).
15. Latest RADIUS shared secret encryption key file backup (DpiKf.bin.encr).
16. List of activated and enabled features.

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

## 3.2 Disaster Recovery Strategy

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

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

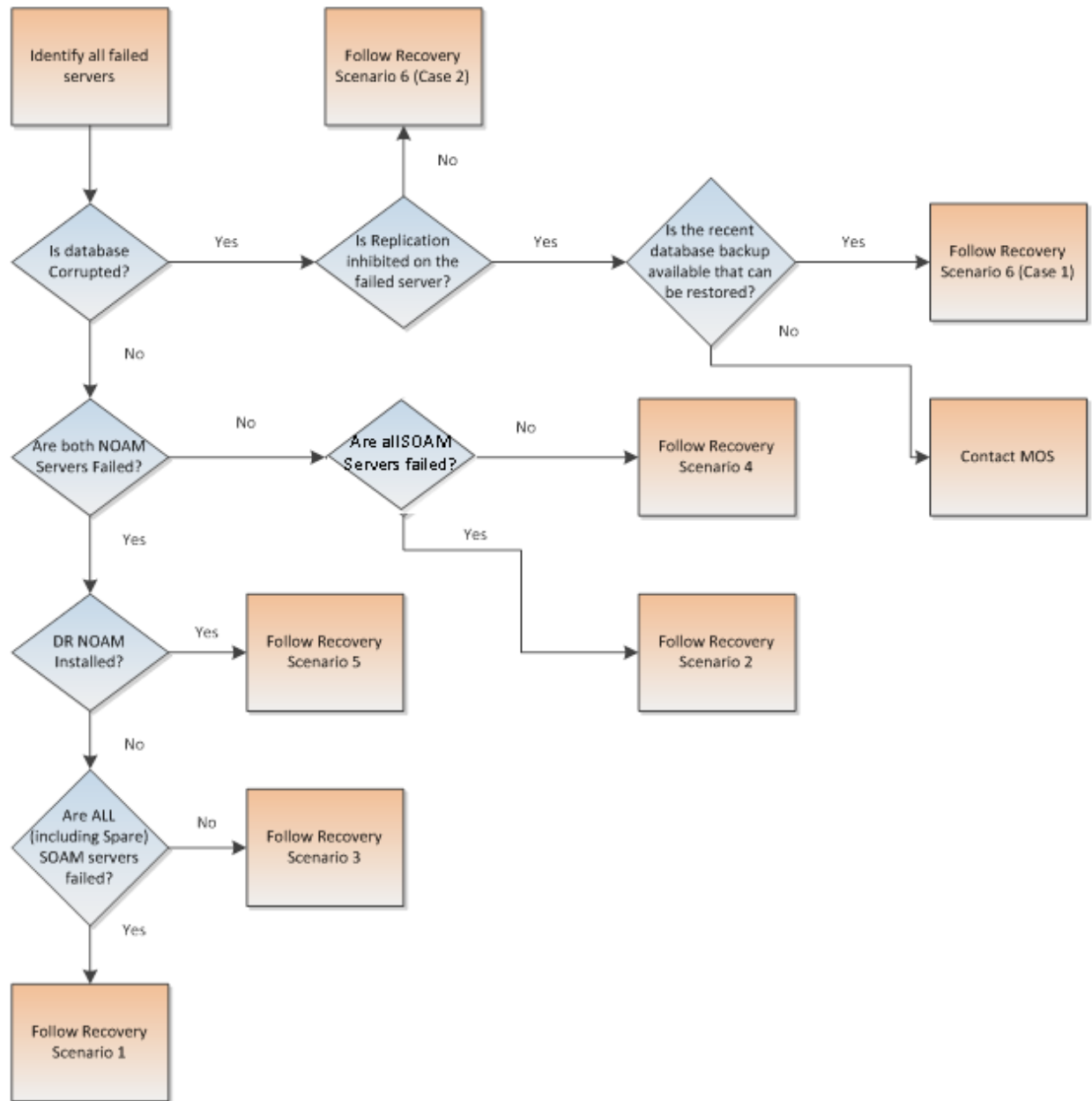


Figure 2. Determining Recovery Scenario

## 4. Disaster Recovery Procedure

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

### WARNING

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

#### Recovering Base Hardware:

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

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



### WARNING

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

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

- Backup.dsr.DSRNO1.Configuration.NETWORK\_OAMP.20180328\_021502.AUTO.tar
- Backup.dsr.DSRNO1.Configuration.SYSTEM\_OAM.20180328\_021502.AUTO.tar
- X7201TVOE-plat-app-201803281022.iso
- backupPmac\_20180328\_050002.pef5.1.1

### 4.1 Recovery Scenario 1 (Complete Server Outage)

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

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

- Recover base hardware and software for all rack mount servers
  - Recover the base hardware
  - Recover the virtual machines
  - Recover the software
- Recover **PMAC**

- Recover active **NOAM** guest
  - Recover the NOAM database
  - Reconfigure the application
- Recover standby **NOAM** guest
  - Reconfigure the application
- Recover query server (SDS only) guest
  - Reconfigure the application
- Recover all **SOAM** and MP/DP guest
  - Recover the SOAM database
  - Reconfigure the application
- Recover **IDIH**, if necessary
- Restart processes and re-enable provisioning and replication.

### Procedure 1. Recovery Scenario 1

S T E P #	<p>This procedure performs recovery if both NOAM servers are failed and all SOAM servers failed. This procedure also covers the C-level server failure.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>	
1. <input type="checkbox"/>	Gather required materials	Gather the documents and required materials listed in the Required Materials section.
2. <input type="checkbox"/>	Create a backup directory, if needed	Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.
3. <input type="checkbox"/>	Replace failed equipment	Work with the hardware vendor to replace the failed equipment.
4. <input type="checkbox"/>	<b>Recover PMAC and PMAC TVOE Host:</b> Configure BIOS settings and update firmware	<ol style="list-style-type: none"> <li>1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:             <ul style="list-style-type: none"> <li>• <b>HP DL380 Gen8:</b> Configure HP Gen 8 Server BIOS Settings</li> <li>• <b>Oracle X5-2/Netra X5-2/X6-2/X7-2:</b> Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings</li> <li>• <b>HP DL380 Gen9:</b> Configure HP Gen9 Server BIOS Settings</li> </ul> </li> <li>2. Verify and/or upgrade server firmware by executing the <b>Upgrade Rack Mount Server Firmware</b> procedure from reference [8].</li> </ol> <p><b>Note:</b> Determine VM placement and pinning by following:</p> <ul style="list-style-type: none"> <li>• Section 3.1, item 14; and</li> <li>• In reference [8], Appendix S VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1 Gbps NICs) and CPU Pinning in HP DL380 Gen 9 (Onboard 1 Gbps NICs) for Pinning Information on HP DL380 Gen 9.</li> </ul>

**Procedure 1. Recovery Scenario 1**

5. <input type="checkbox"/>	<b>Recover PMAC, TVOE Hosts, and Switch:</b> Backups available	<p>This step assumes TVOE and PMAC backups are available. If backups are <b>NOT</b> available, <b>skip this step</b>.</p> <ol style="list-style-type: none"> <li>1. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.</li> <li>2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup.</li> <li>3. Proceed to step 7.</li> </ol>
6. <input type="checkbox"/>	<b>Recover PMAC, TVOE Hosts, and Switch:</b> Backups NOT available	<p>This step assumes TVOE and PMAC backups are <b>NOT</b> available. If the TVOE and PMAC have already been restored, <b>skip this step</b>.</p> <p>Execute these procedures from reference [8]:</p> <ul style="list-style-type: none"> <li>• <b>Install and Configure TVOE on First RMS (PMAC Host)</b></li> <li>• <b>Install PMAC</b></li> <li>• <b>Initialize the PMAC Application</b></li> </ul>
7. <input type="checkbox"/>	Recover failed Cisco 4948 aggregation switches (HP DL380 only)	<p>Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 GEN 9, <b>skip this step</b>.</p> <p>Recover failed Cisco 4948 aggregation switches, if needed:</p> <ol style="list-style-type: none"> <li>1. Back up available configuration files. Refer to Appendix C Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only) to recover failed Cisco 4948 aggregation switches.</li> <li>2. Back up configuration files NOT available. Execute the <b>Configure Cisco 4948E-F Aggregation Switches (HP DL 380 Gen 8 Only)</b> section from reference [8].</li> </ol>
8. <input type="checkbox"/>	Configure PMAC (no backup)	<p>If PMAC backup was <b>NOT</b> restored in step 5. , execute this step; otherwise, skip this step.</p> <p>Execute these procedures from reference [8]:</p> <ul style="list-style-type: none"> <li>• <b>Configure PMAC Server (NetBackup Only)</b></li> <li>• <b>Add RMS to the PMAC Inventory</b></li> </ul>
9. <input type="checkbox"/>	Install/Configure additional rack mount servers	<ol style="list-style-type: none"> <li>1. Execute the <b>Install TVOE on Additional Rack Mount Servers</b> procedure from reference [8].</li> <li>2. <b>If backups are available</b>, restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.</li> </ol> <p><b>If backups are NOT available</b>, execute the <b>Configure TVOE on Additional Rack Mount Servers</b> procedure from reference [8].</p>
10. <input type="checkbox"/>	Configure BIOS settings and update firmware on additional rack mount servers	<ol style="list-style-type: none"> <li>1. Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]: <ul style="list-style-type: none"> <li>• <b>HP DL380 Gen8:</b> Configure HP Gen 8 Server BIOS Settings</li> <li>• <b>Oracle X5-2/Netra X5-2/X6-2/X7-2:</b> Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings</li> <li>• <b>HP DL380 Gen9:</b> Configure HP Gen9 Server BIOS Settings</li> </ul> </li> <li>2. Verify and/or upgrade server firmware by executing the <b>Upgrade Rack Mount Server Firmware</b> procedure from reference [8].</li> </ol>



**Procedure 1. Recovery Scenario 1**

11. <input type="checkbox"/>	Determine VM placement and socket pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 only)	HP DL380 GEN 8, <b>skip this step.</b> Determine VM placement and pinning by following: 1. Section 3.1, item 14; and 2. In reference [8], Appendix S VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1 Gbps NICs) and CPU Pinning in HP DL380 Gen 9 (Onboard 1 Gbps NICs) for Pinning Information on HP DL380 Gen 9.
12. <input type="checkbox"/>	Deploy redundant PMAC, if required	Refer to the <b>Deploy Redundant PMAC (Optional)</b> procedure to re-deploy and configure any redundant PMACs previously configured.
13. <input type="checkbox"/>	<b>PMAC:</b> Determine if the fdconfig file exists from the initial deployment	1. Type: <pre>[admusr@melbourne-pmac-1 ~]\$ ll /usr/TKLC/smac/etc/fdc/</pre> 2. Examine the results and verify if the <b>rms config file &lt;hostname&gt;.cfg</b> exists.  <b>Note:</b> There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS.
14. <input type="checkbox"/>	Create fdconfig backup file, if it does not already exist	Execute this step <b>ONLY</b> If the fdconfig backup file does <b>NOT</b> exist. 1. Create the needed file(s) by executing the <b>Virtual Machine/Network Fast Deployment</b> section from reference [8].  <div style="text-align: center;"><b>WARNING</b></div> <p style="color: red;">It is very important to ensure the file(s) created only affects the TVOE server(s) and the guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.</p> 2. Skip to step 23. if this step was executed.
15. <input type="checkbox"/>	<b>PMAC:</b> Load ISOs into PMAC, if not done already	If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the <b>Virtual Machine/Network Fast Deployment</b> section from reference [8].
16. <input type="checkbox"/>	<b>PMAC:</b> Edit/Update configuration file	Edit the fdconfig file to include only the required/failed servers. <b>Notes:</b> <ul style="list-style-type: none"> <li>Comment out configuration items that are not needed.</li> <li>Create a separate configuration file for EACH rack mount server being deployed.</li> <li>The Cabinet ID in the config file needs to match the cabinet already defined in PMAC.</li> </ul> The following items are mandatory: <ul style="list-style-type: none"> <li>siteName</li> <li>tpdlso</li> <li>dsrlso (if DSR VMs are being configured)</li> <li>sdsIso (if SDS VMs are being configured)</li> <li>NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured)</li> </ul>

**Procedure 1. Recovery Scenario 1**

		<ul style="list-style-type: none"> <li>• XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured)</li> <li>• XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured)</li> <li>• DSRNOAM1XMIIPADDRESS (if DSRNOAM1 is being configured)</li> <li>• DSRNOAM2XMIIPADDRESS (if DSRNOAM2 is being configured)</li> <li>• DSRDRNOAM1XMIIPADDRESS (if DSRDRNOAM1 is being configured)</li> <li>• DSRDRNOAM2XMIIPADDRESS (if DSRDRNOAM2 is being configured)</li> <li>• SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured)</li> <li>• SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured)</li> <li>• SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured)</li> <li>• SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured)</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].</li> <li>• Comment out SDS and DSR profile items if corresponding products are not used.</li> <li>• For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9, refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].</li> <li>• VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName.</li> <li>• VM locations should not be changed from their <b>RMSx</b> format. Each RMS should correspond to a separate rack mount server.</li> </ul> <p style="text-align: center;"><b>WARNING</b></p> <p>Ensure the file(s) created only affect the TVOE server(s) and guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.</p>
17.	<input type="checkbox"/> <b>PMAC:</b> Copy the backed up fdc file to the RMS directory	<p>Copy the fdconfig backup file to the RMS directory.</p> <pre>\$ sudo cp /usr/TKLC/smac/etc/fdc/&lt;backup_fdc_file&gt; /usr/TKLC/smac/etc/RMS/</pre>

**Procedure 1. Recovery Scenario 1**

18. <input type="checkbox"/>	<b>PMAC:</b> Execute the config.sh script	<p>Execute <b>config.sh</b> against the modified backup config file.</p> <p><b>Note:</b> If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>\$ sudo ./config.sh &lt;config file&gt;</pre> </div> <p>Example output:</p> <pre>[admusr@5010441PMAC RMS]\$ sudo ./config.sh rms.cfg Validating cfg file... Successful validation of cfg file. Added Cabinet 101 to Fast Deployment File. Added Zombie_TVOE1 to Fast Deployment File. Added Zombie_TVOE2 to Fast Deployment File. Added xmi(bond0.4) to Fast Deployment File. Added imi(bond0.3) to Fast Deployment File. Added rep(bond1.10) to Fast Deployment File. Added xsi1(bond1.6) to Fast Deployment File. Added xsi2(bond1.7) to Fast Deployment File. Added xsi3(bond1.8) to Fast Deployment File. Added xsi4(bond1.9) to Fast Deployment File. Added xsi5(bond1.11) to Fast Deployment File. Added xsi6(bond1.12) to Fast Deployment File. Added xsi7(bond1.13) to Fast Deployment File. Added xsi8(bond1.14) to Fast Deployment File. Added xsi9(bond1.15) to Fast Deployment File. Added xsi10(bond1.16) to Fast Deployment File. Added xsi11(bond1.17) to Fast Deployment File. Added xsi12(bond1.18) to Fast Deployment File. Added xsi13(bond1.19) to Fast Deployment File. Added xsi14(bond1.20) to Fast Deployment File. Added xsi15(bond1.21) to Fast Deployment File. Added xsi16(bond1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRDRNOAM1 to Fast Deployment File. Added Zombie_DSRDRNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSRNOAM1 to Fast Deployment File. Added Zombie_SDSRNOAM2 to Fast Deployment File. Added Zombie_DSRSOAM1 to Fast Deployment File. Added Zombie_DSRSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM1 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDAMP2 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_DSRIPFE2 to Fast Deployment File. Added Zombie_SSDPSV1 to Fast Deployment File. Added Zombie_SSDPSV2 to Fast Deployment File. Validating Fast Deployment File..... Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!! [admusr@5010441PMAC RMS]\$</pre>
---------------------------------	---	--

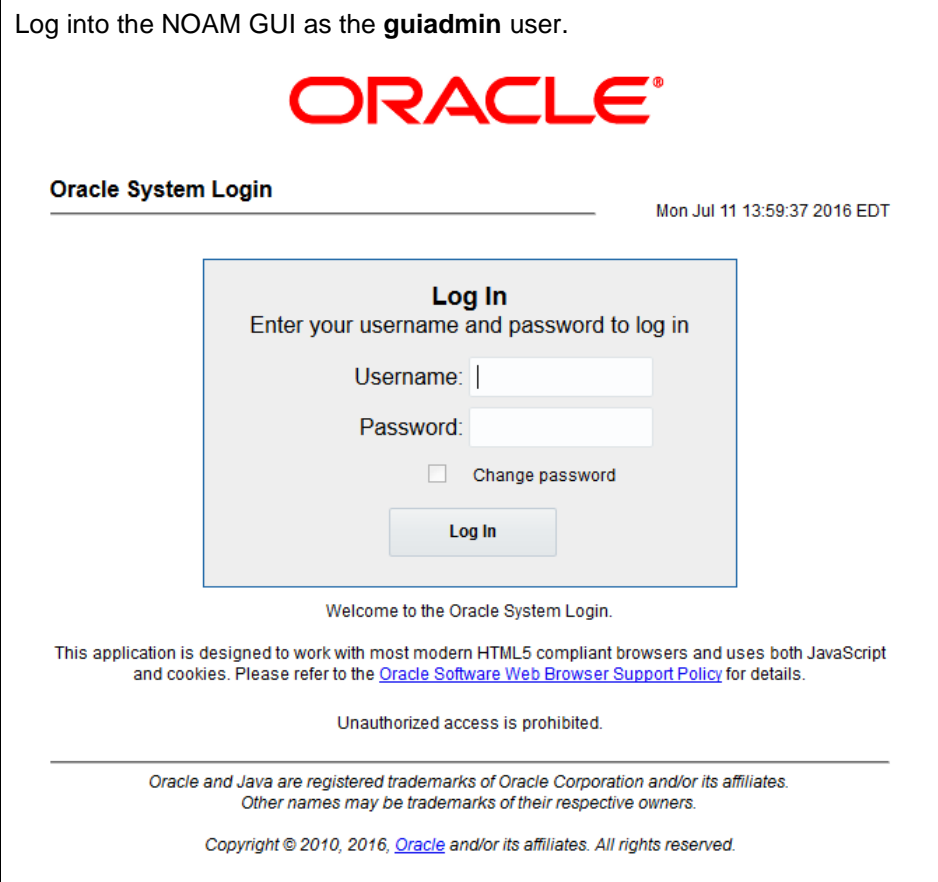
**Procedure 1. Recovery Scenario 1**

19. <input type="checkbox"/>	<b>PMAC:</b> Execute fast deployment	<div>With the file generated from the config.sh script, execute the following command to start fast deployment:</div> <div><pre>\$ screen \$ sudo fdconfig config --file=&lt;fd_config.xml&gt;</pre></div> <div><b>Note:</b> This is a long duration command. If the screen command was run before executing the fdconfig, perform a <b>screen -dr</b> to resume the screen session in the event of a terminal timeout, etc.</div>																																																															
20. <input type="checkbox"/>	<b>PMAC GUI:</b> Monitor the configuration	<div><div>1. If not already done, establish a GUI session on the PMAC server.</div><div>2. Navigate to <b>Task Monitoring</b>.</div><div></div><div>3. Monitor the configuration to completion:</div><div><div>Main Menu: Task Monitoring</div><div>Filter*</div><table><thead><tr><th>ID</th><th>Task</th><th>Target</th><th>Status</th><th>State</th><th>Task Output</th><th>Running Time</th><th>Start Time</th><th>Progress</th></tr></thead><tbody><tr><td>925</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_SDSRNOAM1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:04</td><td>2016-07-11 11:27:35</td><td>100%</td></tr><tr><td>924</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_SDSNOAM1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:04</td><td>2016-07-11 11:27:04</td><td>100%</td></tr><tr><td>923</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_DSRIPEE1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:06</td><td>2016-07-11 11:26:43</td><td>100%</td></tr><tr><td>922</td><td>Accept</td><td>RMS: pc5010439 Guest: Zombie_DSROAMP2</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:05</td><td>2016-07-11 11:26:43</td><td>100%</td></tr><tr><td>921</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_DSROAMP1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:05</td><td>2016-07-11 11:26:43</td><td>100%</td></tr><tr><td>920</td><td>Accept</td><td>RMS: pc5010439 Guest: Zombie_DSRSOAM2</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:06</td><td>2016-07-11 11:26:42</td><td>100%</td></tr></tbody></table></div><div><b>Note:</b> If a failure occurs with fdconfig, logs can be accessed in <b>/var/TKLC/log/fdconfig/fdconfig.log</b> file.</div><div><pre>[admusr@melbourne-pmac-1 fdconfig]\$ sudo fdconfig dumpsteps -- file=deploy_melbourne_20170329T202458_701b.fdcdb Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb" Here are the steps that were generated ----- begin ----- Dump of DB steps: NUM PHS DLY INFRA ID SVRTYPE CMD ELEMENT PRE STATE TO BGTS COMMAND TEXT ----- 1 1 0 pmac Fast_Deployment 0 21 0 Complete 300 0 Check PM&amp;C is available 2 1 0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet 3 1 0 pmac Fast_Deployment 0 3 melbourne_RMS3 1 Skipped 900 0 Add Rms 4 2 0 pmac Fast_Deployment 1</pre></div><div>4. Restart the fdconfig after a failure has occurred and has been resolved:</div><div><pre>\$ sudo fdconfig restart -- file=deploy_melbourne_20170329T202458_701b.fdcdb</pre></div></div>	ID	Task	Target	Status	State	Task Output	Running Time	Start Time	Progress	925	Accept	RMS: pc5010441 Guest: Zombie_SDSRNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:35	100%	924	Accept	RMS: pc5010441 Guest: Zombie_SDSNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:04	100%	923	Accept	RMS: pc5010441 Guest: Zombie_DSRIPEE1	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:43	100%	922	Accept	RMS: pc5010439 Guest: Zombie_DSROAMP2	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%	921	Accept	RMS: pc5010441 Guest: Zombie_DSROAMP1	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%	920	Accept	RMS: pc5010439 Guest: Zombie_DSRSOAM2	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:42	100%
ID	Task	Target	Status	State	Task Output	Running Time	Start Time	Progress																																																									
925	Accept	RMS: pc5010441 Guest: Zombie_SDSRNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:35	100%																																																									
924	Accept	RMS: pc5010441 Guest: Zombie_SDSNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:04	100%																																																									
923	Accept	RMS: pc5010441 Guest: Zombie_DSRIPEE1	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:43	100%																																																									
922	Accept	RMS: pc5010439 Guest: Zombie_DSROAMP2	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%																																																									
921	Accept	RMS: pc5010441 Guest: Zombie_DSROAMP1	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%																																																									
920	Accept	RMS: pc5010439 Guest: Zombie_DSRSOAM2	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:42	100%																																																									

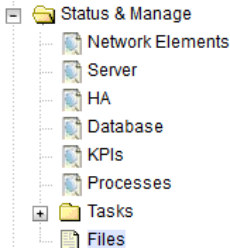
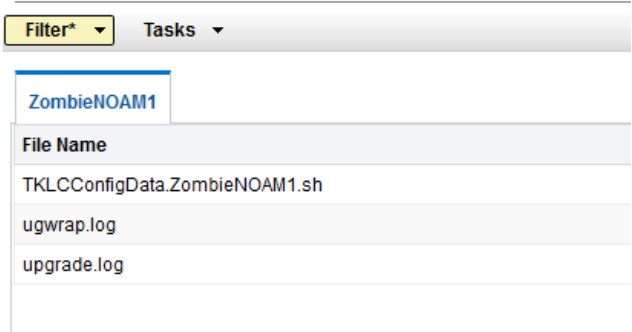
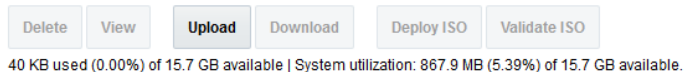
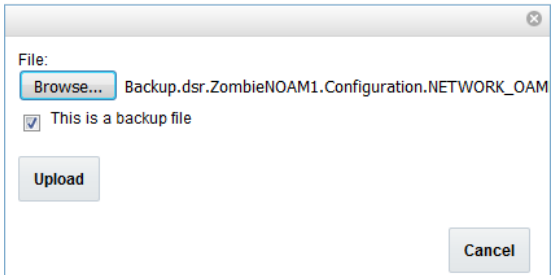
**Procedure 1. Recovery Scenario 1**

21. <input type="checkbox"/>	<b>PMAC:</b> Repeat for each rack mount server configuration file	Repeat steps 13. -20. for each rack mount server/configuration file, if required.
22. <input type="checkbox"/>	<b>PMAC:</b> Back up FDC file	<ol style="list-style-type: none"> <li>Copy the updated fdc file to the fdc backup directory:  <pre>\$ sudo cp /usr/TKLC/smac/etc/RMS/&lt;fdc_file&gt; /usr/TKLC/smac/etc/fdc/</pre> </li> <li>Change permissions:  <pre>\$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/&lt;fdc_file&gt;</pre> </li> </ol>
23. <input type="checkbox"/>	Perform CPU pinning	Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the <b>CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only)</b> procedure from reference [8].
24. <input type="checkbox"/>	Obtain latest database backup and network configuration data	<ol style="list-style-type: none"> <li>Obtain the most recent database backup file from external backup sources (for example, file servers) or tape backup sources.</li> <li>Obtain most recent <b>RADIUS shared secret encryption key</b> from the <b>DpiKf.bin.encr</b> file on external backup sources (only when the RADIUS key revocation MOP has been executed on the system).</li> <li>From required materials list in the Required Materials section, use the site survey documents and Network Element report (if available) to determine network configuration data.</li> </ol>
25. <input type="checkbox"/>	Execute DSR installation procedure for the first NOAM	<p>Verify the networking data for network elements.</p> <p><b>Notes</b></p> <ul style="list-style-type: none"> <li>Use the backup copy of network configuration data and site surveys from step 2.</li> <li>SDS disaster recovery actions can and should be worked simultaneously to allow faster recovery of the complete solution (that is, stale DB on DP servers do not receive updates until SDS-SOAM servers are recovered). The following steps accommodate both DSR and SDS disaster recovery steps.</li> </ul> <p><b>Important:</b> While creating the first NOAMs in this step, it is important that the server hostname is the same as one of the NOAM hostnames used prior to the disaster.</p> <p><b>DSR:</b></p> <ol style="list-style-type: none"> <li>Configure the first NOAM server by executing the <b>Configure First NOAM NE and Server</b> procedure from reference [8].</li> <li>Configure the NOAM server group by executing the <b>Configure the NOAM Server Group</b> procedure from reference [8].</li> </ol> <p><b>SDS:</b></p> <ol style="list-style-type: none"> <li>Configure the first SDS NOAM server by executing <b>Configure First SDS NOAM NE and Server</b> procedure from reference [8].</li> <li>Configure the SDS NOAM server group by executing the <b>Configure the SDS NOAM Server Group</b> procedure from reference [8].</li> <li>Skip to step 31.</li> </ol>

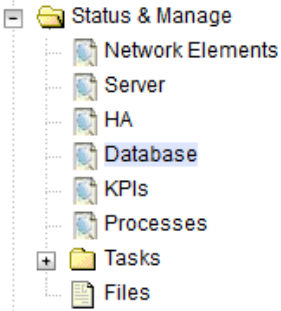


**Procedure 1. Recovery Scenario 1**

26.	<b>NOAM GUI:</b> Login <input type="checkbox"/> DSR only. If SDS, skip to step 31.	<p>Log into the NOAM GUI as the <b>guiadmin</b> user.</p> 
-----	---	---

**Procedure 1. Recovery Scenario 1**

<p>27. <input type="checkbox"/></p>	<p><b>NOAM GUI:</b> Upload the backup database file. DSR only. If SDS, skip to step 31.</p>	<ol style="list-style-type: none"> <li>Navigate to <b>Status &amp; Manage &gt; Files</b>.   </li> <li>Select the active NOAM server.  <b>Main Menu: Status &amp; Manage -&gt; Files</b>   </li> <li>Click <b>Upload</b> and select the <b>NO Provisioning and Configuration</b> file backed up after initial installation and provisioning.   </li> <li>Click <b>Browse</b> and locate the backup file.  <b>Note:</b> If there is no backup file, refer to Appendix L Backup Directory to create the backup directory. </li> <li>Click <b>Open</b>. </li> <li>Mark the <b>This is a backup file</b> checkbox. </li> <li>Click <b>Upload</b>.   </li> </ol> <p>The file takes a few seconds to upload depending on the size of the backup data. The file is visible on the list of entries after the upload is complete.</p>
-------------------------------------	---	--

**Procedure 1. Recovery Scenario 1**

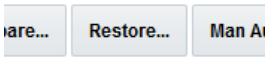
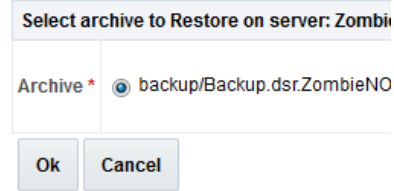
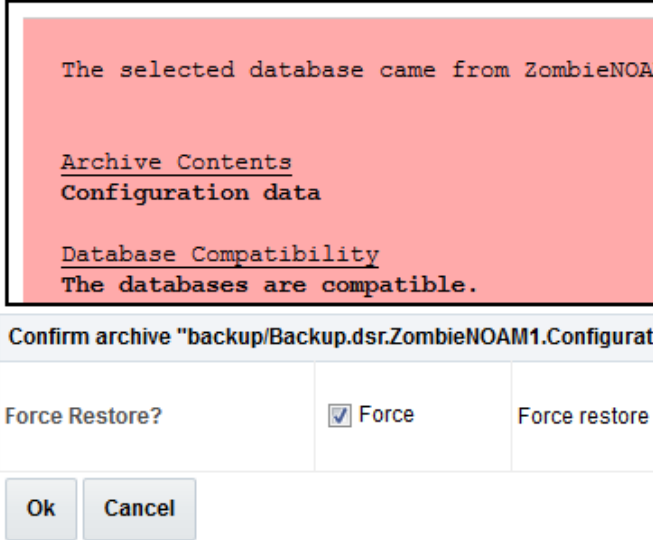
<p>28. <input type="checkbox"/></p>	<p><b>NOAM GUI:</b> Disable provisioning. DSR only. If SDS, skip to step 31.</p>	<p>1. Navigate to <b>Status &amp; Manage &gt; Database</b>.</p>  <p>2. Click <b>Disable Provisioning</b>.</p>  <p>3. Click <b>OK</b> to disable Provisioning.</p> 
-------------------------------------	--	--



**Procedure 1. Recovery Scenario 1**

<p>29. <input type="checkbox"/></p>	<p><b>NOAM GUI:</b> Verify the archive contents and database compatibility. DSR only. If SDS, skip to step 31.</p>	<ol style="list-style-type: none"> <li>1. Select the <b>Active NOAM</b> server and click <b>Compare</b>. <div data-bbox="527 310 922 352"> <div>lication</div> <div>Backup...</div> <div>Compare...</div> <div>Restore...</div> </div> </li> <li>2. Click the button for the restored database file uploaded as a part of step 27. of this procedure. <div data-bbox="539 466 740 489"> <p><b>Database Compare</b></p> </div> <div data-bbox="539 525 997 688"> <div>Select archive to compare on server: ZombieNOAM1</div> <div>Archive * <input type="radio"/> backup/Backup.dsr.ZombieNOAM1.Configuration</div> <div>Ok Cancel</div> </div> </li> <li>3. <b>Verify</b> the output window matches the screen below. <p><b>Note:</b> A database mismatch regarding the Topology Compatibility and possibly User compatibility (due to authentication) display. These warnings are expected. If these are the only mismatches, proceed; otherwise, stop and contact My Oracle Support (MOS) to ask for assistance.</p> <div data-bbox="527 947 1448 1350"> <p><b>Database Archive Compare</b></p> <pre> The selected database came from ZombieNOAM1 on 10/10/2016 at 10:36:44 EDT and contains the following:  Archive Contents Configuration data  Database Compatibility The databases are compatible.  Node Type Compatibility The node types are compatible.  Topology Compatibility THE TOPOLOGY IS NOT COMPATIBLE.  CONTACT ORACLE CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE. Discrepancies: - Server A1860.052 on network XMI is in the current topology but not the selected backup file. - Server A1860.052 on network IMI is in the current topology but not the selected backup file. - Server A0630.238 on network XMI is in the selected backup file but not the current topology. - Server B2934.011 on network XMI is in the selected backup file but not the current topology. - Server C0422.200 on network XMI is in the selected backup file but not the current topology. </pre> </div> <p><b>Note:</b> Archive Contents and Database Compatibilities must be the following:</p> <p><b>Archive Contents:</b> Configuration data.</p> <p><b>Database Compatibility:</b> The databases are compatible.</p> <p><b>Note:</b> The following is expected output for Topology Compatibility Check since we are restoring from an existing backed up database to a database with just one NOAM:</p> <p><b>Topology Compatibility</b></p> <p>THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.</p> <p><b>Note:</b> We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility.</p> </li> <li>4. If the verification is successful, click <b>Back</b> and continue to <b>next step</b> in this procedure.</li> </ol>
-------------------------------------	--	--

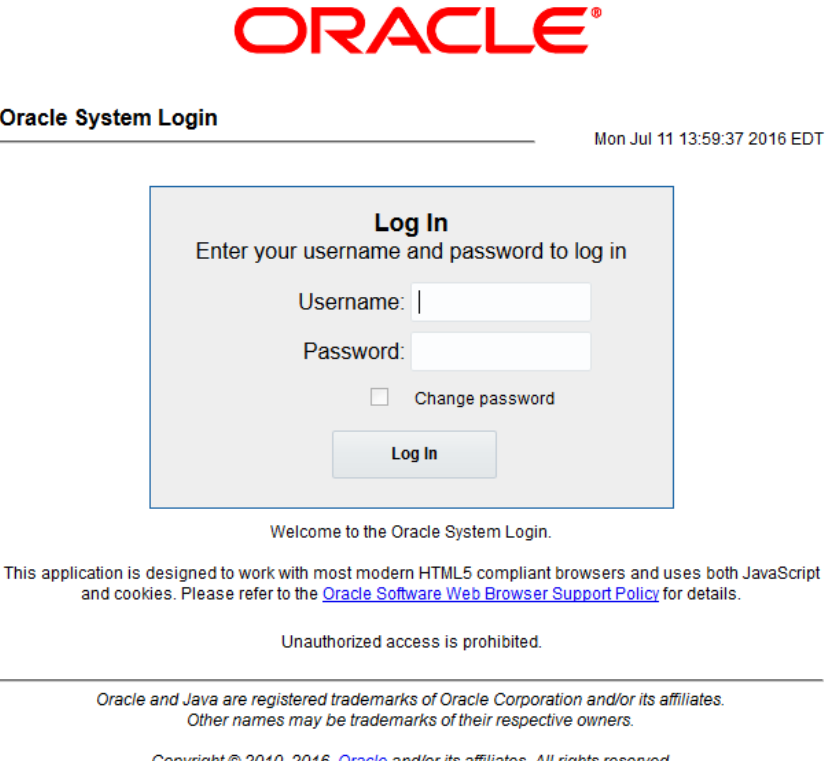
**Procedure 1. Recovery Scenario 1**

<p>30. <input type="checkbox"/></p>	<p><b>Active NOAM:</b> Restore the database. DSR only. If SDS, skip to step 31.</p>	<ol style="list-style-type: none"> <li>From <b>Status &amp; Manage &gt; Database</b>.</li> <li>Select the active NOAM server and click Restore.</li> </ol>  <ol style="list-style-type: none"> <li>Select the proper backup provisioning and configuration file.</li> </ol>  <ol style="list-style-type: none"> <li>Click OK.</li> <li>If you get errors related to the warnings highlighted in the previous step, then it is expected. If no other errors display, then mark the <b>Force</b> checkbox and click <b>OK</b> to proceed with the DB restore.</li> </ol> <p><b>Database Restore Confirm</b></p> <p>Incompatible archive selected</p>  <p><b>Note:</b> After the restore has started, the user is logged out of the XMI NO GUI since the restored topology is old data.</p> <ol style="list-style-type: none"> <li>Go to step 37.</li> </ol>
-------------------------------------	---	---

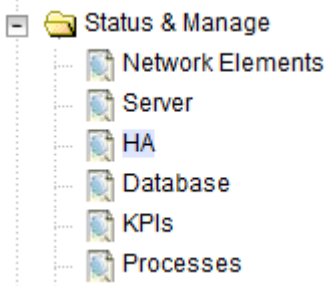
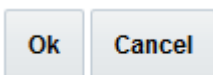
**Procedure 1. Recovery Scenario 1**

31. <input type="checkbox"/>	<b>SDS NOAM:</b> Transfer SDS configuration and provisioning backup database files.  SDS only. If DSR, skip to step 37.	<p>Using the IP of the recovered SDS NOAM, transfer the uncompressed backup database files to the <b>/var/TKLC/db/filemgmt</b> directory.</p> <p><b>Linux:</b></p> <ol style="list-style-type: none"> <li>From the command line of a Linux machine, copy the configuration backup file to the SDS NOAM guest: <div data-bbox="581 432 1435 508" style="border: 1px solid black; padding: 5px;"> <pre># scp &lt;path_to_configuration_db_file&gt; admusr@&lt;SDS_NOAM_IP&gt;:/var/TKLC/db/filemgmt</pre> </div> </li> <li>From the command line of a Linux machine, copy the provisioning backup file to the SDS NOAM guest: <div data-bbox="581 594 1435 669" style="border: 1px solid black; padding: 5px;"> <pre># scp &lt;path_to_provisioning_db_file&gt; admusr@&lt;SDS_NOAM_IP&gt;:/var/TKLC/db/filemgmt</pre> </div> </li> </ol> <p>where <b>&lt;path_to_db_file&gt;</b> is the path to the backup database file on the local system and <b>&lt;SDS_NOAM_IP&gt;</b> is the recovered SDS NOAM IP address.</p> <p><b>Windows:</b></p> <p>Use WinSCP to copy the backup database files into the <b>/var/TKLC/db/filemgmt</b> directory. Refer to the <b>Using WinSCP</b> procedure in reference [9] to copy the backup image to the customer system.</p>
32. <input type="checkbox"/>	<b>SDS NOAM:</b> Login. SDS only. If DSR, skip to step 37.	Establish an SSH session to the SDS active NOAM XMI IP address and login as <b>admusr</b> .
33. <input type="checkbox"/>	<b>SDS NOAM:</b> Stop running applications. SDS only. If DSR, skip to step 37.	<p>Issue the following command to stop running applications. Leave database running:</p> <div data-bbox="532 1144 1339 1192" style="border: 1px solid black; padding: 5px;"> <pre>\$ sudo prod.stop --ignore-cap</pre> </div> <p><b>Note:</b> This step may take several minutes to complete.</p>
34. <input type="checkbox"/>	<b>SDS NOAM:</b> Restore configuration database. SDS only. If DSR, skip to step 37.	<p>Restore the configuration DB by executing the following command:</p> <div data-bbox="532 1304 1435 1379" style="border: 1px solid black; padding: 5px;"> <pre>\$ sudo idb.restore -n -t /var/TKLC/db/filemgmt -v &lt;full path to configuration archive file name&gt;</pre> </div>
35. <input type="checkbox"/>	<b>SDS NOAM:</b> Restore provisioning database. SDS only. If DSR, skip to step 37.	Refer to Appendix I Restore Provisioning Database to restore the provisioning database.
36. <input type="checkbox"/>	<b>SDS NOAM:</b> Start running applications. SDS only. If DSR, skip to step 37.	<p>Start the SDS application by executing the following command:</p> <div data-bbox="532 1717 1339 1766" style="border: 1px solid black; padding: 5px;"> <pre>\$ sudo prod.start</pre> </div>

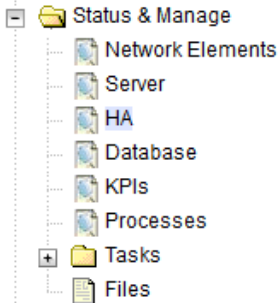
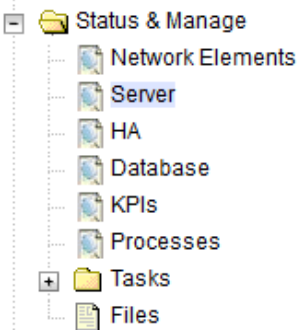

**Procedure 1. Recovery Scenario 1**

37. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Login	<ol style="list-style-type: none"> <li>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  <div style="border: 1px solid black; padding: 2px; margin: 5px 0;">http://&lt;Primary_NOAM_VIP_IP_Address&gt;</div> </li> <li>2. Login as the <b>guiadmin</b> user:</li> </ol> <div style="text-align: center; margin: 20px 0;">  <p>The screenshot shows the Oracle System Login page. At the top is the Oracle logo in red. Below it is the title 'Oracle System Login' and a timestamp 'Mon Jul 11 13:59:37 2016 EDT'. In the center is a 'Log In' box with the text 'Enter your username and password to log in'. Inside this box are fields for 'Username:' and 'Password:', a 'Change password' checkbox, and a 'Log In' button. Below the box is a welcome message, a note about browser compatibility, a prohibition on unauthorized access, and copyright information at the bottom.</p> </div>
38. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Monitor and confirm database restore	<ol style="list-style-type: none"> <li>1. Wait for <b>5-10 minutes</b> for the system to stabilize with the new topology:</li> <li>2. Monitor the Info tab for <b>Success</b>. This indicates the restore is complete and the system is stabilized.</li> </ol> <p>Ignore these alarms for NOAM and MP servers until all the servers are configured:</p> <ul style="list-style-type: none"> <li>• Alarms with Type Column as <b>REPL, COLL, HA</b> (with mate NOAM), <b>DB</b> (about Provisioning Manually Disabled).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Do not pay attention to alarms until all the servers in the system are completely restored.</li> <li>• The Configuration and Maintenance information is in the same state it was when backed up during initial backup.</li> </ul>

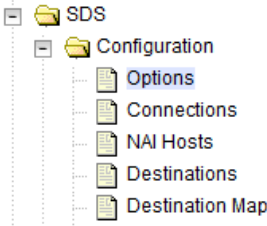




**Procedure 1. Recovery Scenario 1**

39. <input type="checkbox"/>	<b>Active NOAM:</b> Set failed servers to OOS	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>2. Click <b>Edit</b>.</li> <li>3. Set the Max Allowed HA Role option to <b>OOS</b> for the failed servers.  <b>Modifying HA attributes</b>  <table border="1" data-bbox="535 756 1071 1102"> <thead> <tr> <th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td><td>Active</td><td>The maximum des</td></tr> <tr> <td>ZombieNOAM2</td><td>OOS</td><td>The maximum des</td></tr> <tr> <td>ZombieDRNOAM1</td><td>OOS</td><td>The maximum des</td></tr> </tbody> </table> </li> <li>4. Click <b>OK</b>.   </li> </ol>	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active	The maximum des	ZombieNOAM2	OOS	The maximum des	ZombieDRNOAM1	OOS	The maximum des
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active	The maximum des												
ZombieNOAM2	OOS	The maximum des												
ZombieDRNOAM1	OOS	The maximum des												
40. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover standby NOAM	<p>Install the second NOAM server:</p> <p><b>DSR:</b> Execute the <b>Configure the Second NOAM Server</b> procedure, steps 1 and 3-6, from reference [8].</p> <p><b>SDS:</b> Execute the <b>Configure the Second SDS NOAM Server</b> procedure, steps 1 and 3-6, from reference [8].</p>												
41. <input type="checkbox"/>	Install NetBackup client (optional)	If NetBackup is used, execute the <b>Install NetBackup Client (Optional)</b> procedure from reference [8].												

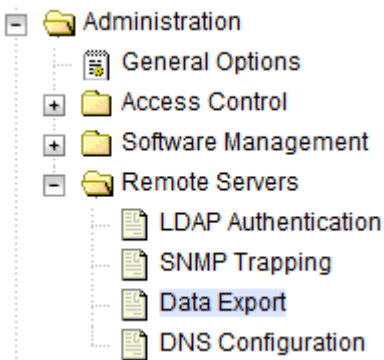

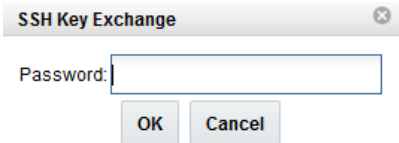
**Procedure 1. Recovery Scenario 1**

42. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set HA on standby NOAM	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>2. Click <b>Edit</b>.</li> <li>3. Select the standby NOAM server and set it to <b>Active</b>.  <b>Modifying HA attributes</b>  <table border="1" data-bbox="542 764 1015 1037"> <thead> <tr> <th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td><td>Active</td><td>The maximum</td></tr> <tr> <td>ZombieNOAM2</td><td>Active</td><td>The maximum</td></tr> <tr> <td>ZombieDRNOAM1</td><td>Active Standby Snare</td><td>The maximum</td></tr> </tbody> </table> </li> <li>4. Click <b>OK</b>.</li> </ol>	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active	The maximum	ZombieNOAM2	Active	The maximum	ZombieDRNOAM1	Active Standby Snare	The maximum
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active	The maximum												
ZombieNOAM2	Active	The maximum												
ZombieDRNOAM1	Active Standby Snare	The maximum												
43. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Restart DSR application	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.   </li> <li>2. Select the recovered standby NOAM server and click <b>Restart</b>.   </li> </ol>												
44. <input type="checkbox"/>	<b>Active NOAM:</b> Correct the recognized authority table	<ol style="list-style-type: none"> <li>1. Establish an SSH session to the active NOAM and login as <b>admusr</b>.</li> <li>2. Execute this command:  <pre data-bbox="542 1703 1435 1892"> \$ sudo top.setPrimary - Using my cluster: A1789 - New Primary Timestamp: 11/09/15 20:21:43.418 - Updating A1789.022: &lt;DSR_NOAM_B_hostname&gt; - Updating A1789.144: &lt;DSR_NOAM_A_hostname&gt; </pre> </li> </ol>												

**Procedure 1. Recovery Scenario 1**

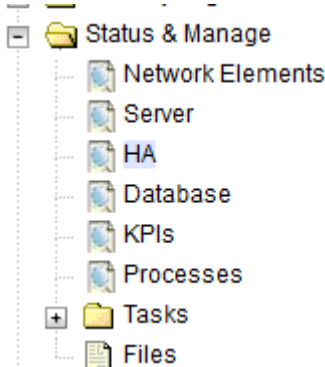
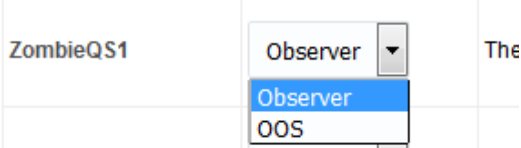
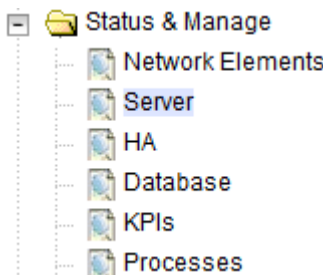


<p>45. <input type="checkbox"/> <b>NOAM VIP GUI:</b> Perform Keyexchange with remote import server. SDS only. If DSR, skip to step 47.</p>		<ol style="list-style-type: none"> <li>1. Navigate to <b>SDS &gt; Configuration &gt; Options</b>.   </li> <li>2. Unmark the <b>Remote Import Enabled</b> checkbox.   </li> <li>3. Click <b>Apply</b>.  <b>Note:</b> Navigate to <b>SDS &gt; Configuration &gt; Options</b> again to clear the banner. </li> <li>4. Enter the <b>Remote Import Password</b>.   </li> <li>5. Click <b>Apply</b>.     <b>Note:</b> Navigate to <b>SDS &gt; Configuration &gt; Options</b> again to clear the banner. </li> <li>6. Mark the <b>Remote Import Enabled</b> checkbox.   </li> </ol>
<p>46. <input type="checkbox"/> <b>NOAM VIP GUI:</b> Repeat for remote export server. SDS only. If DSR, skip to step 47.</p>		<p>Repeat step 45. for the remote export server.</p>

**Procedure 1. Recovery Scenario 1**

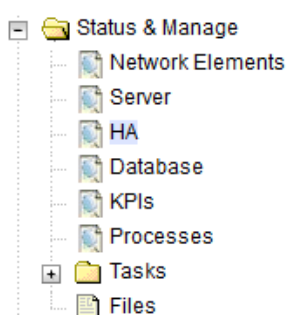
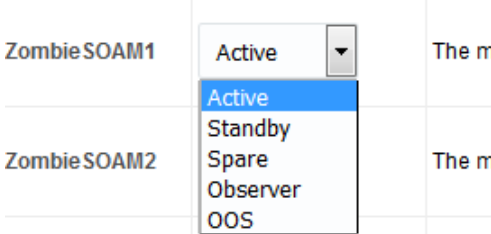
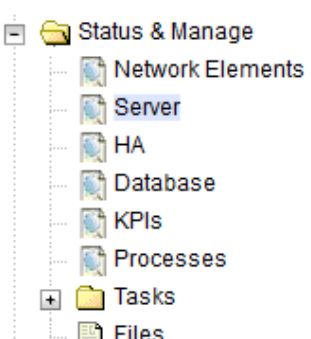
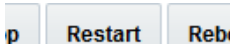
47. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Perform Keyexchange with export server	<ol style="list-style-type: none"> <li>1. Navigate to <b>Administration &gt; Remote Servers &gt; Data Export</b>.   </li> <li>2. Click <b>SSH Key Exchange</b>.   </li> <li>3. Type the <b>Password</b> and click <b>OK</b>.   </li> </ol>
48. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover query servers.  SDS only. If DSR, skip to step 51.	Execute the <b>Configuring SDS Query Servers</b> procedure, steps 1 and 4-7, from reference [8].



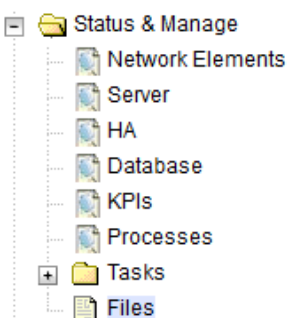
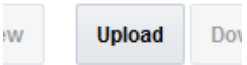
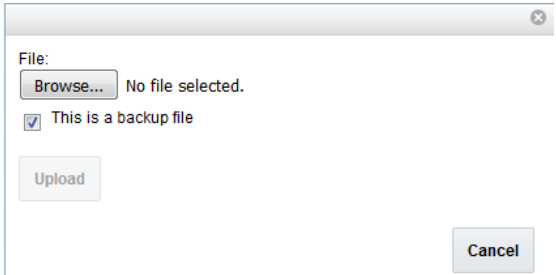
**Procedure 1. Recovery Scenario 1**

49. <input type="checkbox"/>	<b>SDS NOAM VIP GUI:</b> Set HA on query server. SDS only. If DSR, skip to step 51.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>2. Click <b>Edit</b>.</li> <li>3. Select the query server and select <b>Observer</b>.   </li> <li>4. Click <b>OK</b>.</li> </ol>
50. <input type="checkbox"/>	<b>SDS NOAM VIP GUI:</b> Restart SDS application. SDS only. If DSR, skip to step 51.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.   </li> <li>2. Select the recovered query server and click <b>Restart</b>.   </li> </ol>
51. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Stop replication to the C-level servers of this site. DSR only. If SDS, skip to step next step. 	<p style="text-align: center;"><b>Warning</b></p> <p>Before continuing this procedure, replication to C-level servers <b>MUST</b> be inhibited at the SOAM site being recovered.</p> <p>Failure to inhibit replication to the working C-level servers results in the database being destroyed!</p> <p><b>If the spare SOAM is also present in the site and lost</b>, execute Appendix E Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost) to inhibit replication to working C-level servers before continuing.</p> <p><b>If the spare SOAM is NOT deployed in the site</b>, execute Appendix C Inhibit A and B Level Replication on C-level Servers to inhibit replication to working C-level servers before continuing.</p>


**Procedure 1. Recovery Scenario 1**

52. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover active SOAM server	<p>Install the SOAM servers.</p> <p><b>DSR:</b> Execute the <b>Configure the SOAM Servers</b> procedure, steps 1-3 and 5-9, from reference [8].</p> <p><b>Note:</b> If you are using NetBackup, also execute step 12.</p> <p><b>SDS:</b> Execute the <b>Configure the SDS DP SOAM Servers</b> procedure, steps 1-3 and 5-8, from reference [8].</p>
53. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set HA on the SOAM server	<p>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.</p>  <p>2. Click <b>Edit</b>.</p> <p>3. Select the SOAM server and set it to <b>Active</b>.</p>  <p>4. Click <b>OK</b>.</p>
54. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Restart DSR application	<p>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.</p>  <p>2. Select the recovered NOAM server and click <b>Restart</b>.</p> 

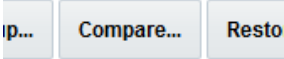
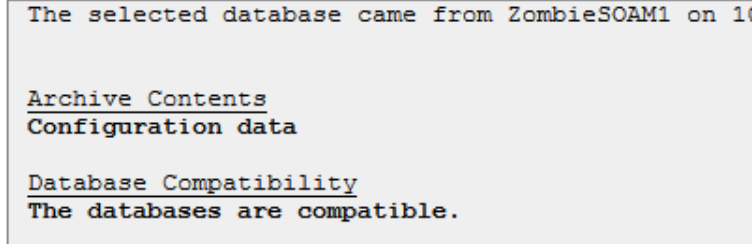
**Procedure 1. Recovery Scenario 1**

<p>55. <input type="checkbox"/></p>	<p><b>NOAM VIP GUI:</b> Upload the backup SOAM database file. DSR only. If SDS, skip to step 60.</p>	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Files</b>.   </li> <li>2. Select the active SOAM server tab. Click <b>Upload</b> and select the file <b>SO Provisioning and Configuration</b> file backed up after initial installation and provisioning.   </li> <li>3. Click <b>Browse</b> and locate the backup file.</li> <li>4. Mark the <b>This is a backup file</b> checkbox.</li> <li>5. Click <b>Open</b>.</li> <li>6. Click <b>Upload</b>.   </li> </ol> <p>The file takes a few seconds to upload depending on the size of the backup data and displays on the list of entries when it has completed the upload.</p>
-------------------------------------	--	--

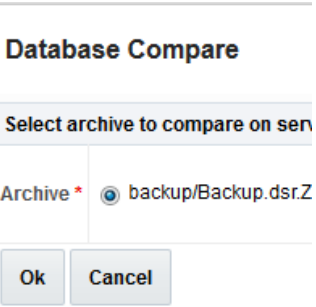
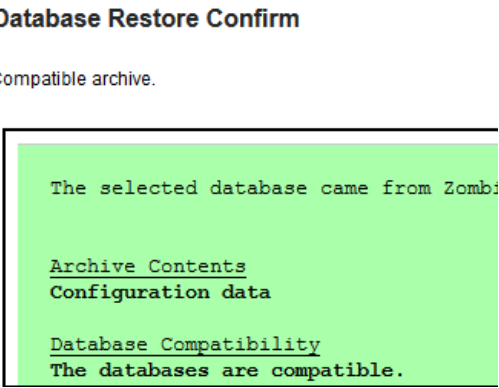
**Procedure 1. Recovery Scenario 1**

56. <input type="checkbox"/>	<b>Recovered SOAM GUI:</b> Login. DSR only. If SDS, skip to step 60.	<ol style="list-style-type: none"> <li>1. Establish a GUI session on the recovered SOAM server.</li> <li>2. Open the web browser and enter a URL of:  <div data-bbox="576 336 1380 388" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> http://&lt;Recovered_SOAM_IP_Address&gt; </div> </li> <li>3. Login as the <b>guiadmin</b> user:</li> </ol> <div data-bbox="535 451 1461 1186">  </div>
------------------------------	---	--


**Procedure 1. Recovery Scenario 1**

57. <input type="checkbox"/>	<p><b>Recovered SOAM GUI:</b> Verify the archive contents and database compatibility.</p> <p>DSR only. If SDS, skip to step 60.</p>	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Database</b>.</li> <li>2. Select the <b>Active SOAM</b> server and click <b>Compare</b>.</li> </ol>  <ol style="list-style-type: none"> <li>3. Click the button for the restored database file uploaded as a part of step 27. of this procedure.</li> </ol> <p><b>Database Compare</b></p> <p>Select archive to compare on server: 2</p> <p>Archive * <input checked="" type="radio"/> backup/Backup.DSR.Zom</p> <p>Ok Cancel</p> <ol style="list-style-type: none"> <li>4. Verify the output window matches the screen below.</li> </ol> <p><b>Database Archive Compare</b></p>  <p><b>Note:</b> Archive Contents and Database Compatibilities must be the following:</p> <p><b>Archive Contents:</b> Configuration data.</p> <p><b>Database Compatibility:</b> The databases are compatible.</p> <p><b>Note:</b> The following is expected output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM:</p> <p><b>Topology Compatibility</b></p> <p>THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.</p> <p><b>Note:</b> We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility.</p> <ol style="list-style-type: none"> <li>5. If the verification is successful, click <b>Back</b> and continue to <b>next step</b> in this procedure.</li> </ol>
------------------------------	---	--

**Procedure 1. Recovery Scenario 1**

58. <input type="checkbox"/>	<b>Recovered SOAM GUI:</b> Restore the database. DSR only. If SDS, skip to step 60.	<ol style="list-style-type: none"> <li>1. Select the <b>Active SOAM</b> server and click <b>Restore</b>.</li> <li>2. Select the backup provisioning and configuration file.</li> </ol>  <ol style="list-style-type: none"> <li>3. Click <b>OK</b>.</li> </ol>  <ol style="list-style-type: none"> <li>4. If the Node Type Compatibility error displays, it is expected. If no other errors display, mark the <b>Force</b> checkbox and click <b>OK</b> to proceed with the DB restore.</li> </ol> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• After the restore has started, the user is logged out of XMI SOAM GUI since the restored topology is old data.</li> <li>• If the spare SOAM is in another network and is unreachable, the database restore cannot be done.</li> </ul> <p><b>Workaround:</b> If the spare SOAM is unreachable and ping (from recovered SOAM server to spare SOAM server) hangs (as evidenced by <b>ps -ef   grep ping</b> showing the same ping process and its child for more than 10 seconds), then kill the hung ping processes and the restore proceeds.</p>
59. <input type="checkbox"/>	<b>Recovered SOAM GUI:</b> Monitor and confirm database restoral. DSR only. If SDS, skip to step 60.	<p>Wait for <b>5-10 minutes</b> for the system to stabilize with the new topology: Monitor the Info tab for <b>Success</b>. This indicates the restore is complete and the system is stabilized.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Do not pay attention to alarms until all the servers in the system are completely restored.</li> <li>• The Configuration and Maintenance information is in the same state it was when backed up during initial backup.</li> </ul>

**Procedure 1. Recovery Scenario 1**

60. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Login	<ol style="list-style-type: none"> <li>Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  <div style="border: 1px solid black; padding: 2px; margin: 5px 0;">http://&lt;Primary_NOAM_VIP_IP_Address&gt;</div> </li> <li>Login as the <b>guiadmin</b> user:</li> </ol> 
61. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover the remaining SOAM servers (standby, spare)	<p><b>DSR:</b>          Execute the <b>Configure the SOAM Servers</b> procedure, steps 1-3 and 5-9, from reference [8].</p> <p><b>Note:</b> If you are using NetBackup, also execute step 12.</p> <p><b>SDS:</b>          Execute the <b>Configure the SDS DP SOAM Servers</b> procedure, steps 1-3 and 5-8, from reference [8].</p>

Procedure 1. Recovery Scenario 1

62.	<div><div></div><div>NOAM VIP GUI: Set HA on SOAM server</div></div>	<div><div><div>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.</div><div><div><div></div><div>Status &amp; Manage</div><div><div>Network Elements</div><div>Server</div><div>HA</div><div>Database</div><div>KPIs</div><div>Processes</div><div>Tasks</div><div>Files</div></div></div></div></div><div><div>2. Click <b>Edit</b>.</div><div>3. Select the SOAM server and set it to <b>Active</b>.</div><div><div><div>ZombieSOAM1</div><div>Active</div><div>The m</div></div><div><div>ZombieSOAM2</div><div>Active</div><div>The m</div></div></div><div><div>4. Click <b>OK</b>.</div></div></div></div>
-----	--	--



**Procedure 1. Recovery Scenario 1**

63.

**NOAM VIP GUI:**

Start replication on working C-level servers.

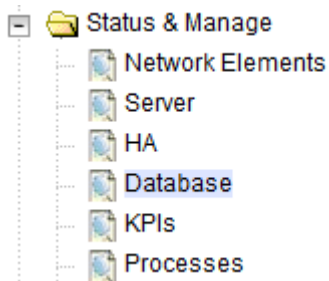
DSR only. If SDS, skip to next step.

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

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

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

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



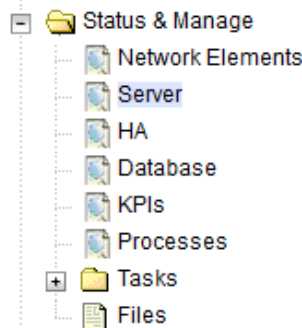

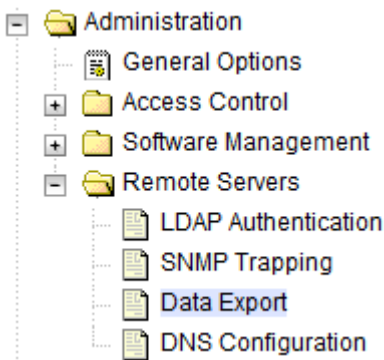
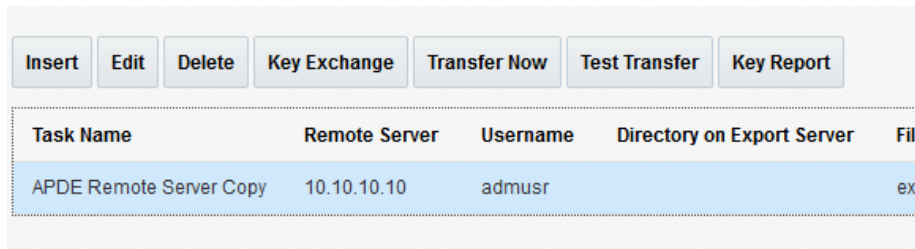
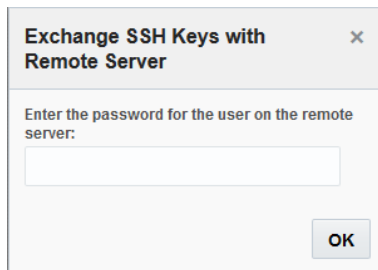
2. If the **Repl Status** is set to **Inhibited**, click **Allow Replication** using this order; otherwise, if none of the servers are inhibited, skip this step and continue with the next step:

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

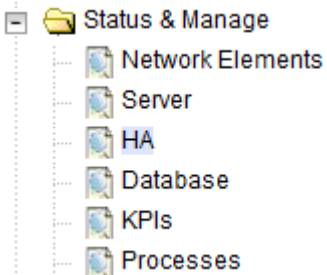
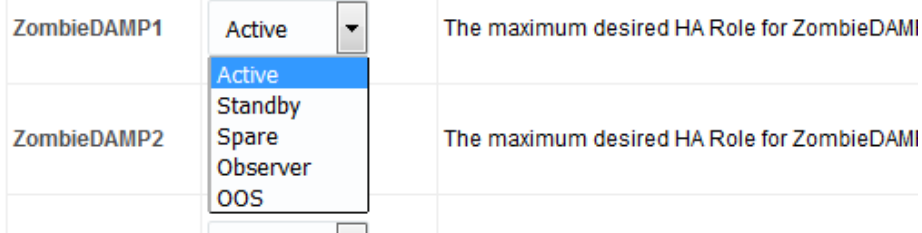
3. Verify the replication on all the working servers is allowed. This can be done by examining the Repl Status table.

OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
NotApplicable	NotApplicable	Allowed	NotApplicable
Normal	NotApplicable	Allowed	NotApplicable
Normal	NotApplicable	Allowed	NotApplicable
Normal	NotApplicable	Allowed	NotApplicable

**Procedure 1. Recovery Scenario 1**

64.	<b>NOAM VIP GUI:</b> Restart DSR application	<div>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.</div> <div></div> <div>2. Select the recovered standby NOAM server and click <b>Restart</b>.</div> <div></div>										
65.	<b>NOAM VIP GUI:</b> Perform Keyexchange with export server	<div>1. Navigate to <b>Administration &gt; Remote Servers &gt; Data Export</b>.</div> <div></div> <div>2. Click the <b>Task Name</b> and click <b>Key Exchange</b>.</div> <div><table><tr><th>Task Name</th><th>Remote Server</th><th>Username</th><th>Directory on Export Server</th><th>File</th></tr><tr><td>APDE Remote Server Copy</td><td>10.10.10.10</td><td>admusr</td><td></td><td>ex</td></tr></table></div> <div>3. Type the <b>Password</b> and click <b>OK</b>.</div> <div></div>	Task Name	Remote Server	Username	Directory on Export Server	File	APDE Remote Server Copy	10.10.10.10	admusr		ex
Task Name	Remote Server	Username	Directory on Export Server	File								
APDE Remote Server Copy	10.10.10.10	admusr		ex								

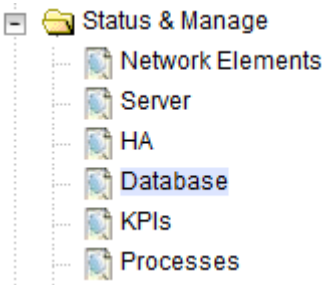
**Procedure 1. Recovery Scenario 1**

66. <input type="checkbox"/>	Activate PCA feature. DSR only	<p>If you have PCA installed in the system being recovered, re-activate PCA by executing the <b>PCA Activation on Entire Network</b> procedure on the recovered NOAM server from [7].</p> <p><b>Note:</b> If not all SOAM sites are recovered at this point, then repeat the activation for each “new” SOAM site that comes online.</p>
67. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover the C-level server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs	<p><b>DSR:</b> Execute the <b>Configure the MP Servers</b> procedure, steps 1 and 9-13, from reference [8].</p> <p><b>Note:</b> Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.</p> <p><b>SDS</b> (Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only): Execute the <b>Configure the SDS DP Servers</b> procedure, steps 1 and 5-8, from reference [8].</p> <p>Repeat this step for any remaining failed MP servers.</p>
68. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set HA on all C-level servers	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage -&gt; HA</b>.   </li> <li>2. Click <b>Edit</b>.</li> <li>3. For each recovered C-Level with a Max Allowed HA Role set to <b>OOS</b>, set it to <b>Active</b>.   </li> <li>4. Click <b>OK</b>.</li> </ol>

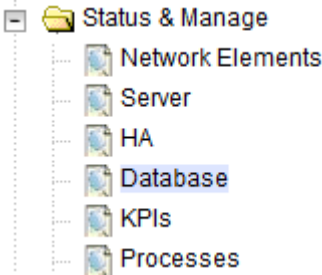

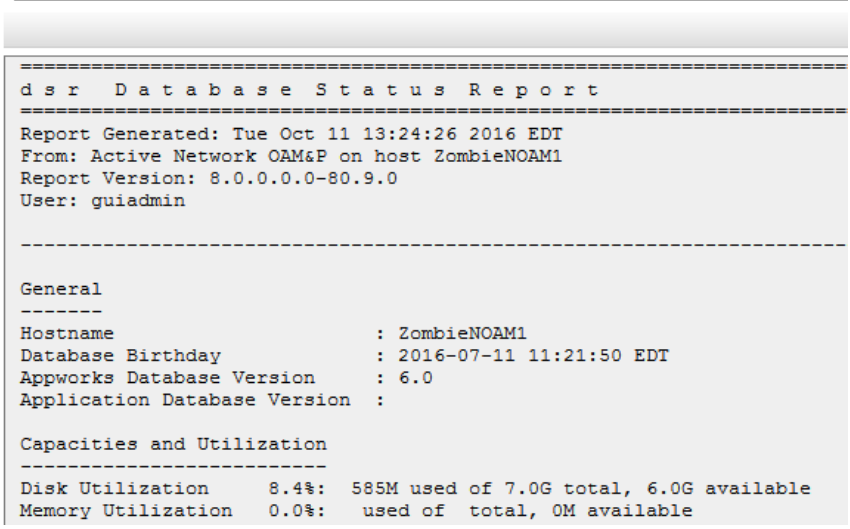
Procedure 1. Recovery Scenario 1

<div>69.</div> <div><input type="checkbox"/></div>	<p><b>NOAM VIP GUI:</b> Restart DSR application on the recovered C-level servers</p>	<div><div>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.</div><div><div><div><div></div></div><div>Status &amp; Manage</div><div><div></div></div><div>Network Elements</div><div><div></div></div><div>Server</div><div><div></div></div><div>HA</div><div><div></div></div><div>Database</div><div><div></div></div><div>KPIs</div><div><div></div></div><div>Processes</div></div></div></div> <div><div>2. Select the recovered C-level servers and click <b>Restart</b>.</div><div><div><div>p</div><div>Restart</div><div>Rebo</div></div></div></div>
--	--	--

**Procedure 1. Recovery Scenario 1**

70. <div></div>	<p><b>NOAM VIP GUI:</b> Start replication on all C-Level servers. DSR only. If SDS, then skip to next step.</p>	<p>Un-Inhibit (start) replication to the <b>ALL</b> C-level servers.</p> <p>1. Navigate to <b>Status &amp; Manage &gt; Database</b>.</p> <div></div> <p>2. If the <b>Repl Status</b> is set to <b>Inhibited</b>, click <b>Allow Replication</b> using this order:</p> <ul style="list-style-type: none"><li>• Active NOAMP Server</li><li>• Standby NOAMP Server</li><li>• Active SOAM Server</li><li>• Standby SOAM Server</li><li>• Spare SOAM Server (<b>if applicable</b>) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only)</li><li>• Active DR NOAM Server</li><li>• Standby DR NOAM Server</li><li>• MP/IPFE Servers</li><li>• SBRS (if SBR servers are configured, start with the active SBR, then standby, then spare) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only</li></ul> <p>3. Verify the replication on all servers is allowed. This can be done by checking the <b>Repl Status</b>.</p> <table><tr><th>OAM Repl Status</th><th>SIG Repl Status</th><th>Repl Status</th><th>Repl Audit Status</th></tr><tr><td>NotApplicable</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr></table>	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status	NotApplicable	NotApplicable	Allowed	NotApplicable	Normal	NotApplicable	Allowed	NotApplicable	Normal	NotApplicable	Allowed	NotApplicable	Normal	NotApplicable	Allowed	NotApplicable
OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status																			
NotApplicable	NotApplicable	Allowed	NotApplicable																			
Normal	NotApplicable	Allowed	NotApplicable																			
Normal	NotApplicable	Allowed	NotApplicable																			
Normal	NotApplicable	Allowed	NotApplicable																			
71. <div></div>	<p><b>Active NOAM:</b> Perform keyexchange between the active-NOAM and recovered servers</p>	<p>1. Establish an SSH session to the active NOAM and login as <b>admusr</b>.</p> <p>2. Perform a keyexchange from the active NOAM to each recovered server:</p> <div><pre>\$ keyexchange admusr@&lt;Recovered Server Hostname&gt;</pre></div> <p><b>Note:</b> If an export server is configured, perform this step.</p>																				

**Procedure 1. Recovery Scenario 1**

72. <input type="checkbox"/>	<b>Active NOAM:</b> Activate optional features. DSR only. If SDS, then skip to next step.	<p>Establish an SSH session to the active NOAM and login as <b>admusr</b>.</p> <p><b>Note for PCA Feature Activation:</b></p> <p>If you have PCA installed in the system being recovered, re-activate the PCA by executing the <b>PCA Activation on Entire Server</b> procedure on the recovered NOAM server from [6].</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• If not all SOAM sites are recovered at this point, then repeat the activation for each “new” SOAM site that comes online.</li> <li>• If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature.</li> </ul> <p>Refer to section 1.5 Optional Features to activate any features that were previously activated.</p>
73. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Fetch and store the database report for the newly restored data and save it	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Database</b>.</li> </ol>  <ol style="list-style-type: none"> <li>2. Select the active NOAM server and click <b>Report</b>.</li> </ol>  <p>The following screen displays:</p> <p><b>Main Menu: Status &amp; Manage -&gt; Database [Report]</b></p>  <ol style="list-style-type: none"> <li>3. Click <b>Save</b> and save the report to your local machine.</li> </ol>

**Procedure 1. Recovery Scenario 1**

74. <input type="checkbox"/>	<b>Active NOAM:</b> Verify replication between servers	<ol style="list-style-type: none"> <li>Log into the active NOAM as <b>admusr</b> using SSH terminal.</li> <li>Execute this command: <div data-bbox="532 338 1435 386" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> \$ sudo irepstat -m </div> </li> </ol> <p><b>Example output:</b></p> <pre>-- Policy 0 ActStb [DbReplication] ----- Oahu-DAMP-1 -- Active   BC From Oahu-SOAM-2  Active  0    0.50 ^0.15%cpu 25B/s  A=me   CC To   Oahu-DAMP-2  Active  0    0.10  0.14%cpu 25B/s  A=me Oahu-DAMP-2 -- Stby   BC From Oahu-SOAM-2  Active  0    0.50 ^0.11%cpu 31B/s  A=C3642.212   CC From Oahu-DAMP-1  Active  0    0.10 ^0.14 1.16%cpu 31B/s A=C3642.212 Oahu-IPFE-1 -- Active   BC From Oahu-SOAM-2  Active  0    0.50 ^0.03%cpu 24B/s  A=C3642.212 Oahu-IPFE-2 -- Active   BC From Oahu-SOAM-2  Active  0    0.50 ^0.03%cpu 28B/s  A=C3642.212 Oahu-NOAM-1 -- Stby   AA From Oahu-NOAM-2  Active  0    0.25 ^0.03%cpu 23B/s Oahu-NOAM-2 -- Active   AA To   Oahu-NOAM-1  Active  0    0.25 1%R 0.04%cpu 61B/s   AB To   Oahu-SOAM-2  Active  0    0.50 1%R 0.05%cpu 75B/s Oahu-SOAM-1 -- Stby   BB From Oahu-SOAM-2  Active  0    0.50 ^0.03%cpu 27B/s Oahu-SOAM-2 -- Active   AB From Oahu-NOAM-2  Active  0    0.50 ^0.03%cpu 24B/s   BB To   Oahu-SOAM-1  Active  0    0.50 1%R 0.04%cpu 32B/s   BC To   Oahu-IPFE-1  Active  0    0.50 1%R 0.04%cpu 21B/s   BC To   Oahu-SS7MP-2 Active  0    0.50 1%R 0.04%cpu 21B/s irepstat ( 40 lines) (h)elp (m)erged</pre>
---------------------------------	--	--

**Procedure 1. Recovery Scenario 1**

75. **NOAM VIP GUI:**  
☐ Verify the database states

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

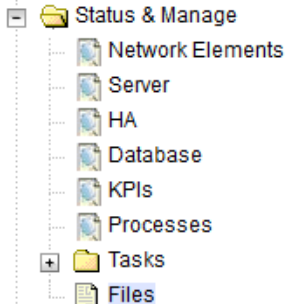
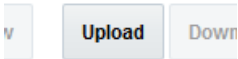
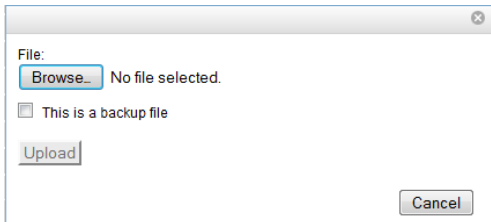
A screenshot of the NOAM VIP GUI. On the left, there is a vertical navigation pane with a tree structure. The 'Status & Manager' folder is expanded, showing sub-items: 'Network Elements', 'Server', 'HA', 'Database' (which is highlighted in blue), 'KPIs', and 'Processes'. Each item has a small icon to its left.

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

Network Element	Server	Role	OAM Max HA Role
ZombieDRNOAM	ZombieDRNOAM1	Network OAM&P	Active
ZombieNOAM	ZombieNOAM2	Network OAM&P	Standby
ZombieSOAM	ZombieSOAM2	System OAM	N/A
ZombieNOAM	ZombieNOAM1	Network OAM&P	Active
ZombieSOAM	ZombieSOAM1	System OAM	Active
ZombieDRNOAM	ZombieDRNOAM2	Network OAM&P	Standby
ZombieSOAM	ZombieDAMP2	MP	Standby
ZombieSOAM	ZombieSS7MP2	MP	Active
ZombieSOAM	ZombieSS7MP1	MP	Active
ZombieSOAM	ZombieIPFE1	MP	Active
ZombieSOAM	ZombieIPFE2	MP	Active



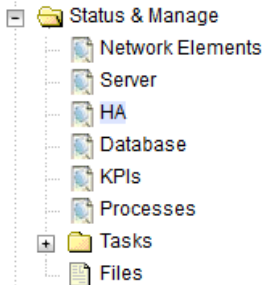
**Procedure 1. Recovery Scenario 1**

<p>76. <input type="checkbox"/></p>	<p><b>NOAM VIP GUI:</b> Upload the backed up RADIUS key file (RADIUS only). DSR only. If SDS, skip to the next step.</p>	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Files</b>.</li> </ol>  <ol style="list-style-type: none"> <li>2. Select the active NOAM server tab. Click <b>Upload</b> and select the <b>RADIUS shared secret encryption key</b> file backed up after initial installation and provisioning or after key revocation execution.</li> </ol>  <ol style="list-style-type: none"> <li>3. Click <b>Browse</b>.</li> <li>4. Locate the <b>DpiKf.bin.encr</b> file.</li> <li>5. Click <b>Upload</b>.</li> </ol>  <p>The file takes a few seconds to upload depending on the size of the file. The file is visible on the list of entries after the upload is complete.</p> <p><b>Note:</b> This file should be deleted from the operator's local servers as soon as key file is uploaded to the active NOAM server.</p>
-------------------------------------	--	---

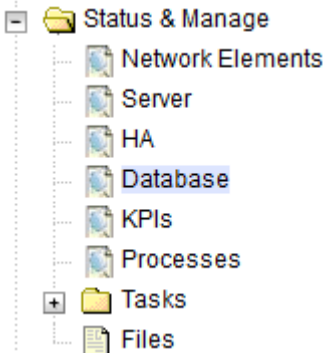
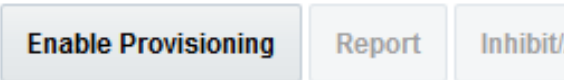
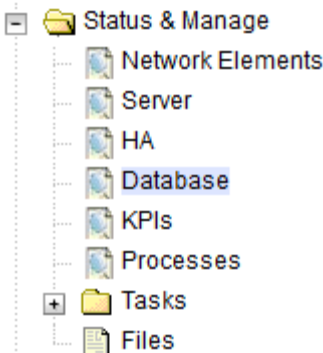
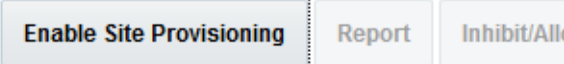
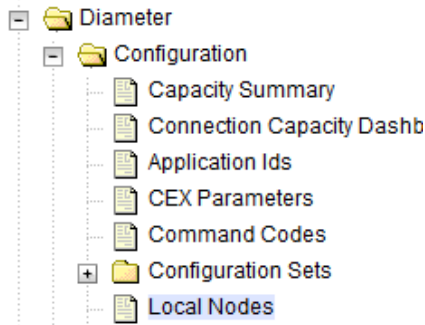
**Procedure 1. Recovery Scenario 1**

77. <input type="checkbox"/>	<b>NOAM VIP:</b> Copy and distribute RADIUS key file on active NOAM (RADIUS only) — Part 1	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>1. Log into the active NOAM VIP as <b>admusr</b> user using SSH terminal.</li> <li>2. Copy the key file:</li> </ol> <pre>\$ cd /usr/TKLC/dpi/bin \$ ./sharedKrevo -decr \$ sudo rm /var/TKLC/db/filemgmt/&lt;backed up key file name&gt;</pre> <ol style="list-style-type: none"> <li>3. Make sure all servers in the topology are accessible.</li> </ol> <pre>\$ ./sharedKrevo -checkAccess</pre> <pre>[admusr@NOAM-2 bin]\$ ./sharedKrevo -checkAccess FIPS integrity verification test failed. 1450723084: [INFO] 'NOAM-1' is accessible. FIPS integrity verification test failed. 1450723084: [INFO] 'SOAM-1' is accessible. FIPS integrity verification test failed. 1450723085: [INFO] 'SOAM-2' is accessible. FIPS integrity verification test failed. 1450723085: [INFO] 'IPFE' is accessible. FIPS integrity verification test failed. 1450723085: [INFO] 'MP-2' is accessible.</pre> <p><b>Note:</b> If all the servers are not accessible, then contact My Oracle Support (MOS).</p>
------------------------------	--	--

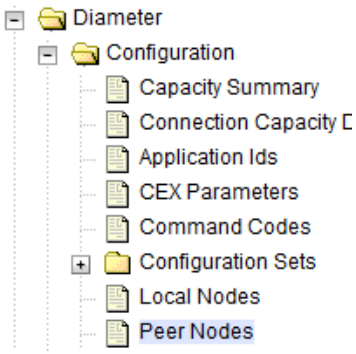
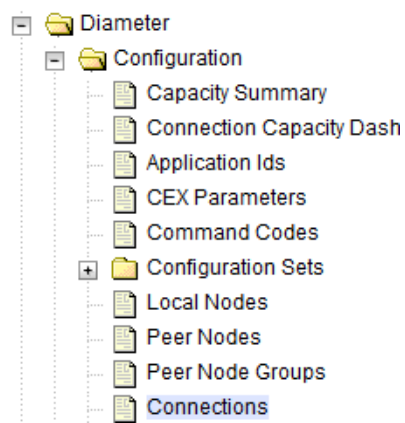
**Procedure 1. Recovery Scenario 1**

78.	<div><div></div><div><b>NOAM VIP:</b> Copy and distribute the RADIUS key file on active NOAM (RADIUS only) — Part 2</div></div>	<div>Distribute key file to all the servers in the topology:</div> <div><pre>\$ ./sharedKrevo -synchronize \$ ./sharedKrevo -updateData</pre></div> <div>Example output:</div> <div><pre>1450723210: [INFO] Key file on Active NOAM and IPFE are same. 1450723210: [INFO] NO NEED to sync key file to IPFE. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723210: [INFO] Key file on Active NOAM and MP-2 are same. 1450723210: [INFO] NO NEED to sync key file to MP-2. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723211: [INFO] Key file on Active NOAM and MP-1 are same. 1450723211: [INFO] NO NEED to sync key file to MP-1. [admusr@NOAM-2 bin]\$ ./sharedKrevo -updateData 1450723226: [INFO] Updating data on server 'NOAM-2' 1450723227: [INFO] Data updated to 'NOAM-2' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723228: [INFO] Updating data on server 'SOAM-2' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723230: [INFO] 1 rows updated on 'SOAM-2'... 1450723230: [INFO] Data updated to 'SOAM-2' [admusr@NOAM-2 bin]\$</pre></div> <div><b>Note:</b> For any errors refer My Oracle Support (MOS).</div>																												
79.	<div><div></div><div><b>NOAM VIP GUI:</b> Verify the HA status</div></div>	<div><div>1. Navigate to <b>Status and Manage &gt; HA</b>.</div><div></div><div>2. Select the row for all of the servers.</div><div>3. Verify the HA Role is either <b>Active</b> or <b>Standby</b>.</div></div> <table><tr><th>Hostname</th><th>OAM HA Role</th><th>Application HA Role</th><th>Max Allowed HA Role</th></tr><tr><td>ZombieNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieDRNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieDRNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieSOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieSOAM2</td><td>Standby</td><td>N/A</td><td>Standby</td></tr></table>	Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role	ZombieNOAM1	Active	N/A	Active	ZombieNOAM2	Standby	N/A	Active	ZombieDRNOAM1	Active	N/A	Active	ZombieDRNOAM2	Standby	N/A	Active	ZombieSOAM1	Active	N/A	Active	ZombieSOAM2	Standby	N/A	Standby
Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role																											
ZombieNOAM1	Active	N/A	Active																											
ZombieNOAM2	Standby	N/A	Active																											
ZombieDRNOAM1	Active	N/A	Active																											
ZombieDRNOAM2	Standby	N/A	Active																											
ZombieSOAM1	Active	N/A	Active																											
ZombieSOAM2	Standby	N/A	Standby																											

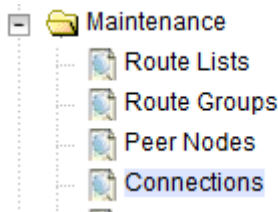
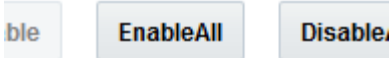
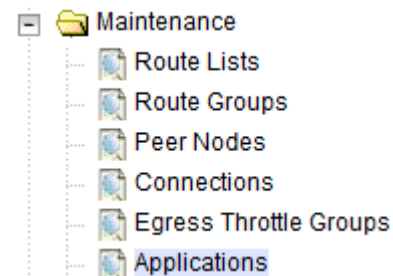
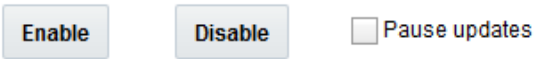
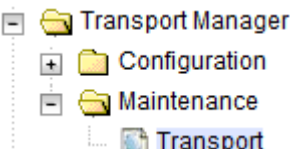

**Procedure 1. Recovery Scenario 1**

80. <input type="checkbox"/>	<b>NOAM GUI:</b> Enable provisioning	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Database</b>.   </li> <li>2. Click <b>Enable Provisioning</b>.   </li> <li>3. Click <b>OK</b>.</li> </ol>
81. <input type="checkbox"/>	<b>SOAM GUI:</b> Enable site provisioning. DSR only. If SDS, then skip to step 91.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Database</b>.   </li> <li>2. Click <b>Enable Site Provisioning</b>.   </li> <li>3. Click <b>OK</b>.</li> </ol>
82. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Verify the local node information. DSR only. If SDS, then skip to step 91.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Diameter &gt; Configuration &gt; Local Node</b>.   </li> <li>2. Verify all the local nodes are shown.</li> </ol>

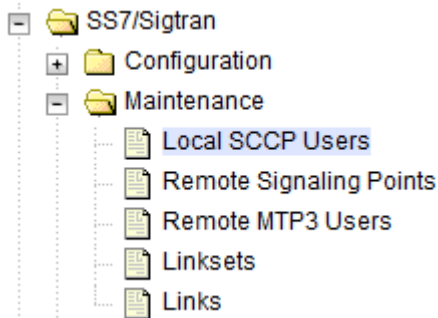
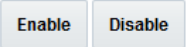
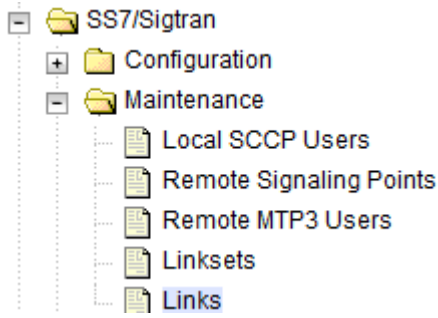

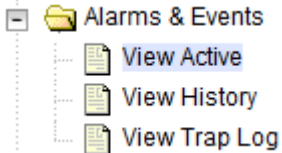
**Procedure 1. Recovery Scenario 1**

83. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Verify the peer node information. DSR only. If SDS, then skip to step 91.	1. Navigate to <b>Diameter &gt; Configuration &gt; Peer Node</b> .  2. Verify all the peer nodes are shown.
84. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Verify the connections information. DSR only. If SDS, then skip to step 91.	1. Navigate to <b>Diameter &gt; Configuration &gt; Connections</b> .  2. Verify all the connections are shown.
85. <input type="checkbox"/>	<b>MP Servers:</b> Disable SCTP Auth Flag. DSR only. If SDS, then skip to step 91.	For SCTP connections without DTLS enabled, refer to the <b>Enable/Disable DTLS (SCTP Diameter Connections Only)</b> section in reference [8]. Execute this procedure on all failed MP servers.

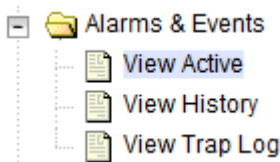
**Procedure 1. Recovery Scenario 1**

86. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Enable connections, if needed. DSR only. If SDS, then skip to step 91.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Diameter &gt; Maintenance &gt; Connections.</b>   </li> <li>2. Select each connection and click <b>Enable</b>. Alternatively, enable all the connections by clicking <b>EnableAll</b>.   </li> <li>3. Verify the Operational State is <b>Available</b>.  <b>Note:</b> If a disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution </li> </ol>
87. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Enable optional features. DSR only. If SDS, then skip to step 91.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Diameter &gt; Maintenance &gt; Applications.</b>   </li> <li>2. Select the optional feature application configured in step 72.</li> <li>3. Click <b>Enable</b>.   </li> </ol>
88. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Re-enable transports, if needed. DSR only. If SDS, then skip to step 91.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Transport Manager &gt; Maintenance &gt; Transport.</b>   </li> <li>2. Select each transport and click <b>Enable</b>.   </li> <li>3. Verify the Operational Status for each transport is <b>Up</b>.</li> </ol>

**Procedure 1. Recovery Scenario 1**

<p>89. <input type="checkbox"/></p>	<p><b>SOAM VIP GUI:</b> Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 91.</p>	<p>1. Navigate to <b>SS7/Sigtran &gt; Maintenance &gt; Local SCCP Users</b>.</p>  <p>2. Click the <b>Enable</b> button corresponding to MAPIWF Application Name.</p>  <p>3. Verify the SSN Status is <b>Enabled</b>.</p>
<p>90. <input type="checkbox"/></p>	<p><b>SOAM VIP GUI:</b> Re-enable links, if needed. DSR only. If SDS, then skip to step 91.</p>	<p>1. Navigate to <b>SS7/Sigtran &gt; Maintenance &gt; Links</b>.</p>  <p>2. Click <b>Enable</b> for each link.</p>  <p>3. Verify the Operational Status for each link is <b>Up</b>.</p>
<p>91. <input type="checkbox"/></p>	<p><b>SOAM VIP GUI:</b> Examine all alarms</p>	<p>1. Navigate to <b>Alarms &amp; Events &gt; View Active</b>.</p>  <p>2. Examine all active alarms and refer to the on-line help on how to address them.</p> <p>If needed, contact My Oracle Support (MOS).</p>

**Procedure 1. Recovery Scenario 1**

92. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Examine all alarms	<p>1. Navigate to <b>Alarms &amp; Events &gt; View Active</b>.</p>  <p>2. Examine all active alarms and refer to the on-line help on how to address them.</p> <p>If needed, contact My Oracle Support (MOS).</p>
93. <input type="checkbox"/>	Restore GUI usernames and passwords	If applicable, execute the section 5 <b>Resolve User Credential Issues after Database Restore</b> procedure to recover the user and group information restored.
94. <input type="checkbox"/>	Back up and archive all the databases from the recovered system	Execute the <b>DSR Database Backup</b> procedure to back up the configuration databases.
95. <input type="checkbox"/>	Recover IDIH, if configured	If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.
96. <input type="checkbox"/>	SNMP workaround	<p>Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases:</p> <ol style="list-style-type: none"> <li>1. If SNMP is not configured in DSR/SDS.</li> <li>2. If SNMP is already configured and SNMPv3 is selected as enabled version.</li> </ol>

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

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

- Recover **standby NOAM** server (if needed) by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover **Query Server** (if needed) by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover **active SOAM** server by recovering base hardware, software, and database
  - Recover the base hardware



- Recover the software
- Recover the database
- Recover any failed **SOAM and MP/DP** servers by recovering base hardware and software
  - Recover the base hardware
  - Recover the software


The database has already been restored at the active SOAM server and does not require restoration at the SO and MP/DP servers.

- Recover IDIH if necessary

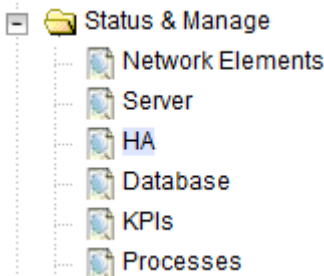
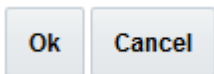
## Procedure 2. Recovery Scenario 2

S T E P #		<p>This procedure performs recovery if at least one NOAM server is available, but all SOAM servers in a site have failed. This includes any SOAM server that is in another location.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>
1. <input type="checkbox"/>	Workarounds	<p>Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.</p> <p>Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases:</p> <ol style="list-style-type: none"> <li>1. If SNMP is not configured in DSR.</li> <li>2. If SNMP is already configured and SNMPv3 is selected as enabled version.</li> </ol>
2. <input type="checkbox"/>	Gather required materials	Gather the documents and required materials listed in Required Materials.

**Procedure 2. Recovery Scenario 2**

<div data-bbox="203 247 235 315">3. <input type="checkbox"/></div>	<b>NOAM VIP GUI:</b> Login	<div data-bbox="516 247 1430 310"><p>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:</p></div> <div data-bbox="565 323 1369 369"><p><code>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</code></p></div> <div data-bbox="516 382 901 411"><p>2. Login as the <b>guiadmin</b> user:</p></div> <div data-bbox="769 443 1159 499"></div> <div data-bbox="522 548 760 577"><p>Oracle System Login</p></div> <div data-bbox="1144 571 1395 594"><p>Tue Jun 7 13:49:06 2016 EDT</p></div> <div data-bbox="683 632 1234 968"><div data-bbox="917 657 998 686"><b>Log In</b></div><div data-bbox="732 686 1187 716">Enter your username and password to log in</div><div data-bbox="841 741 1146 770">Username: <input type="text"/></div><div data-bbox="846 791 1146 821">Password: <input type="password"/></div><div data-bbox="914 842 1109 865"><input type="checkbox"/> Change password</div><div data-bbox="937 900 987 924"><input type="button" value="Log In"/></div></div> <div data-bbox="548 982 1372 1026"><p>Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.</p></div> <div data-bbox="630 1045 1287 1087"><p>Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</p></div> <div data-bbox="686 1108 1232 1131"><p>Copyright © 2010, 2016, <a href="#">Oracle</a> and/or its affiliates. All rights reserved.</p></div>
--	-------------------------------	--

**Procedure 2. Recovery Scenario 2**

<p>4. <input type="checkbox"/></p>	<p><b>Active NOAM:</b> Set failed servers to OOS</p>	<p>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.</p>  <p>2. Click <b>Edit</b>.</p> <p><b>Modifying HA attributes</b></p> <table border="1" data-bbox="521 709 1057 1052"> <thead> <tr> <th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td><td>Active</td><td>The maximum des</td></tr> <tr> <td>ZombieNOAM2</td><td>OOS</td><td>The maximum des</td></tr> <tr> <td>ZombieDRNOAM1</td><td>OOS</td><td>The maximum des</td></tr> </tbody> </table> <p>3. Set the Max Allowed HA Role option to <b>OOS</b> for the failed servers.</p> <p>4. Click <b>OK</b>.</p> 	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active	The maximum des	ZombieNOAM2	OOS	The maximum des	ZombieDRNOAM1	OOS	The maximum des
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active	The maximum des												
ZombieNOAM2	OOS	The maximum des												
ZombieDRNOAM1	OOS	The maximum des												
<p>5. <input type="checkbox"/></p>	<p>Replace failed equipment</p>	<p>Work with the hardware vendor to replace the failed equipment.</p>												
<p>6. <input type="checkbox"/></p>	<p><b>Recover PMAC TVOE Host:</b> (if required) Configure BIOS settings and update firmware</p>	<p>1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:</p> <ul style="list-style-type: none"> <li>• <b>HP DL380 Gen8:</b> Configure HP Gen 8 Server BIOS Settings</li> <li>• <b>Oracle X5-2/Netra X5-2/X6-2/X7-2:</b> Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings</li> <li>• <b>HP DL380 Gen9:</b> Configure HP Gen9 Server BIOS Settings</li> </ul> <p>2. Verify and/or upgrade server firmware by executing the <b>Upgrade Rack Mount Server Firmware</b> procedure from reference [8].</p>												

**Procedure 2. Recovery Scenario 2**

7. <input type="checkbox"/>	<b>Recover PMAC and PMAC TVOE</b> <b>Host:</b> Backups available	<p>If PMAC is located on the failed rack mount server(s), execute this step; otherwise, skip to step 11.</p> <p>This step assumes TVOE and PMAC backups are available. If backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> <li>1. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.</li> <li>2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup.</li> <li>3. Proceed to step 11.</li> </ol>
8. <input type="checkbox"/>	<b>Recover PMAC and PMAC TVOE</b> <b>Host:</b> Backups not available	<p>This step assumes TVOE and PMAC backups are <b>NOT</b> available, if the TVOE and PMAC have already been restored, <b>skip this step</b>.</p> <ol style="list-style-type: none"> <li>1. Execute these procedures from reference [8]: <ul style="list-style-type: none"> <li>• <b>Install and Configure TVOE on First RMS (PMAC Host)</b></li> <li>• <b>Install PMAC</b></li> <li>• <b>Initialize the PMAC Application</b></li> </ul> </li> <li>2. Proceed to next step.</li> </ol>
9. <input type="checkbox"/>	<b>Configure PMAC:</b> No Backup	<p>If PMAC backup was <b>NOT</b> restored in step 7. , execute this step; otherwise, skip this step.</p> <p>Execute these procedures from reference [8]:</p> <ul style="list-style-type: none"> <li>• <b>Configure PMAC Server (NetBackup Only)</b></li> <li>• <b>Add RMS to the PMAC Inventory</b></li> </ul>
10. <input type="checkbox"/>	Install/Configure additional rack mount servers	<p>This step assumes TVOE backups are available on any additional rack mount servers; otherwise, skip this step.</p> <p>Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on additional rack mount servers.</p>
11. <input type="checkbox"/>	Install/Configure additional rack mount servers	<p>If TVOE backups were NOT performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step.</p> <ol style="list-style-type: none"> <li>1. Execute these procedures from reference [8]: <ul style="list-style-type: none"> <li>• <b>Install TVOE on Additional Rack Mount Servers</b></li> <li>• <b>Configure TVOE on Additional Rack Mount Servers</b></li> </ul> </li> <li>2. Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]: <ul style="list-style-type: none"> <li>• <b>HP DL380 Gen8:</b> Configure HP Gen 8 Server BIOS Settings</li> <li>• <b>Oracle X5-2/Netra X5-2/X6-2/X7-2:</b> Configure Oracle X5-2/Netra X5-2/X6-2/X7-2 Server BIOS Settings</li> <li>• <b>HP DL380 Gen9:</b> Configure HP Gen9 Server BIOS Settings</li> </ul> </li> </ol>

**Procedure 2. Recovery Scenario 2**

12. <input type="checkbox"/>	Determine VM placement and socket pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only)	HP DL380 GEN 8, <b>skip this step</b> . Determine VM placement and pinning by following section 3.1, item 14.
13. <input type="checkbox"/>	Deploy redundant PMAC	If the redundant PMAC is located on the failed rack mount server(s), execute this step; otherwise, skip to the next step. Refer to the <b>Deploy Redundant PMAC (Optional)</b> procedure to re-deploy and configure any redundant PMACs previously configured.
14. <input type="checkbox"/>	<b>PMAC:</b> Determine if the fdconfig file exists from the initial deployment	<ol style="list-style-type: none"> <li>Type: <pre>[admusr@melbourne-pmac-1 ~]\$ ll /usr/TKLC/smac/etc/fdc/</pre></li> <li>Examine the results and verify if the <b>rms config file &lt;hostname&gt;.cfg</b> exists.  <b>Note:</b> There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS.</li> <li>If the file exists, skip to step 16.</li> </ol>
15. <input type="checkbox"/>	Create fdconfig backup file, if it does not already exist	<p>Execute this step <b>ONLY</b> If the fdconfig backup file does <b>NOT</b> exist.</p> <ol style="list-style-type: none"> <li>Create the needed file(s) by executing the <b>Virtual Machine/Network Fast Deployment</b> section from reference [8].</li> </ol> <p style="text-align: center;"><b>WARNING</b></p> <p>It is very important to ensure the file(s) created only affects the TVOE server(s) and the guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.</p> <ol style="list-style-type: none"> <li>Skip to step 24.</li> </ol>
16. <input type="checkbox"/>	<b>PMAC:</b> Load ISOs into PMAC, if not done already	If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the <b>Virtual Machine/Network Fast Deployment</b> section from reference [8].
17. <input type="checkbox"/>	<b>PMAC:</b> Edit/Update configuration file	<p>Edit the fdconfig file to include only the required/failed servers.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Comment out configuration items that are not needed.</li> <li>Create a separate configuration file for EACH rack mount server being deployed.</li> <li>The Cabinet ID in the config file needs to match the cabinet already defined in PMAC.</li> </ul> <p>The following items are mandatory:</p> <ul style="list-style-type: none"> <li>siteName</li> <li>tpdlso</li> <li>dsrlso (if DSR VMs are being configured)</li> </ul>

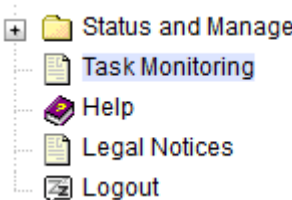
**Procedure 2. Recovery Scenario 2**

		<ul style="list-style-type: none"> <li>• sdsIso (if SDS VMs are being configured)</li> <li>• NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured)</li> <li>• XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured)</li> <li>• XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured)</li> <li>• DSRNOAM1XMIIPADDRESS (if DSRNOAM1 is being configured)</li> <li>• DSRNOAM2XMIIPADDRESS (if DSRNOAM2 is being configured)</li> <li>• DSRDRNOAM1XMIIPADDRESS (if DSRDRNOAM1 is being configured)</li> <li>• DSRDRNOAM2XMIIPADDRESS (if DSRDRNOAM2 is being configured)</li> <li>• SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured)</li> <li>• SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured)</li> <li>• SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured)</li> <li>• SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured)</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].</li> <li>• Comment out SDS and DSR profile items if corresponding products are not used.</li> <li>• For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9, refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].</li> <li>• VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName.</li> <li>• VM locations should not be changed from their <b>RMSx</b> format. Each RMS should correspond to a separate rack mount server.</li> </ul> <p style="text-align: center;"><b>WARNING</b></p> <p>Ensure the file(s) created only affect the TVOE server(s) and guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.</p>
18.	<input type="checkbox"/> <b>PMAC:</b> Copy the backed up fdconfig file to the RMS directory	<p>Copy the fdconfig backup file to the RMS directory.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo cp /usr/TKLC/smac/etc/fdc/&lt;backup_fdc_file&gt; /usr/TKLC/smac/etc/RMS/</pre>

## Procedure 2. Recovery Scenario 2

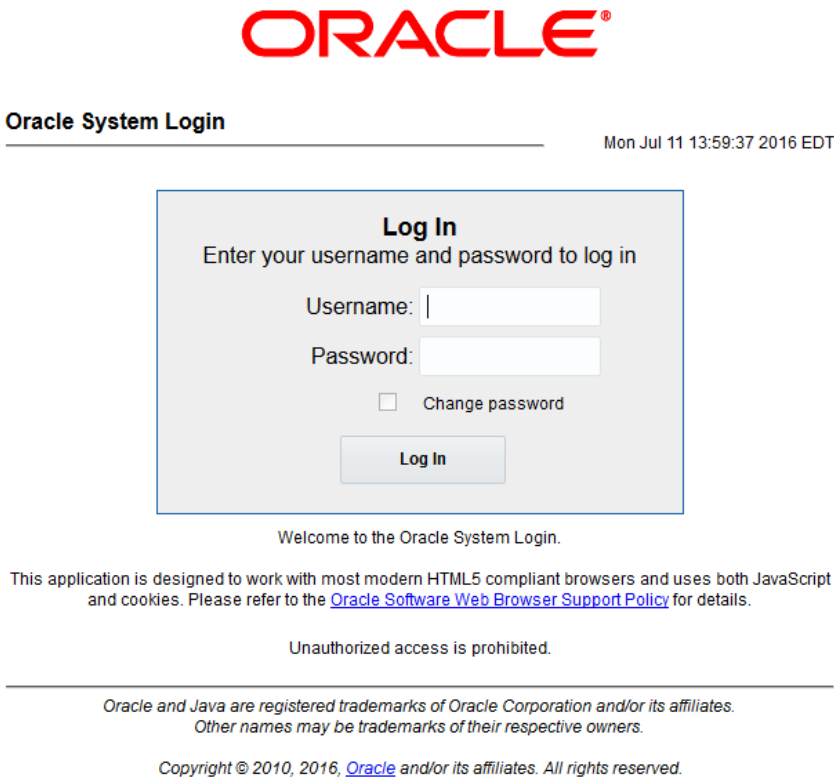
19. <input type="checkbox"/>	<b>PMAC:</b> Execute the config.sh script	<p>Execute <b>config.sh</b> against the modified backup config file.</p> <p><b>Note:</b> If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again.</p> <pre>\$ sudo ./config.sh &lt;config file&gt;</pre> <p>Example output:</p> <pre>[admusr@5010441PMAC RMS]\$ sudo ./config.sh rms.cfg Validating cfg file... Successful validation of cfg file. Added Cabinet 101 to Fast Deployment File. Added Zombie_TVOE1 to Fast Deployment File. Added Zombie_TVOE2 to Fast Deployment File. Added xmi(bond0.4) to Fast Deployment File. Added imi(bond0.3) to Fast Deployment File. Added rep(bond1.10) to Fast Deployment File. Added xsi1(bond1.6) to Fast Deployment File. Added xsi2(bond1.7) to Fast Deployment File. Added xsi3(bond1.8) to Fast Deployment File. Added xsi4(bond1.9) to Fast Deployment File. Added xsi5(bond1.11) to Fast Deployment File. Added xsi6(bond1.12) to Fast Deployment File. Added xsi7(bond1.13) to Fast Deployment File. Added xsi8(bond1.14) to Fast Deployment File. Added xsi9(bond1.15) to Fast Deployment File. Added xsi10(bond1.16) to Fast Deployment File. Added xsi11(bond1.17) to Fast Deployment File. Added xsi12(bond1.18) to Fast Deployment File. Added xsi13(bond1.19) to Fast Deployment File. Added xsi14(bond1.20) to Fast Deployment File. Added xsi15(bond1.21) to Fast Deployment File. Added xsi16(bond1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRDRNOAM1 to Fast Deployment File. Added Zombie_DSRDRNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSDRNOAM1 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_DSRSOAM1 to Fast Deployment File. Added Zombie_DSRSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM1 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDAMP2 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_DSRIPFE2 to Fast Deployment File. Added Zombie_SSDPSV1 to Fast Deployment File. Added Zombie_SSDPSV2 to Fast Deployment File. Validating Fast Deployment File..... Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!! [admusr@5010441PMAC RMS]\$</pre>
---------------------------------	---	--

**Procedure 2. Recovery Scenario 2**

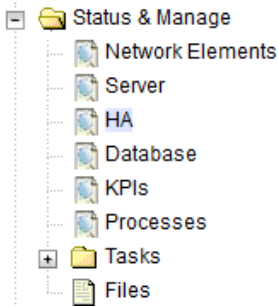
20. <input type="checkbox"/>	<b>PMAC:</b> Execute fast deployment	<p>With the file generated from the config.sh script, execute the following command to start fast deployment:</p> <pre>\$ screen \$ sudo fdconfig config --file=&lt;fd_config.xml&gt;</pre> <p><b>Note:</b> This is a long duration command. If the screen command was run before executing the fdconfig, perform a <b>screen -dr</b> to resume the screen session in the event of a terminal timeout, etc.</p>																																																															
21. <input type="checkbox"/>	<b>PMAC GUI:</b> Monitor the configuration	<p>1. If not already done, establish a GUI session on the PMAC server.</p> <p>2. Navigate to <b>Task Monitoring</b>.</p> <div></div> <p>3. Monitor the configuration to completion:</p> <div><p>Main Menu: Task Monitoring</p><p>Filter*</p><table><tr><th>ID</th><th>Task</th><th>Target</th><th>Status</th><th>State</th><th>Task Output</th><th>Running Time</th><th>Start Time</th><th>Progress</th></tr><tr><td>925</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_SDSRNOAM1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:04</td><td>2016-07-11 11:27:35</td><td>100%</td></tr><tr><td>924</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_SDSNOAM1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:04</td><td>2016-07-11 11:27:04</td><td>100%</td></tr><tr><td>923</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_DSRIPE1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:06</td><td>2016-07-11 11:26:43</td><td>100%</td></tr><tr><td>922</td><td>Accept</td><td>RMS: pc5010439 Guest: Zombie_DSRIPE2</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:05</td><td>2016-07-11 11:26:43</td><td>100%</td></tr><tr><td>921</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_DSRIPE1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:05</td><td>2016-07-11 11:26:43</td><td>100%</td></tr><tr><td>920</td><td>Accept</td><td>RMS: pc5010439 Guest: Zombie_DSRSOAM2</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:06</td><td>2016-07-11 11:26:42</td><td>100%</td></tr></table></div> <p><b>Note:</b> If a failure occurs with fdconfig, logs can be accessed in <b>/var/TKLC/log/fdconfig/fdconfig.log</b> file.</p> <pre>[admusr@melbourne-pmac-1 fdconfig]\$ sudo fdconfig dumpsteps -- file=deploy_melbourne_20170329T202458_701b.fdcdb Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb" Here are the steps that were generated ----- begin ----- Dump of DB steps: NUM PHS DLY INFRA ID SVRTYPE CMD ELEMENT PRE STATE TO BGTS COMMAND TEXT ----- 1 1 0 pmac Fast_Deployment 0 21 0 Complete 300 0 Check PM&amp;C is available 2 1 0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet 3 1 0 pmac Fast_Deployment 0 3 melbourne_RMS3 1 Skipped 900 0 Add Rms 4 2 0 pmac Fast_Deployment 1</pre> <p>4. Restart the fdconfig after a failure has occurred and has been resolved:</p> <pre>\$ sudo fdconfig restart -- file=deploy_melbourne_20170329T202458_701b.fdcdb</pre>	ID	Task	Target	Status	State	Task Output	Running Time	Start Time	Progress	925	Accept	RMS: pc5010441 Guest: Zombie_SDSRNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:35	100%	924	Accept	RMS: pc5010441 Guest: Zombie_SDSNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:04	100%	923	Accept	RMS: pc5010441 Guest: Zombie_DSRIPE1	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:43	100%	922	Accept	RMS: pc5010439 Guest: Zombie_DSRIPE2	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%	921	Accept	RMS: pc5010441 Guest: Zombie_DSRIPE1	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%	920	Accept	RMS: pc5010439 Guest: Zombie_DSRSOAM2	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:42	100%
ID	Task	Target	Status	State	Task Output	Running Time	Start Time	Progress																																																									
925	Accept	RMS: pc5010441 Guest: Zombie_SDSRNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:35	100%																																																									
924	Accept	RMS: pc5010441 Guest: Zombie_SDSNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:04	100%																																																									
923	Accept	RMS: pc5010441 Guest: Zombie_DSRIPE1	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:43	100%																																																									
922	Accept	RMS: pc5010439 Guest: Zombie_DSRIPE2	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%																																																									
921	Accept	RMS: pc5010441 Guest: Zombie_DSRIPE1	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%																																																									
920	Accept	RMS: pc5010439 Guest: Zombie_DSRSOAM2	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:42	100%																																																									



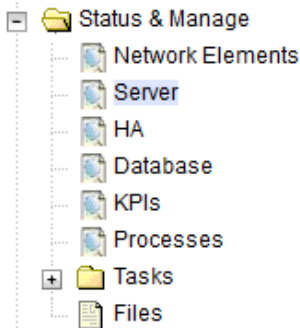

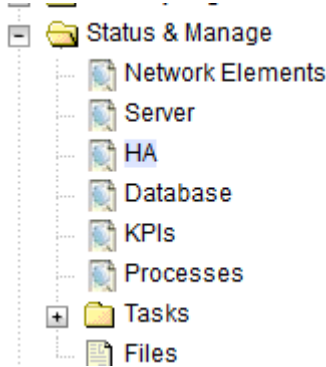
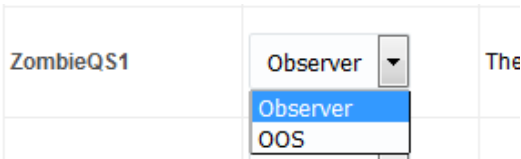
**Procedure 2. Recovery Scenario 2**

22. <input type="checkbox"/>	<b>PMAC:</b> Repeat for each rack mount server configuration file	Repeat steps 14. -21. for each rack mount server/configuration file, if required.
23. <input type="checkbox"/>	<b>PMAC:</b> Back up FDC file	<ol style="list-style-type: none"> <li>Copy the updated fdc file to the fdc backup directory:  <pre>\$ sudo cp /usr/TKLC/smac/etc/RMS/&lt;fdc_file&gt; /usr/TKLC/smac/etc/fdc/</pre> </li> <li>Change permissions:  <pre>\$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/&lt;fdc_file&gt;</pre> </li> </ol>
24. <input type="checkbox"/>	Perform CPU pinning	Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the <b>CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only)</b> procedure from reference [8].
25. <input type="checkbox"/>	<b>NOAM GUI:</b> Login If the failed server is not OAM, then skip to step 47.	<ol style="list-style-type: none"> <li>Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  <pre>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</pre> </li> <li>Login as the <b>guiadmin</b> user:</li> </ol> 

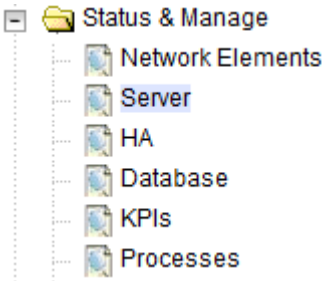

**Procedure 2. Recovery Scenario 2**

26. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover standby NOAM, if needed	<p>Install the second NOAM server:</p> <p><b>DSR:</b> Execute the <b>Configure the Second NOAM Server</b> procedure, steps 1 and 3-6, from reference [8].</p> <p><b>SDS:</b> Execute the <b>Configure the Second SDS NOAM Server</b> procedure, steps 1 and 3-6, from reference [8].</p>												
27. <input type="checkbox"/>	Install NetBackup client (optional)	If NetBackup is used, execute the <b>Install NetBackup Client (Optional)</b> procedure from reference [8].												
28. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set HA on standby NOAM	<ol style="list-style-type: none"> <li>Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>Click <b>Edit</b>.</li> <li>Select the standby NOAM server and set it to <b>Active</b>.  <p><b>Modifying HA attributes</b></p> <table border="1" data-bbox="532 1136 1198 1514"> <thead> <tr> <th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td><td>Active ▼</td><td>The maximum</td></tr> <tr> <td>ZombieNOAM2</td><td>Active ▼</td><td>The maximum</td></tr> <tr> <td>ZombieDRNOAM1</td><td>Active ▼ Standby Snare</td><td>The maximum</td></tr> </tbody> </table> </li> <li>Click <b>OK</b>.</li> </ol>	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active ▼	The maximum	ZombieNOAM2	Active ▼	The maximum	ZombieDRNOAM1	Active ▼ Standby Snare	The maximum
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active ▼	The maximum												
ZombieNOAM2	Active ▼	The maximum												
ZombieDRNOAM1	Active ▼ Standby Snare	The maximum												

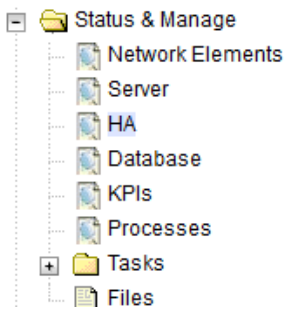
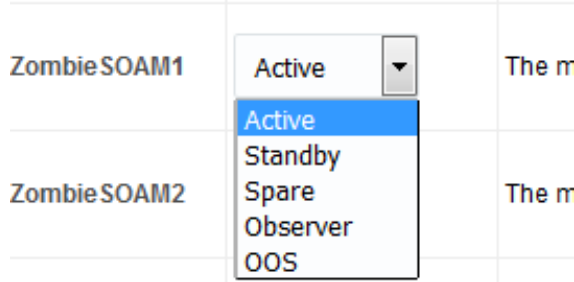
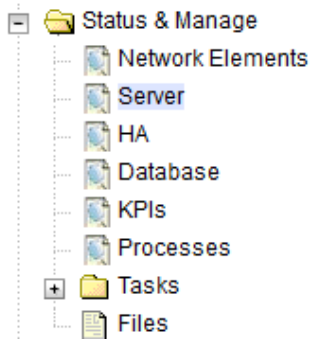

**Procedure 2. Recovery Scenario 2**

29. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Restart DSR application	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.   </li> <li>2. Select the recovered standby NOAM server and click <b>Restart</b>.   </li> </ol>
30. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover query servers. SDS only. If DSR, skip to step 33.	Execute the <b>Configuring SDS Query Servers</b> procedure, steps 1 and 4-7, from reference [8].
31. <input type="checkbox"/>	<b>SDS NOAM VIP GUI:</b> Set HA on query server. SDS only. If DSR, skip to step 33.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>2. Click <b>Edit</b>.</li> <li>3. Select the query server and select <b>Observer</b>.   </li> <li>4. Click <b>OK</b>.</li> </ol>

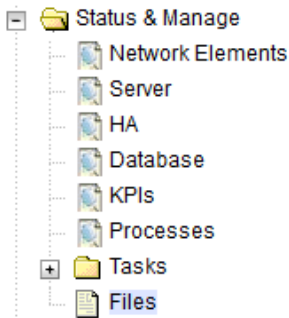

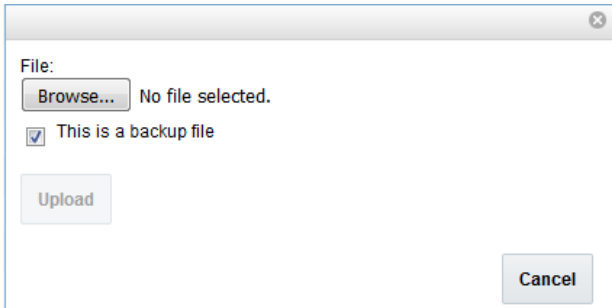
**Procedure 2. Recovery Scenario 2**

32. <input type="checkbox"/>	<b>SDS NOAM VIP GUI:</b> Restart SDS application. SDS only. If DSR, skip to step 33.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.   </li> <li>2. Select the recovered query server and click <b>Restart</b>.   </li> </ol>
33. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Stop replication to the C-level servers of this site.	<p><b>For DSR:</b></p> <p>Before continuing this procedure, replication to C-level servers <b>MUST</b> be inhibited at the SOAM site being recovered.</p> <p>Failure to inhibit replication to the working C-level servers results in the database being destroyed!</p> <p><b>If the spare SOAM is also present in the site and lost</b>, execute Appendix E Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost) to inhibit replication to working C-level servers before continuing.</p> <p><b>If the spare SOAM is NOT deployed in the site</b>, execute Appendix C Inhibit A and B Level Replication on C-level Servers to inhibit replication to working C-level servers before continuing.</p> <p><b>For SDS,</b></p> <p>Inhibit database replication for defective SOAM servers and DP servers associated with this SOAM network element.</p> <p>NOTE: It is expected that each SOAM and subtending DP will have a DB Level of "UNKNOWN" until the SOAMs are restored.</p> <ol style="list-style-type: none"> <li>1. Go to the NOAMP GUI.</li> <li>2. Select <b>[Main Menu: Status &amp; Manage → Database]</b> screen</li> <li>3. Filter on the SOAM Network Element name.</li> <li>4. Record the DP server hostnames (Role: MP).</li> <li>5. Click "Inhibit Replication" button for each DP server until all DP servers associated with this SOAM Network Element have been inhibited</li> </ol> <p>"Inhibiting" SOAM server: Click "Inhibit Replication" button for each defective SOAM servers.</p>


**Procedure 2. Recovery Scenario 2**

34. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover active SOAM server	<p>Install the SOAM servers.</p> <p><b>DSR:</b> Execute the <b>Configure the SOAM Servers</b> procedure, steps 1-3 and 5-9, from reference [8].</p> <p><b>Note:</b> If you are using NetBackup, also execute step 12.</p> <p><b>SDS:</b> Execute the <b>Configure the SDS DP SOAM Servers</b> procedure, steps 1-3 and 5-8, from reference [8].</p>
35. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set HA on the SOAM server	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>2. Click <b>Edit</b>.</li> <li>3. Select the SOAM server and set it to <b>Active</b>.   </li> <li>4. Click <b>OK</b>.</li> </ol>
36. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Restart DSR application	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.   </li> <li>2. Select the recovered SOAM server and click <b>Restart</b>.   </li> </ol>

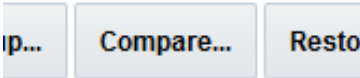
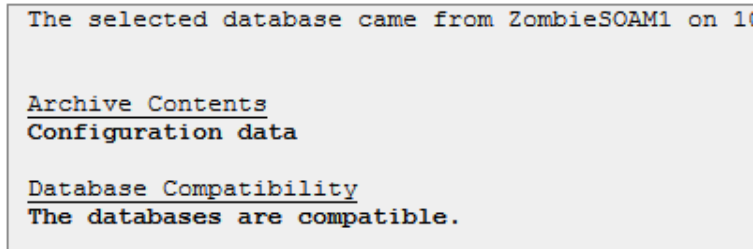
**Procedure 2. Recovery Scenario 2**

<p>37. <input type="checkbox"/></p>	<p><b>NOAM VIP GUI:</b> Upload the backup SOAM database file. DSR only. If SDS, skip to step 42.</p>	<ol style="list-style-type: none"><li>1. Navigate to <b>Status &amp; Manage &gt; Files</b>. </li><li>2. Select the active SOAM server tab. Click <b>Upload</b> and select the file <b>SO Provisioning and Configuration</b> file backed up after initial installation and provisioning. </li><li>3. Click <b>Browse</b> and locate the backup file.</li><li>4. Mark the <b>This is a backup file</b> checkbox.</li><li>5. Click <b>Open</b>.</li><li>6. Click <b>Upload</b>. </li></ol> <p>The file takes a few seconds to upload depending on the size of the backup data and displays on the list of entries when it has completed the upload.</p>
-------------------------------------	--	--

**Procedure 2. Recovery Scenario 2**

<div>38.</div> <div><input type="checkbox"/></div>	<b>Recovered SOAM GUI:</b> Login. DSR only. If SDS, skip to step 42.	<div><div>1. Establish a GUI session on the recovered SOAM server.</div><div>2. Open the web browser and enter a URL of: <div>http://&lt;Recovered_SOAM_IP_Address&gt;</div></div><div>3. Login as the <b>guiadmin</b> user:</div><div></div></div>
--	--	--

**Procedure 2. Recovery Scenario 2**


<p>39. <input type="checkbox"/></p>	<p><b>Recovered SOAM GUI:</b> Verify the archive contents and database compatibility. DSR only. If SDS, skip to step 42.</p>	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Database</b>.</li> <li>2. Select the <b>Active SOAM</b> server and click <b>Compare</b>.</li> </ol>  <ol style="list-style-type: none"> <li>3. Click the button for the restored database file uploaded as a part of step 27. of this procedure.</li> </ol> <p><b>Database Compare</b></p> <p>Select archive to compare on server: 2</p> <p>Archive * <input checked="" type="radio"/> backup/Backup.DSR.Zom</p> <p>Ok Cancel</p> <ol style="list-style-type: none"> <li>4. Verify the output window matches the screen below.</li> </ol>  <p><b>Note:</b> Archive Contents and Database Compatibilities must be the following:</p> <p><b>Archive Contents:</b> Configuration data.</p> <p><b>Database Compatibility:</b> The databases are compatible.</p> <p><b>Note:</b> The following is expected output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM:</p> <p><b>Topology Compatibility</b></p> <p>The topology should be compatible minus the NODEID.</p> <p><b>Note:</b> We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility.</p> <ol style="list-style-type: none"> <li>5. If the verification is successful, click <b>Back</b> and continue to <b>next step</b> in this procedure.</li> </ol>
-------------------------------------	--	--



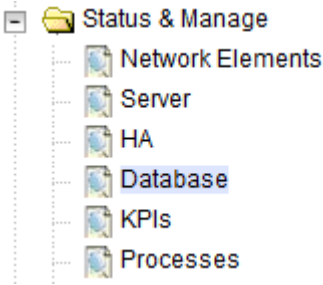
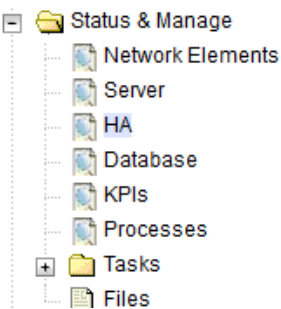
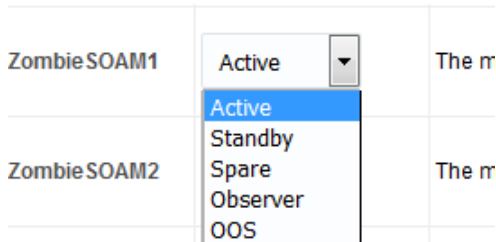
**Procedure 2. Recovery Scenario 2**

<p>40. <input type="checkbox"/></p>	<p><b>Recovered SOAM GUI:</b> Restore the database. DSR only. If SDS, skip to step 42.</p>	<ol style="list-style-type: none"> <li>1. Select the <b>Active SOAM</b> server and click <b>Restore</b>.</li> <li>2. Select the backup provisioning and configuration file.   <div data-bbox="539 340 818 375" data-label="Section-Header"><b>Database Compare</b></div> <div data-bbox="527 415 904 653" data-label="Form"> <div>Select archive to compare on server</div> <div>Archive * <input checked="" type="radio"/> backup/Backup.dsr.Z</div> <div>Ok Cancel</div> </div> </li> <li>3. Click <b>OK</b>.   <div data-bbox="521 730 836 760" data-label="Section-Header"><b>Database Restore Confirm</b></div> <div data-bbox="518 791 693 819" data-label="Text">Compatible archive.</div> <div data-bbox="534 852 1027 1113" data-label="Image"> </div> </li> <li>4. If the Node Type Compatibility error displays, it is expected. If no other errors display, mark the <b>Force</b> checkbox and click <b>OK</b> to proceed with the DB restore.   <b>Notes:</b> <ul style="list-style-type: none"> <li>• After the restore has started, the user is logged out of XMI SOAM GUI since the restored topology is old data.</li> <li>• If the spare SOAM is in another network and is unreachable, the database restore cannot be done.</li> </ul> <b>Workaround:</b> If the spare SOAM is unreachable and ping (from recovered SOAM server to spare SOAM server) hangs (as evidenced by <b>ps -ef   grep ping</b> showing the same ping process and its child for more than 10 seconds), then kill the hung ping processes and the restore proceeds. </li> </ol>
<p>41. <input type="checkbox"/></p>	<p><b>Recovered SOAM GUI:</b> Monitor and confirm database restoral. DSR only. If SDS, skip to step 42.</p>	<p>Wait for <b>5-10 minutes</b> for the system to stabilize with the new topology: Monitor the Info tab for <b>Success</b>. This indicates the restore is complete and the system is stabilized.   <b>Notes:</b> <ul style="list-style-type: none"> <li>• Do not pay attention to alarms until all the servers in the system are completely restored.</li> <li>• The Configuration and Maintenance information is in the same state it was when backed up during initial backup.</li> </ul> </p>

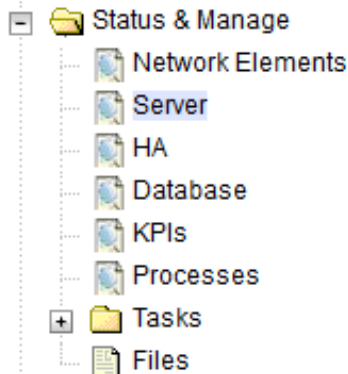

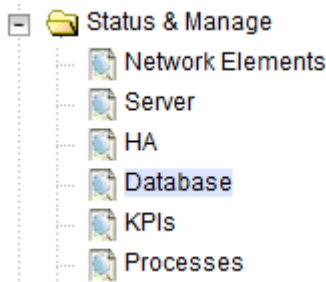
**Procedure 2. Recovery Scenario 2**

42. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Login	<ol style="list-style-type: none"> <li>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  <div style="border: 1px solid black; padding: 2px; margin: 5px 0;">http://&lt;Primary_NOAM_VIP_IP_Address&gt;</div> </li> <li>2. Login as the <b>guiadmin</b> user:</li> </ol> <div style="text-align: center; margin: 20px 0;">  </div> <div style="text-align: center;"> <b>Oracle System Login</b> </div> <div style="text-align: right; margin-top: 5px;">Tue Jun 7 13:49:06 2016 EDT</div> <div style="text-align: center; margin: 20px 0;"> <div style="border: 1px solid gray; padding: 10px; width: 300px; margin: 0 auto;"> <p><b>Log In</b></p> <p>Enter your username and password to log in</p> <p>Username: <input style="width: 100px;" type="text"/></p> <p>Password: <input style="width: 100px;" type="password"/></p> <p style="text-align: center;"> <input type="checkbox"/> Change password </p> <p style="text-align: center;"> <input type="button" value="Log In"/> </p> </div> </div> <p style="font-size: small; text-align: center;">Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.</p> <hr/> <p style="font-size: x-small; text-align: center;">Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</p> <p style="font-size: x-small; text-align: center;">Copyright © 2010, 2016, <a href="#">Oracle</a> and/or its affiliates. All rights reserved.</p>
43. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover the remaining SOAM servers (standby, spare)	<p><b>DSR:</b></p> <p>Execute the <b>Configure the SOAM Servers</b> procedure, steps 1-3 and 5-9, from reference [8].</p> <p><b>Note:</b> If you are using NetBackup, also execute step 12.</p> <p><b>SDS:</b></p> <p>Execute the <b>Configure the SDS DP SOAM Servers</b> procedure, steps 1-3 and 5-8, from reference [8].</p>

**Procedure 2. Recovery Scenario 2**

44. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Start replication on the recovered SOAMs, if replication is inhibited	<p>Un-Inhibit (start) replication to the recovered SOAM servers</p> <p>5. Navigate to <b>Status &amp; Manage &gt; Database</b>.</p>  <p>6. Click <b>Allow Replication</b> on the recovered SOAM servers.</p> <p>7. Verify the replication on all SOAMs servers is allowed. This can be done by checking <b>Repl status</b> column of respective server</p>
45. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set HA on the recovered standby SOAM server	<p>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.</p>  <p>2. Click <b>Edit</b> at the bottom of the screen</p> <p>3. Select the recovered standby SOAM server and set it to <b>Active</b>.</p>  <p>4. Click <b>OK</b>.</p>

## Procedure 2. Recovery Scenario 2

46. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Restart DSR application	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.   </li> <li>2. Select the recovered NOAM server and click <b>Restart</b>.   </li> </ol>
47. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Start replication on working C-level servers.	<p>Un-Inhibit (start) replication to the <b>working</b> C-level Servers which belongs to the same site as of the failed SOAM servers.</p> <p><b>If the spare SOAM is also present in the site and lost</b>, execute Appendix F Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost).</p> <p><b>If the spare SOAM is NOT deployed in the site</b>, execute Appendix D Un-Inhibit A and B Level Replication on C-level Servers.</p> <ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Database</b>.   </li> <li>2. If the <b>Repl Status</b> is set to <b>Inhibited</b>, click <b>Allow Replication</b> using this order; otherwise, if none of the servers are inhibited, skip this step and continue with the next step: <ul style="list-style-type: none"> <li>• Active NOAM Server</li> <li>• Standby NOAM Server</li> <li>• Active SOAM Server</li> <li>• Standby SOAM Server</li> <li>• Spare SOAM Server (<b>if applicable</b>) — Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only</li> <li>• Active DR NOAM Server</li> <li>• Standby DR NOAM Server</li> </ul> </li> </ol>

**Procedure 2. Recovery Scenario 2**

		<ul style="list-style-type: none"><li>MP/IPFE Servers (if MPs are configured as active/standby, start with the active MP; otherwise, the order of the MPs does not matter)</li><li>SBRs (if SBR servers are configured, start with the active SBR, then standby, then spare) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only</li></ul> <p>3. Verify the replication on all the working servers is allowed. This can be done by examining the Repl Status table.</p> <table><tr><th>OAM Repl Status</th><th>SIG Repl Status</th><th>Repl Status</th><th>Repl Audit Status</th></tr><tr><td>NotApplicable</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr></table> <p><b>For SDS:</b></p> <p>Allow database replication for SOAM-A and SOAM-B servers and DP servers associated with this SOAM network element.</p> <ol style="list-style-type: none"><li>Go to the NOAMP GUI.</li><li>Select <b>[Main Menu: Status &amp; Manage → Database]</b> screen</li><li>Filter on the SOAM Network Element name.</li><li>Record the DP server hostnames (Role: MP).</li><li>Wait until audit becomes active on SOAM's. Allowing Replication: Click “Allow Replication” button for each newly replaced SOAM-A and SOAM-B servers</li></ol> <p>Allowing Replication: Click “Allow Replication” button for each DP server until all DP servers associated with this SOAM Network Element have been inhibited</p>	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status	NotApplicable	NotApplicable	Allowed	NotApplicable	Normal	NotApplicable	Allowed	NotApplicable	Normal	NotApplicable	Allowed	NotApplicable	Normal	NotApplicable	Allowed	NotApplicable
OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status																			
NotApplicable	NotApplicable	Allowed	NotApplicable																			
Normal	NotApplicable	Allowed	NotApplicable																			
Normal	NotApplicable	Allowed	NotApplicable																			
Normal	NotApplicable	Allowed	NotApplicable																			
48.	<div><input type="checkbox"/></div> Activate PCA feature. DSR only	If you have PCA installed in the system being recovered, re-activate PCA by executing the <b>PCA Activation on Entire Network</b> procedure on the recovered standby NOAM server from [7].																				
49.	<div><input type="checkbox"/></div> <b>NOAM VIP GUI:</b> Recover the C-level server (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs	<p><b>DSR:</b></p> <p>Execute the <b>Configure the MP Servers</b> procedure, steps 1 and 9-13, from reference [8].</p> <p><b>Note:</b> Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.</p> <p><b>SDS</b> (Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only):</p> <p>Execute the <b>Configure the SDS DP Servers</b> procedure, steps 1 and 5-8, from reference [8].</p> <p>Repeat this step for any remaining failed MP servers.</p>																				

Procedure 2. Recovery Scenario 2

50. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set HA on all C-level servers	<div><div>1. Navigate to <b>Status &amp; Manage -&gt; HA.</b></div><div><div><div>Status &amp; Manage</div><div>Network Elements</div><div>Server</div><div>HA</div><div>Database</div><div>KPIs</div><div>Processes</div></div></div><div>2. Click <b>Edit.</b></div><div>3. For each recovered C-Level with a Max Allowed HA Role set to <b>OOS</b>, set it to <b>Active.</b></div><div><div><div>ZombieDAMP1</div><div>Active</div><div>The maximum desired HA Role for ZombieDAMP1</div></div><div><div>ZombieDAMP2</div><div>Active</div><div>The maximum desired HA Role for ZombieDAMP2</div></div></div><div>4. Click <b>OK.</b></div></div>
51. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Restart DSR application on the recovered C-level servers	<div><div>1. Navigate to <b>Status &amp; Manage &gt; Server.</b></div><div><div><div>Status &amp; Manage</div><div>Network Elements</div><div>Server</div><div>HA</div><div>Database</div><div>KPIs</div><div>Processes</div></div></div><div>2. Select the recovered C-level servers and click <b>Restart.</b></div><div><div><div>p</div><div>Restart</div><div>Rebo</div></div></div></div>

**Procedure 2. Recovery Scenario 2**

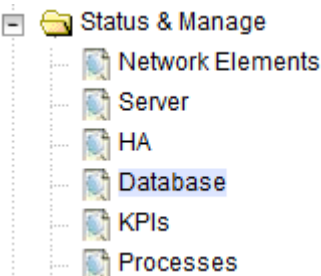

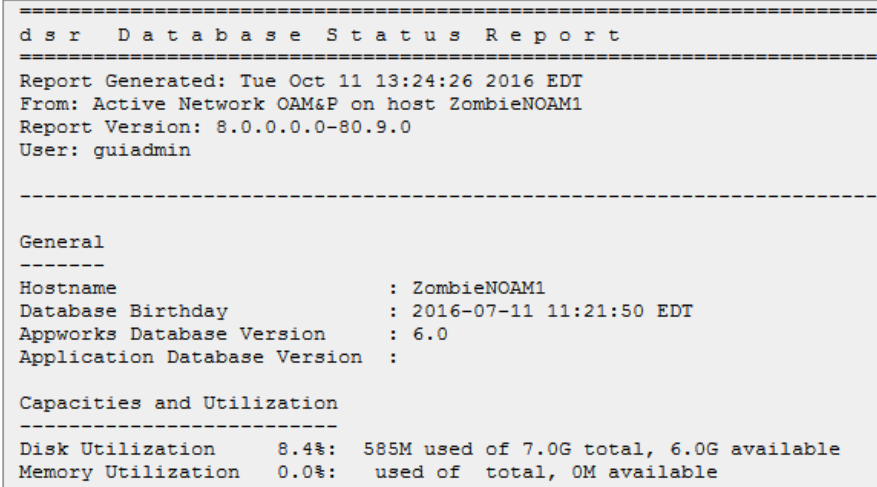
52.	<div><div><div></div></div><div><b>NOAM VIP GUI:</b> Start replication on all C-Level servers.  DSR only. If SDS, then skip to next step.</div></div>	<div>Un-Inhibit (start) replication to the <b>ALL</b> C-level servers.</div> <div><div>1. Navigate to <b>Status &amp; Manage &gt; Database</b>.</div><div><div><div><div></div><div></div><div></div><div></div><div></div><div></div></div><div><div>Status &amp; Manage</div><div>Network Elements</div><div>Server</div><div>HA</div><div>Database</div><div>KPIs</div><div>Processes</div></div></div></div></div> <div><div>2. If the <b>Repl Status</b> is set to <b>Inhibited</b>, click <b>Allow Replication</b> using this order:</div><div><div><div>• Active NOAMP Server</div><div>• Standby NOAMP Server</div><div>• Active SOAM Server</div><div>• Standby SOAM Server</div><div>• Spare SOAM Server (if applicable) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only)</div><div>• Active DR NOAM Server</div><div>• Standby DR NOAM Server</div><div>• MP/IPFE Servers</div><div>• SBRs (if SBR servers are configured, start with the active SBR, then standby, then spare) — Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only</div></div></div></div> <div><div>3. Verify the replication on all servers is allowed. This can be done by checking the <b>Repl Status</b>.</div><div><table><tr><th>OAM Repl Status</th><th>SIG Repl Status</th><th>Repl Status</th><th>Repl Audit Status</th></tr><tr><td>NotApplicable</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr></table></div></div>	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status	NotApplicable	NotApplicable	Allowed	NotApplicable	Normal	NotApplicable	Allowed	NotApplicable	Normal	NotApplicable	Allowed	NotApplicable	Normal	NotApplicable	Allowed	NotApplicable
OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status																			
NotApplicable	NotApplicable	Allowed	NotApplicable																			
Normal	NotApplicable	Allowed	NotApplicable																			
Normal	NotApplicable	Allowed	NotApplicable																			
Normal	NotApplicable	Allowed	NotApplicable																			
53.	<div><div><div></div></div><div><b>Active NOAM:</b> Perform keyexchange between the active-NOAM and recovered servers</div></div>	<div><div>1. Establish an SSH session to the active NOAM and login as <b>admusr</b>.</div><div>2. Perform a keyexchange from the active NOAM to each recovered server:</div><div><div><div>\$ keyexchange admusr@&lt;Recovered Server Hostname&gt;</div></div></div><div><div><b>Note:</b> If an export server is configured, perform this step.</div></div></div>																				

**Procedure 2. Recovery Scenario 2**

54. <input type="checkbox"/>	<b>Active NOAM:</b> Activate optional features. DSR only. If SDS, then skip to next step.	<p>Establish an SSH session to the active NOAM and login as <b>admusr</b>.</p> <p><b>Note for PCA Feature Activation:</b></p> <p>If you have PCA installed in the system being recovered, re-activate the PCA by executing the <b>PCA Activation on Stand By NOAM Server</b> procedure on the recovered standby NOAM server; and the <b>PCA Activation on Active SOAM Server</b> procedure on the recovered active SOAM server from [6].</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• If not all SOAM sites are recovered at this point, then repeat the activation for each “new” SOAM site that comes online.</li> <li>• If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature.</li> </ul> <p>Refer to section 1.5 Optional Features to activate any features that were previously activated.</p> <p><b>Note:</b> While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored:</p> <pre> i1oad#31000{S/W Fault} </pre>
---------------------------------	---	---



**Procedure 2. Recovery Scenario 2**

55. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Fetch and store the database report for the newly restored data and save it	<ol style="list-style-type: none"> <li>Navigate to <b>Status &amp; Manage &gt; Database</b>.   </li> <li>Select the active NOAM server and click <b>Report</b>.   <p>The following screen displays:</p> <p><b>Main Menu: Status &amp; Manage -&gt; Database [Report]</b></p>  </li> <li>Click <b>Save</b> and save the report to your local machine.</li> </ol>
------------------------------	---	--

**Procedure 2. Recovery Scenario 2**

56. <input type="checkbox"/>	<b>Active NOAM:</b> Verify replication between servers	<ol style="list-style-type: none"> <li>1. Log into the active NOAM as <b>admusr</b> using SSH terminal.</li> <li>2. Execute this command: <div data-bbox="516 338 1425 386" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>\$ sudo irepstat -m</pre> </div> </li> </ol> <p><b>Example output:</b></p> <pre>-- Policy 0 ActStb [DbReplication] ----- Oahu-DAMP-1 -- Active   BC From Oahu-SOAM-2 Active 0 0.50 ^0.15%cpu 25B/s A=me   CC To Oahu-DAMP-2 Active 0 0.10 0.14%cpu 25B/s A=me Oahu-DAMP-2 -- Stby   BC From Oahu-SOAM-2 Active 0 0.50 ^0.11%cpu 31B/s A=C3642.212   CC From Oahu-DAMP-1 Active 0 0.10 ^0.14 1.16%cpu 31B/s A=C3642.212 Oahu-IPFE-1 -- Active   BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 24B/s A=C3642.212 Oahu-IPFE-2 -- Active   BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 28B/s A=C3642.212 Oahu-NOAM-1 -- Stby   AA From Oahu-NOAM-2 Active 0 0.25 ^0.03%cpu 23B/s Oahu-NOAM-2 -- Active   AA To Oahu-NOAM-1 Active 0 0.25 1%R 0.04%cpu 61B/s   AB To Oahu-SOAM-2 Active 0 0.50 1%R 0.05%cpu 75B/s Oahu-SOAM-1 -- Stby   BB From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 27B/s Oahu-SOAM-2 -- Active   AB From Oahu-NOAM-2 Active 0 0.50 ^0.03%cpu 24B/s   BB To Oahu-SOAM-1 Active 0 0.50 1%R 0.04%cpu 32B/s   BC To Oahu-IPFE-1 Active 0 0.50 1%R 0.04%cpu 21B/s   BC To Oahu-SS7MP-2 Active 0 0.50 1%R 0.04%cpu 21B/s irepstat ( 40 lines) (h)elp (m)erged</pre>
---------------------------------	--	--

**Procedure 2. Recovery Scenario 2**

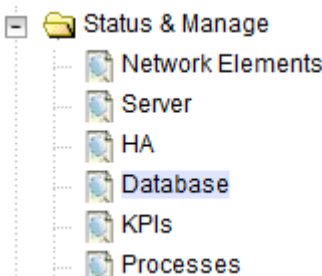
57.

☐

NOAM VIP GUI:

Verify the database states

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



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

Network Element	Server	Role	OAM Max HA Role
ZombieDRNOAM	ZombieDRNOAM1	Network OAM&P	Active
ZombieNOAM	ZombieNOAM2	Network OAM&P	Standby
ZombieSOAM	ZombieSOAM2	System OAM	N/A
ZombieNOAM	ZombieNOAM1	Network OAM&P	Active
ZombieSOAM	ZombieSOAM1	System OAM	Active
ZombieDRNOAM	ZombieDRNOAM2	Network OAM&P	Standby
ZombieSOAM	ZombieDAMP2	MP	Standby
ZombieSOAM	ZombieSS7MP2	MP	Active
ZombieSOAM	ZombieSS7MP1	MP	Active
ZombieSOAM	ZombieIPFE1	MP	Active
ZombieSOAM	ZombieIPFE2	MP	Active

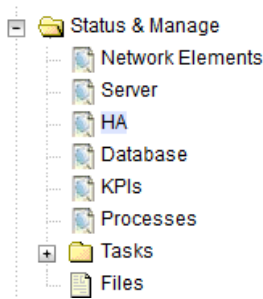
58.

☐

NOAM VIP GUI:

Verify the HA status

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

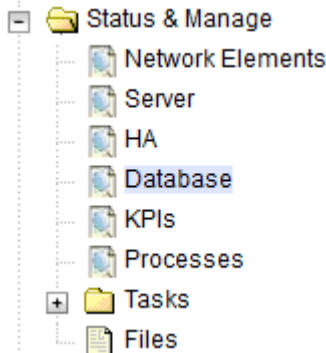
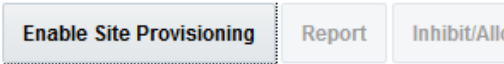
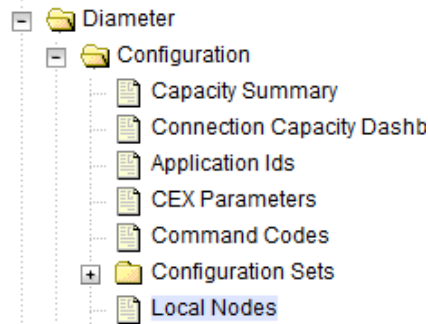
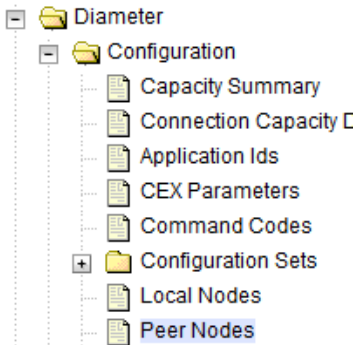


2. Select the row for all of the servers.

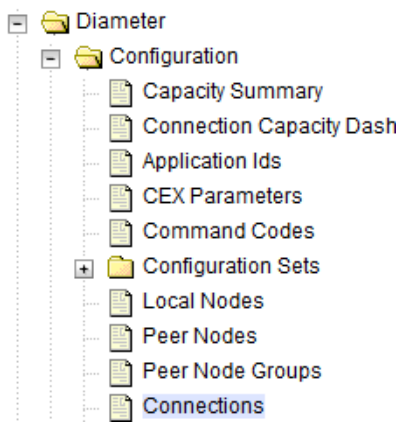
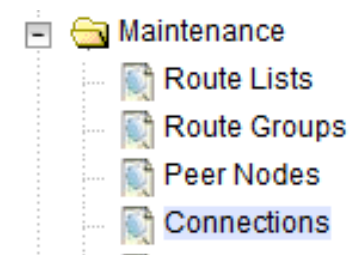
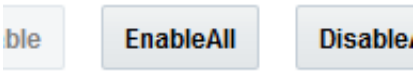
3. Verify the HA Role is either **Active** or **Standby**.

Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role
ZombieNOAM1	Active	N/A	Active
ZombieNOAM2	Standby	N/A	Active
ZombieDRNOAM1	Active	N/A	Active
ZombieDRNOAM2	Standby	N/A	Active
ZombieSOAM1	Active	N/A	Active
ZombieSOAM2	Standby	N/A	Standby

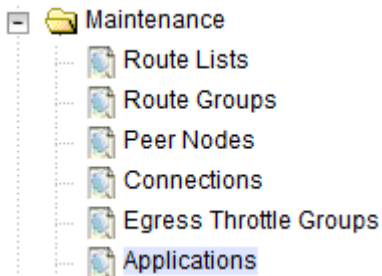
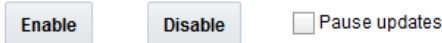
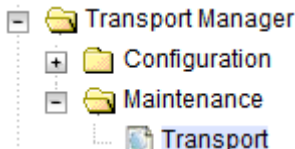

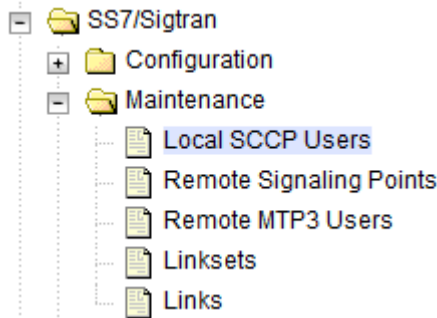
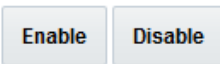
**Procedure 2. Recovery Scenario 2**

59. <input type="checkbox"/>	<b>SOAM GUI:</b> Enable site provisioning. DSR only. If SDS, skip to step 69.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Database</b>.   </li> <li>2. Click <b>Enable Site Provisioning</b>.   </li> <li>3. A confirmation window displays. Click <b>OK</b> to enable provisioning.</li> </ol>
60. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Verify local node information. DSR only. If SDS, skip to step 69.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Diameter &gt; Configuration &gt; Local Node</b>.   </li> <li>2. Verify all the local nodes are shown.</li> </ol>
61. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Verify the peer node information. DSR only. If SDS, then skip to step 69.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Diameter &gt; Configuration &gt; Peer Node</b>.   </li> <li>2. Verify all the peer nodes are shown.</li> </ol>

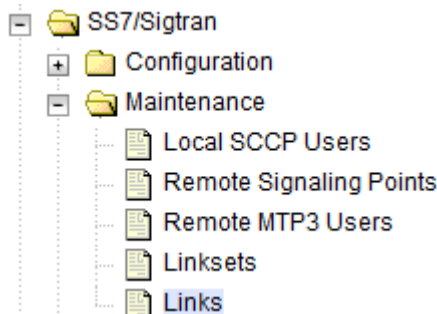

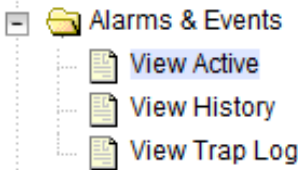
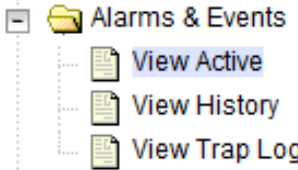
**Procedure 2. Recovery Scenario 2**

62. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Verify the connections information. DSR only. If SDS, then skip to step 69.	1. Navigate to <b>Diameter &gt; Configuration &gt; Connections</b> .  2. Verify all the connections are shown.
63. <input type="checkbox"/>	<b>MP Servers:</b> Disable SCTP Auth Flag. DSR only. If SDS, then skip to step 69.	For SCTP connections without DTLS enabled, refer to the <b>Enable/Disable DTLS (SCTP Diameter Connections Only)</b> section in reference [8]. Execute this procedure on all failed MP servers.
64. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Enable connections, if needed. DSR only. If SDS, then skip to step 69.	3. Navigate to <b>Diameter &gt; Maintenance &gt; Connections</b> .  4. Select each connection and click <b>Enable</b> . Alternatively, enable all the connections by clicking <b>EnableAll</b> .  5. Verify the Operational State is <b>Available</b> . <b>Note:</b> If a disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution

**Procedure 2. Recovery Scenario 2**

65. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Enable optional features. DSR only. If SDS, then skip to step 69.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Diameter &gt; Maintenance &gt; Applications</b>.   </li> <li>2. Select the optional feature application configured in step 72.</li> <li>3. Click <b>Enable</b>.   </li> </ol>
66. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Re-enable transports, if needed. DSR only. If SDS, then skip to step 69.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Transport Manager &gt; Maintenance &gt; Transport</b>.   </li> <li>2. Select each transport and click <b>Enable</b>.   </li> <li>3. Verify the Operational Status for each transport is <b>Up</b>.</li> </ol>
67. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 69.	<ol style="list-style-type: none"> <li>1. Navigate to <b>SS7/Sigtran &gt; Maintenance &gt; Local SCCP Users</b>.   </li> <li>2. Click the <b>Enable</b> button corresponding to MAPIWF Application Name.   </li> <li>3. Verify the SSN Status is <b>Enabled</b>.</li> </ol>

**Procedure 2. Recovery Scenario 2**

68. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Re-enable links, if needed. DSR only. If SDS, then skip to step 69.	<ol style="list-style-type: none"> <li>1. Navigate to <b>SS7/Sigtran &gt; Maintenance &gt; Links</b>.   </li> <li>2. Click <b>Enable</b> for each link.   </li> <li>3. Verify the Operational Status for each link is <b>Up</b>.</li> </ol>
69. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Examine all alarms	<ol style="list-style-type: none"> <li>1. Navigate to <b>Alarms &amp; Events &gt; View Active</b>.   </li> <li>2. Examine all active alarms and refer to the on-line help on how to address them.            If needed, contact My Oracle Support (MOS).         </li> </ol>
70. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Examine all alarms	<ol style="list-style-type: none"> <li>1. Navigate to <b>Alarms &amp; Events &gt; View Active</b>.   </li> <li>2. Examine all active alarms and refer to the on-line help on how to address them.            If needed, contact My Oracle Support (MOS).         </li> </ol>

**Procedure 2. Recovery Scenario 2**

71. <input type="checkbox"/>	<b>NOAM VIP:</b> Verify all servers in topology are accessible (RADIUS only)	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>1. Establish an SSH session to the NOAM VIP and login as <b>admusr</b>.</li> <li>2. Check if all the servers in the topology are accessible:</li> </ol> <pre>\$ /usr/TKLC/dpi/bin/ \$ ./sharedKrevo -checkAccess</pre> <p>Example output:</p> <pre>[admusr@NOAM-2 bin]\$ ./sharedKrevo -checkAccess FIPS integrity verification test failed. 1450723403: [INFO] 'NOAM-1' is accessible. FIPS integrity verification test failed. 1450723403: [INFO] 'SOAM-1' is accessible. FIPS integrity verification test failed. 1450723403: [INFO] 'SOAM-2' is accessible. FIPS integrity verification test failed. 1450723404: [INFO] 'IPFE' is accessible. FIPS integrity verification test failed. 1450723404: [INFO] 'MP-2' is accessible. FIPS integrity verification test failed. 1450723404: [INFO] 'MP-1' is accessible. [admusr@NOAM-2 bin]\$</pre> <p><b>Note:</b> If any server is not accessible, stop and contact My Oracle Support (MOS).</p>
72. <input type="checkbox"/>	<b>NOAM VIP:</b> Copy key file to all the servers in topology (RADIUS only)	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>1. Check if existing key file on active NOAM (the NOAM, which is intact and was not recovered) server is valid:</li> </ol> <pre>\$ cd /usr/TKLC/dpi/bin/ \$ ./sharedKrevo -validate</pre> <p>Example output:</p>



## Procedure 2. Recovery Scenario 2

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

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

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

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

Example output:

```
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722733: [INFO] Synched key to IPFE
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722734: NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722735: [INFO] Synched key to MP-2
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722736: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722738: [INFO] Synched key to MP-1
[admusr@NOAM-2 bin]$
```

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

Example output:

**Procedure 2. Recovery Scenario 2**

		<pre>[admusr@NOAM-1 bin]\$ ./sharedKrevo -updateData 1450203518: [INFO] Updating data on server 'NOAM-1' 1450203519: [INFO] Data updated to 'NOAM-1' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203520: [INFO] Updating data on server 'SOAM-2' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203522: [INFO] 1 rows updated on 'SOAM-2'... 1450203522: [INFO] Data updated to 'SOAM-2'</pre> <p><b>Note:</b> If any errors display, stop and contact My Oracle Support (MOS).</p>
73. <input type="checkbox"/>	Back up and archive all the databases from the recovered system	Execute Appendix A DSR Database Backup to back up the Configuration databases.
74. <input type="checkbox"/>	Recover IDIH	If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.

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

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

- Recover **Active NOAM** server by recovering base hardware, software, and the database
  - Recover the base hardware
  - Recover the software
  - Recover the database
- Recover **NOAM servers** by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover **Query Server** (if needed) by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover any failed **SOAM and MP/DP servers** by recovering base hardware and software
  - Recover the base hardware
  - Recover the software

Database is already intact at one SOAM server and does not require restoration at the other SOAM and MP/DP servers.

- Recover IDIH if necessary

### Procedure 3. Recovery Scenario 3

STEP #	<p>This procedure performs recovery if ALL NOAM servers are failed but 1 or more SOAM servers are intact. This includes any SOAM server that is in another location (spare SOAM server).</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>	
1. <input type="checkbox"/>	Gather required materials	Gather the documents and required materials listed in the Required Materials section.
2. <input type="checkbox"/>	Create a backup directory, if needed	Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.
3. <input type="checkbox"/>	Replace failed equipment	HW vendor to replace the failed equipment.
4. <input type="checkbox"/>	<b>Recover PMAC and PMAC TVOE Host:</b> Configure BIOS settings and update firmware	<ol style="list-style-type: none"> <li>1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]:             <ul style="list-style-type: none"> <li>• HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings</li> <li>• Oracle X5-2/Netra X5-2/X6-2/ X7-2: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings</li> <li>• HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings</li> </ul> </li> <li>2. Verify and/or upgrade server firmware by executing the <b>Upgrade Rack Mount Server Firmware</b> procedure from reference [8].</li> </ol>
5. <input type="checkbox"/>	<b>PMAC, TVOE Hosts, and Switch Recovery:</b> Backups available	<p>This step assumes TVOE and PMAC backups are available. If backups are <b>NOT</b> available, <b>skip this step</b>.</p> <ol style="list-style-type: none"> <li>1. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.</li> <li>2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup.</li> <li>3. Proceed to step 7.</li> </ol>
6. <input type="checkbox"/>	<b>PMAC, TVOE Hosts, and Switch Recovery:</b> Backups NOT available	<p>This step assumes TVOE and PMAC backups are <b>NOT</b> available. If the TVOE and PMAC have already been restored, <b>skip this step</b>.</p> <ol style="list-style-type: none"> <li>1. Execute the <b>Install and Configure TVOE on First RMS (PMAC Host)</b> procedure from reference [8].</li> <li>2. Execute the <b>Install PMAC</b> procedure from reference [8].</li> <li>3. Execute the <b>Initialize the PMAC Application</b> section from reference [8].</li> </ol>

**Procedure 3. Recovery Scenario 3**

7. <input type="checkbox"/>	Recovery failed Cisco 4948 aggregation switches (HP DL380 only)	<p>Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 GEN 9, <b>skip this step.</b></p> <p>Recover failed Cisco 4948 aggregation switches, if needed:</p> <ol style="list-style-type: none"> <li>1. Back up available configuration files. Refer to Appendix C Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only) to recover failed Cisco 4948 aggregation switches.</li> <li>2. Back up configuration files NOT available. Execute <b>Configure Cisco 4948E-F Aggregation Switches (HP DL 380 Gen 8 Only)</b> section from reference [8].</li> </ol>
8. <input type="checkbox"/>	Configure PMAC (no backup)	<p>If PMAC backup was <b>NOT</b> restored in step 5, execute this step; otherwise skip this step.</p> <p>Execute the <b>Configure PMAC Server (NetBackup Only)</b> and <b>Add RMS to the PMAC Inventory</b> sections from reference [8].</p>
9. <input type="checkbox"/>	Install/Configure additional rack mount servers	<ol style="list-style-type: none"> <li>1. Execute the <b>Install TVOE on Additional Rack Mount Servers</b> procedure from reference [8].</li> <li>2. <b>If backups are available</b>, restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.</li> </ol> <p><b>If backups are NOT available</b>, execute the <b>Configure TVOE on Additional Rack Mount Servers</b> procedure from reference [8].</p>
10. <input type="checkbox"/>	Configure BIOS settings and update firmware on additional rack mount servers	<ol style="list-style-type: none"> <li>1. Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]: <ul style="list-style-type: none"> <li>• HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings</li> <li>• Oracle X5-2/Netra X5-2/X6-2/ X7-2: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings</li> <li>• HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings</li> </ul> </li> <li>2. Verify and/or upgrade server firmware by executing the <b>Upgrade Rack Mount Server Firmware</b> procedure from reference [8].</li> </ol>
11. <input type="checkbox"/>	Determine VM Placement and Socket Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 only)	<p>HP DL380 GEN 8, skip this step.</p> <p>Determine VM placement and pinning by following:</p> <ol style="list-style-type: none"> <li>1. From this document, section 3.1, item 14, to determine the VM placement; and</li> <li>2. In reference [8], Appendix S VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1 Gbps NICs) and CPU Pinning in HP DL380 Gen 9 (Onboard 1 Gbps NICs) for Pinning Information on HP DL380 Gen 9.</li> </ol>
12. <input type="checkbox"/>	Deploy redundant PMAC, if required	Refer to the <b>Deploy Redundant PMAC (Optional)</b> procedure to re-deploy and configure any redundant PMACs previously configured.

**Procedure 3. Recovery Scenario 3**

13. <input type="checkbox"/>	<b>PMAC:</b> Determine if the fdconfig file exists from the initial deployment	<p>1. Type:</p> <pre>[admusr@melbourne-pmac-1 ~]\$ ll /usr/TKLC/smac/etc/fdc/</pre> <p>2. Examine the results and verify if the <b>rms config file &lt;hostname&gt;.cfg</b> exists.</p> <p><b>Note:</b> There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS.</p>
14. <input type="checkbox"/>	Create fdconfig backup file, if it does not already exist	<p>Execute this step <b>ONLY</b> If the fdconfig backup file does <b>NOT</b> exist.</p> <p>1. Create the needed file(s) by executing the <b>Virtual Machine/Network Fast Deployment</b> section from reference [8].</p> <p style="text-align: center;"><b>WARNING</b></p> <p style="color: red;">It is very important to ensure the file(s) created only affects the TVOE server(s) and the guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.</p> <p>2. Skip to step 23. if this step was executed.</p>
15. <input type="checkbox"/>	<b>PMAC:</b> Load ISOs into PMAC, if not done already	If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the <b>Virtual Machine/Network Fast Deployment</b> section from reference [8].
16. <input type="checkbox"/>	<b>PMAC:</b> Edit/Update configuration file	<p>Edit the fdconfig file to include only the required/failed servers.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Comment out configuration items that are not needed.</li> <li>• Create a separate configuration file for EACH rack mount server being deployed.</li> <li>• The Cabinet ID in the config file needs to match the cabinet already defined in PMAC.</li> </ul> <p>The following items are mandatory:</p> <ul style="list-style-type: none"> <li>• siteName</li> <li>• tpdIso</li> <li>• dsrIso (if DSR VMs are being configured)</li> <li>• sdsIso (if SDS VMs are being configured)</li> <li>• NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured)</li> <li>• XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured)</li> <li>• XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured)</li> <li>• DSRNOAM1XMIIPADDRESS (if DSRNOAM1 is being configured)</li> <li>• DSRNOAM2XMIIPADDRESS (if DSRNOAM2 is being configured)</li> <li>• DSRDRNOAM1XMIIPADDRESS (if DSRDRNOAM1 is being configured)</li> <li>• DSRDRNOAM2XMIIPADDRESS (if DSRDRNOAM2 is being configured)</li> </ul>

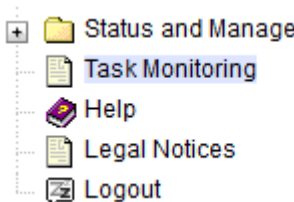
**Procedure 3. Recovery Scenario 3**

		<ul style="list-style-type: none"> <li>• SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured)</li> <li>• SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured)</li> <li>• SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured)</li> <li>• SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured)</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].</li> <li>• Comment out SDS and DSR profile items if corresponding products are not used.</li> <li>• For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9: Refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].</li> <li>• VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName.</li> <li>• VM locations should not be changed from their <b>RMSx</b> format. Each RMS should correspond to a separate rack mount server.</li> </ul> <p style="text-align: center;"><b>WARNING</b></p> <p>Ensure the file(s) created only affect the TVOE server(s) and guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.</p>
17.	<input type="checkbox"/> <b>PMAC:</b> Copy the backed up fdconfig file to the RMS directory	<p>Copy the fdconfig backup file to the RMS directory.</p> <pre>\$ sudo cp /usr/TKLC/smac/etc/fdc/&lt;backup_fdc_file&gt; /usr/TKLC/smac/etc/RMS/</pre>

## Procedure 3. Recovery Scenario 3

18. <input type="checkbox"/>	<b>PMAC:</b> Execute the config.sh script	<p>Execute <b>config.sh</b> against the modified backup config file.</p> <p><b>Note:</b> If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again.</p> <pre>\$ sudo ./config.sh &lt;config file&gt;</pre> <p>Example output:</p> <pre>[admusr@5010441PMAC RMS]\$ sudo ./config.sh rms.cfg Validating cfg file... Successful validation of cfg file. Added Cabinet 101 to Fast Deployment File. Added Zombie_TVOE1 to Fast Deployment File. Added Zombie_TVOE2 to Fast Deployment File. Added xmi(bond0.4) to Fast Deployment File. Added imi(bond0.3) to Fast Deployment File. Added rep(bond1.10) to Fast Deployment File. Added xsi1(bond1.6) to Fast Deployment File. Added xsi2(bond1.7) to Fast Deployment File. Added xsi3(bond1.8) to Fast Deployment File. Added xsi4(bond1.9) to Fast Deployment File. Added xsi5(bond1.11) to Fast Deployment File. Added xsi6(bond1.12) to Fast Deployment File. Added xsi7(bond1.13) to Fast Deployment File. Added xsi8(bond1.14) to Fast Deployment File. Added xsi9(bond1.15) to Fast Deployment File. Added xsi10(bond1.16) to Fast Deployment File. Added xsi11(bond1.17) to Fast Deployment File. Added xsi12(bond1.18) to Fast Deployment File. Added xsi13(bond1.19) to Fast Deployment File. Added xsi14(bond1.20) to Fast Deployment File. Added xsi15(bond1.21) to Fast Deployment File. Added xsi16(bond1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRDRNOAM1 to Fast Deployment File. Added Zombie_DSRDRNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SSDRNOAM1 to Fast Deployment File. Added Zombie_SSDRNOAM2 to Fast Deployment File. Added Zombie_DSRSOAM1 to Fast Deployment File. Added Zombie_DSRSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM1 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDAMP2 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_DSRIPFE2 to Fast Deployment File. Added Zombie_SSDPSV1 to Fast Deployment File. Added Zombie_SSDPSV2 to Fast Deployment File. Validating Fast Deployment File..... Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!! [admusr@5010441PMAC RMS]\$</pre>
---------------------------------	---	--

**Procedure 3. Recovery Scenario 3**


19.	<div><input type="checkbox"/></div> <b>PMAC:</b> Execute fast deployment	<div>With the file generated from the config.sh script, execute the following command to start fast deployment:</div> <div><pre>\$ screen \$ sudo fdconfig config --file=&lt;fd_config.xml&gt;</pre></div> <div><b>Note:</b> This is a long duration command. If the screen command was run before executing the fdconfig, perform a <b>screen -dr</b> to resume the screen session in the event of a terminal timeout, etc.</div>																																																															
20.	<div><input type="checkbox"/></div> <b>PMAC GUI:</b> Monitor the configuration	<div><div>1. If not already done, establish a GUI session on the PMAC server.</div><div>2. Navigate to <b>Task Monitoring</b>.</div><div></div><div>3. Monitor the configuration to completion:</div><div><div>Main Menu: Task Monitoring</div><div><div>Filter*</div><table><tr><th>ID</th><th>Task</th><th>Target</th><th>Status</th><th>State</th><th>Task Output</th><th>Running Time</th><th>Start Time</th><th>Progress</th></tr><tr><td>925</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_SDSRNOAM1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:04</td><td>2016-07-11 11:27:35</td><td>100%</td></tr><tr><td>924</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_SDSNOAM1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:04</td><td>2016-07-11 11:27:04</td><td>100%</td></tr><tr><td>923</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_DSRIPE1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:06</td><td>2016-07-11 11:26:43</td><td>100%</td></tr><tr><td>922</td><td>Accept</td><td>RMS: pc5010439 Guest: Zombie_DSRDAMP2</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:05</td><td>2016-07-11 11:26:43</td><td>100%</td></tr><tr><td>921</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_DSRDAMP1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:05</td><td>2016-07-11 11:26:43</td><td>100%</td></tr><tr><td>920</td><td>Accept</td><td>RMS: pc5010439 Guest: Zombie_DSRSOAM2</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:06</td><td>2016-07-11 11:26:42</td><td>100%</td></tr></table></div></div><div><b>Note:</b> If a failure occurs with fdconfig, logs can be accessed in <b>/var/TKLC/log/fdconfig/fdconfig.log</b> file.</div><div><pre>[admusr@melbourne-pmac-1 fdconfig]\$ sudo fdconfig dumpsteps -- file=deploy_melbourne_20170329T202458_701b.fdcdb Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb" Here are the steps that were generated ----- begin ----- Dump of DB steps: NUM PHS DLY INFRA ID SVRTYPE CMD ELEMENT PRE STATE TO BGTS COMMAND TEXT ----- 1 1 0 pmac Fast_Deployment 0 21 0 Complete 300 0 Check PM&amp;C is available 2 1 0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet 3 1 0 pmac Fast_Deployment 0 3 melbourne_RMS3 1 Skipped 900 0 Add Rms 4 2 0 pmac Fast_Deployment 1</pre></div><div>4. Restart the fdconfig after a failure has occurred and has been resolved:</div><div><pre>\$ sudo fdconfig restart -- file=deploy_melbourne_20170329T202458_701b.fdcdb</pre></div></div>	ID	Task	Target	Status	State	Task Output	Running Time	Start Time	Progress	925	Accept	RMS: pc5010441 Guest: Zombie_SDSRNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:35	100%	924	Accept	RMS: pc5010441 Guest: Zombie_SDSNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:04	100%	923	Accept	RMS: pc5010441 Guest: Zombie_DSRIPE1	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:43	100%	922	Accept	RMS: pc5010439 Guest: Zombie_DSRDAMP2	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%	921	Accept	RMS: pc5010441 Guest: Zombie_DSRDAMP1	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%	920	Accept	RMS: pc5010439 Guest: Zombie_DSRSOAM2	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:42	100%
ID	Task	Target	Status	State	Task Output	Running Time	Start Time	Progress																																																									
925	Accept	RMS: pc5010441 Guest: Zombie_SDSRNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:35	100%																																																									
924	Accept	RMS: pc5010441 Guest: Zombie_SDSNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:04	100%																																																									
923	Accept	RMS: pc5010441 Guest: Zombie_DSRIPE1	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:43	100%																																																									
922	Accept	RMS: pc5010439 Guest: Zombie_DSRDAMP2	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%																																																									
921	Accept	RMS: pc5010441 Guest: Zombie_DSRDAMP1	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%																																																									
920	Accept	RMS: pc5010439 Guest: Zombie_DSRSOAM2	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:42	100%																																																									



**Procedure 3. Recovery Scenario 3**

21. <input type="checkbox"/>	<b>PMAC:</b> Repeat for each rack mount server configuration file	Repeat steps 13. -20. for each rack mount server/configuration file, if required.
22. <input type="checkbox"/>	<b>PMAC:</b> Back up FDC file	<ol style="list-style-type: none"> <li>Copy the updated fdc file to the fdc backup directory:  <pre>\$ sudo cp /usr/TKLC/smac/etc/RMS/&lt;fdc_file&gt; /usr/TKLC/smac/etc/fdc/</pre> </li> <li>Change permissions:  <pre>\$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/&lt;fdc_file&gt;</pre> </li> </ol>
23. <input type="checkbox"/>	Perform CPU pinning	Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the <b>CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only)</b> procedure from reference [8].
24. <input type="checkbox"/>	Obtain latest database backup and network configuration data	<ol style="list-style-type: none"> <li>Obtain the most recent database backup file from external backup sources (for example, file servers) or tape backup sources.</li> <li>Obtain most recent <b>RADIUS shared secret encryption key</b> from the <b>DpiKf.bin.encr</b> file on external backup sources (only when the RADIUS key revocation MOP has been executed on the system).</li> <li>From required materials list in the Required Materials section, use the site survey documents and Network Element report (if available) to determine network configuration data.</li> </ol>
25. <input type="checkbox"/>	Execute DSR installation procedure for the first NOAM	<p>Verify the networking data for network elements.</p> <p><b>Notes</b></p> <ul style="list-style-type: none"> <li>Use the backup copy of network configuration data and site surveys from step 2.</li> <li>SDS disaster recovery actions can and should be worked simultaneously to allow faster recovery of the complete solution (that is, stale DB on DP servers do not receive updates until SDS-SOAM servers are recovered). The following steps accommodate both DSR and SDS disaster recovery steps.</li> </ul> <p><b>Important:</b> While creating the first NOAMs in this step, it is important that the server hostname is the same as one of the NOAM hostnames used prior to the disaster.</p> <p><b>DSR:</b></p> <ol style="list-style-type: none"> <li>Configure the first NOAM server by executing the <b>Configure First NOAM NE and Server</b> procedure from reference [8].</li> <li>Configure the NOAM server group by executing the <b>Configure the NOAM Server Group</b> procedure from reference [8].</li> </ol> <p><b>SDS:</b></p> <ol style="list-style-type: none"> <li>Configure the first SDS NOAM server by executing <b>Configure First SDS NOAM NE and Server</b> procedure from reference [8].</li> <li>Configure the SDS NOAM server group by executing the <b>Configure the SDS NOAM Server Group</b> procedure from reference [8].</li> <li>Skip to step 31.</li> </ol>

**Procedure 3. Recovery Scenario 3**

<p>26. <input type="checkbox"/></p>	<p><b>NOAM GUI:</b> Login DSR only. If SDS, skip to step 31. If the failed server is not OAM, then skip to step 37.</p>	<ol style="list-style-type: none"> <li>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  <div data-bbox="565 323 1370 369" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <code>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</code> </div> </li> <li>2. Login as the <b>guiadmin</b> user:</li> </ol> <div data-bbox="548 449 1380 1226" style="text-align: center;">  <p>The screenshot shows the Oracle System Login page. At the top is the Oracle logo in red. Below it is the text 'Oracle System Login' followed by a horizontal line and the date 'Mon Jul 11 13:59:37 2016 EDT'. In the center is a 'Log In' box with the text 'Enter your username and password to log in'. Inside this box are fields for 'Username:' and 'Password:', a 'Change password' checkbox, and a 'Log In' button. Below the box is the text 'Welcome to the Oracle System Login.' followed by a paragraph about browser compatibility and a link to the 'Oracle Software Web Browser Support Policy'. Below that is the text 'Unauthorized access is prohibited.' and a footer with copyright information.</p> </div>
-------------------------------------	---	--

## Procedure 3. Recovery Scenario 3

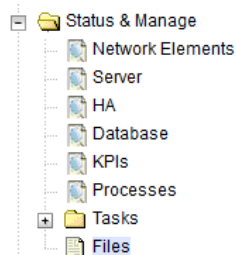
27.

**NOAM GUI:**

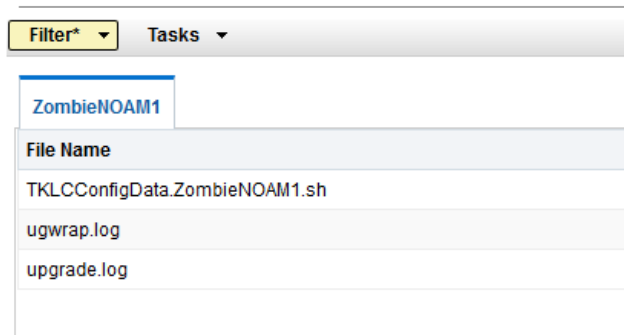
Upload the backup database file.

DSR only. If SDS, skip to step 31.

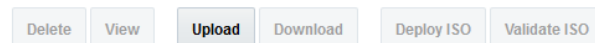
1. Navigate to **Status & Manage > Files**.



2. Select the active NOAM server.

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

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

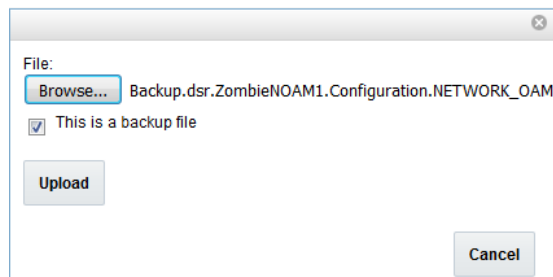


40 KB used (0.00%) of 15.7 GB available | System utilization: 867.9 MB (5.39%) of 15.7 GB available.

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

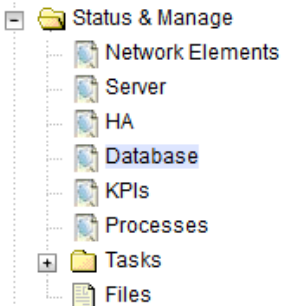


**Note:** If there is no backup file, refer to Appendix L Backup Directory to create the backup directory.

5. Click **Open**.
6. Mark the **This is a backup file** checkbox.
7. Click **Upload**.

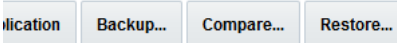
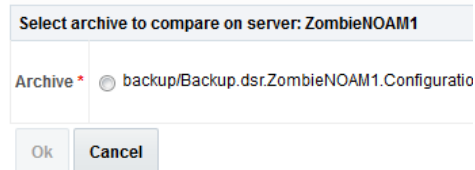
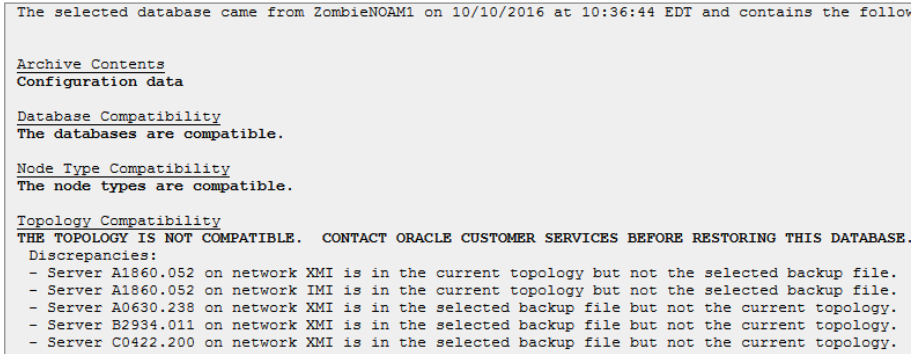


The file takes a few seconds to upload depending on the size of the backup data. The file is visible on the list of entries after the upload is complete.


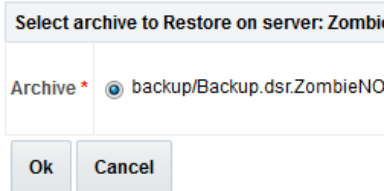
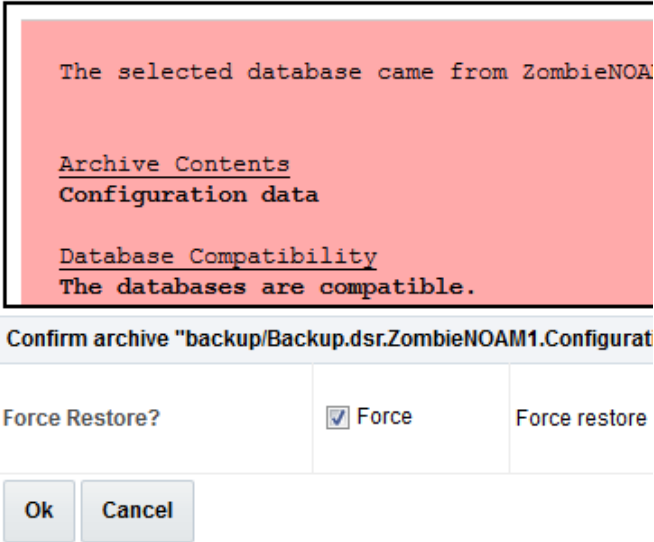
**Procedure 3. Recovery Scenario 3**

28. <input type="checkbox"/>	<b>NOAM GUI:</b> Disable provisioning. DSR only. If SDS, skip to step 31.	<ol style="list-style-type: none"><li>1. Navigate to <b>Status &amp; Manage &gt; Database</b>. </li><li>2. Click <b>Disable Provisioning</b>. </li><li>3. Click <b>OK</b> to disable Provisioning. </li></ol>
------------------------------	---	--

**Procedure 3. Recovery Scenario 3**

<p>29. <input type="checkbox"/></p>	<p><b>NOAM GUI:</b> Verify the archive contents and database compatibility. DSR only. If SDS, skip to step 31.</p>	<ol style="list-style-type: none"> <li>1. Select the active NOAM server and click <b>Compare</b>.</li> </ol>  <ol style="list-style-type: none"> <li>2. Click the button for the restored database file uploaded as a part of step 27. of this procedure.</li> </ol> <p><b>Database Compare</b></p>  <ol style="list-style-type: none"> <li>3. <b>Verify</b> the output window matches the screen below.</li> </ol> <p><b>Note:</b> A database mismatch regarding the Topology Compatibility and possibly User compatibility (due to authentication) display. These warnings are expected. If these are the only mismatches, proceed; otherwise, stop and contact My Oracle Support (MOS) to ask for assistance.</p> <p><b>Database Archive Compare</b></p>  <p><b>Note:</b> Archive Contents and Database Compatibilities must be the following:</p> <p><b>Archive Contents:</b> Configuration data.</p> <p><b>Database Compatibility:</b> The databases are compatible.</p> <p><b>Note:</b> The following is expected output for Topology Compatibility Check since we are restoring from an existing backed up database to a database with just one NOAM:</p> <p><b>Topology Compatibility</b> The topology should be compatible minus the NODEID.</p> <p><b>Note:</b> We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility.</p> <ol style="list-style-type: none"> <li>4. If the verification is successful, click <b>Back</b> and continue to <b>next step</b> in this procedure.</li> </ol>
-------------------------------------	--	---


**Procedure 3. Recovery Scenario 3**

<p>30. <input type="checkbox"/></p>	<p><b>Active NOAM:</b> Restore the database. DSR only. If SDS, skip to step 31.</p>	<ol style="list-style-type: none"> <li>From <b>Status &amp; Manage &gt; Database</b>.</li> <li>Select the active NOAM server and click <b>Restore</b>. </li> <li>Select the proper backup provisioning and configuration file. </li> <li>Click <b>OK</b>.</li> <li>If you get errors related to the warnings highlighted in the previous step, then it is expected. If no other errors display, then mark the <b>Force</b> checkbox and click <b>OK</b> to proceed with the DB restore.</li> </ol> <p><b>Database Restore Confirm</b></p> <p>Incompatible archive selected</p>  <p><b>Note:</b> After the restore has started, the user is logged out of the XMI NO GUI since the restored topology is old data.</p> <ol style="list-style-type: none"> <li>Go to step 37.</li> </ol>
-------------------------------------	---	---

**Procedure 3. Recovery Scenario 3**

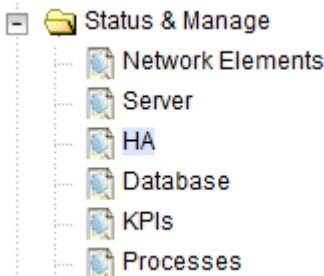
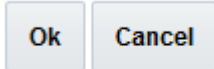
31. <input type="checkbox"/>	<b>SDS NOAM:</b> Transfer SDS configuration and provisioning backup database files.  SDS only. If DSR, skip to step 37.	<p>Using the IP of the recovered SDS NOAM, transfer the uncompressed backup database files to the <b>/var/TKLC/db/filemgmt</b> directory.</p> <p><b>Linux:</b></p> <ol style="list-style-type: none"> <li>1. From the command line of a Linux machine, copy the configuration backup file to the SDS NOAM guest: <div data-bbox="565 432 1424 510" style="border: 1px solid black; padding: 5px;"> <pre># scp &lt;path_to_configuration_db_file&gt; admusr@&lt;SDS_NOAM_IP&gt;:/var/TKLC/db/filemgmt</pre> </div> </li> <li>2. From the command line of a Linux machine, copy the provisioning backup file to the SDS NOAM guest: <div data-bbox="565 594 1424 672" style="border: 1px solid black; padding: 5px;"> <pre># scp &lt;path_to_provisioning_db_file&gt; admusr@&lt;SDS_NOAM_IP&gt;:/var/TKLC/db/filemgmt</pre> </div> </li> </ol> <p>where <b>&lt;path_to_db_file&gt;</b> is the path to the backup database file on the local system and <b>&lt;SDS_NOAM_IP&gt;</b> is the recovered SDS NOAM IP address.</p> <p><b>Windows:</b></p> <p>Use WinSCP to copy the backup database files into the <b>/var/TKLC/db/filemgmt</b> directory. Refer to the <b>Using WinSCP</b> procedure in reference [9] to copy the backup image to the customer system.</p>
32. <input type="checkbox"/>	<b>SDS NOAM:</b> Login. SDS only. If DSR, skip to step 37.	Establish an SSH session to the SDS active NOAM XMI IP address and login as <b>admusr</b> .
33. <input type="checkbox"/>	<b>SDS NOAM:</b> Stop running applications. SDS only. If DSR, skip to step 37.	<p>Issue the following command to stop running applications. Leave database running:</p> <div data-bbox="516 1144 1328 1192" style="border: 1px solid black; padding: 5px;"> <pre>\$ sudo prod.stop --ignore-cap</pre> </div> <p><b>Note:</b> This step may take several minutes to complete.</p>
34. <input type="checkbox"/>	<b>SDS NOAM:</b> Restore configuration database. SDS only. If DSR, skip to step 37.	<p>Restore the configuration DB by executing the following command:</p> <div data-bbox="516 1304 1424 1381" style="border: 1px solid black; padding: 5px;"> <pre>\$ sudo idb.restore -n -t /var/TKLC/db/filemgmt -v &lt;full path to configuration archive file name&gt;</pre> </div>
35. <input type="checkbox"/>	<b>SDS NOAM:</b> Restore provisioning database. SDS only. If DSR, skip to step 37.	Refer to Appendix I Restore Provisioning Database to restore the provisioning database.
36. <input type="checkbox"/>	<b>SDS NOAM:</b> Start running applications. SDS only. If DSR, skip to step 37.	<p>Start the SDS application by executing the following command:</p> <div data-bbox="516 1717 1328 1766" style="border: 1px solid black; padding: 5px;"> <pre>\$ sudo prod.start</pre> </div>

## Procedure 3. Recovery Scenario 3

37. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Login	<ol style="list-style-type: none"> <li>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  <div style="border: 1px solid black; padding: 2px; margin: 5px 0;">http://&lt;Primary_NOAM_VIP_IP_Address&gt;</div> </li> <li>2. Login as the <b>guiadmin</b> user:</li> </ol> <div style="text-align: center; margin: 20px 0;">  </div> <div style="text-align: center;"> <b>Oracle System Login</b> </div> <div style="text-align: right; margin-top: 5px;">Mon Jul 11 13:59:37 2016 EDT</div> <div style="text-align: center; margin: 20px 0;"> <div style="border: 1px solid #ccc; padding: 10px; width: 300px; margin: 0 auto;"> <p><b>Log In</b></p> <p>Enter your username and password to log in</p> <p>Username: <input style="width: 100%;" type="text"/></p> <p>Password: <input style="width: 100%;" type="password"/></p> <p style="text-align: center;"><input type="checkbox"/> Change password</p> <p style="text-align: center;"><input type="button" value="Log In"/></p> </div> </div> <p style="text-align: center; margin-top: 10px;">Welcome to the Oracle System Login.</p> <p style="text-align: center; font-size: small;">This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the <a href="#">Oracle Software Web Browser Support Policy</a> for details.</p> <p style="text-align: center; font-size: small;">Unauthorized access is prohibited.</p> <hr style="width: 50%; margin: 10px auto;"/> <p style="text-align: center; font-size: x-small;">Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</p> <p style="text-align: center; font-size: x-small;">Copyright © 2010, 2016, <a href="#">Oracle</a> and/or its affiliates. All rights reserved.</p>
38. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Monitor and confirm database restore	<ol style="list-style-type: none"> <li>1. Wait for <b>5-10 minutes</b> for the system to stabilize with the new topology:</li> <li>2. Monitor the Info tab for <b>Success</b>. This indicates the restore is complete and the system is stabilized.</li> </ol> <p>Ignore these alarms for NOAM and MP servers until all the servers are configured:</p> <ul style="list-style-type: none"> <li>• Alarms with Type Column as <b>REPL, COLL, HA</b> (with mate NOAM), <b>DB</b> (about Provisioning Manually Disabled).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Do not pay attention to alarms until all the servers in the system are completely restored.</li> <li>• The Configuration and Maintenance information is in the same state it was when backed up during initial backup.</li> </ul>



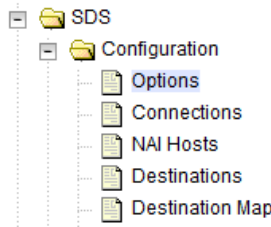

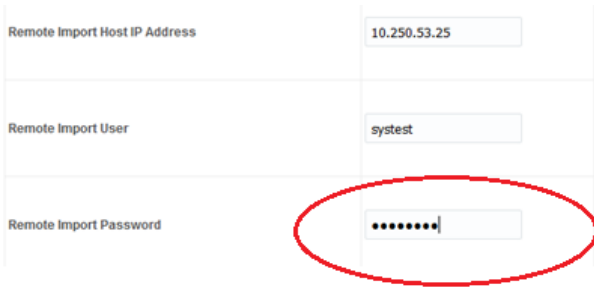


**Procedure 3. Recovery Scenario 3**

39. <input type="checkbox"/>	<b>Active NOAM:</b> Set failed servers to OOS	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>2. Click <b>Edit</b>.</li> <li>3. Set the Max Allowed HA Role option to <b>OOS</b> for the failed servers.   <b>Modifying HA attributes</b>  <table border="1" data-bbox="521 758 1057 1104"> <thead> <tr> <th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td><td>Active</td><td>The maximum des</td></tr> <tr> <td>ZombieNOAM2</td><td>OOS</td><td>The maximum des</td></tr> <tr> <td>ZombieDRNOAM1</td><td>OOS</td><td>The maximum des</td></tr> </tbody> </table> </li> <li>4. Click <b>OK</b>.   </li> </ol>	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active	The maximum des	ZombieNOAM2	OOS	The maximum des	ZombieDRNOAM1	OOS	The maximum des
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active	The maximum des												
ZombieNOAM2	OOS	The maximum des												
ZombieDRNOAM1	OOS	The maximum des												
40. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover standby NOAM	Install the second NOAM server: <b>DSR:</b> Execute the <b>Configure the Second NOAM Server</b> procedure, steps 1, 3-6, from reference [8]. <b>SDS:</b> Execute the <b>Configure the Second SDS NOAM Server</b> procedure, steps 1, 3-6, from reference [8].												
41. <input type="checkbox"/>	Install NetBackup client (optional)	If NetBackup is used, execute the <b>Install NetBackup Client (Optional)</b> procedure from reference [8].												

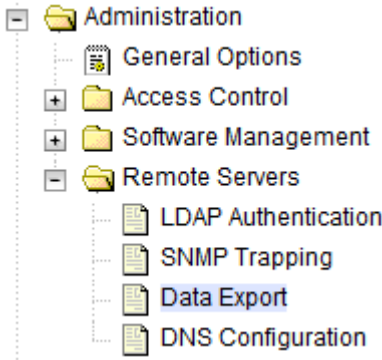
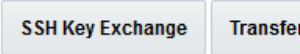
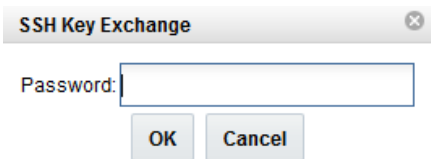
Procedure 3. Recovery Scenario 3

42.	<div><div></div><div>NOAM VIP GUI: Set HA on standby NOAM</div></div>	<div><div><div>1. Navigate to <b>Status &amp; Manage &gt; HA.</b></div><div><div><div>Status &amp; Manage</div><div>Network Elements</div><div>Server</div><div>HA</div><div>Database</div><div>KPIs</div><div>Processes</div><div>Tasks</div><div>Files</div></div></div></div><div><div>2. Click <b>Edit.</b></div><div>3. Select the standby NOAM server and set it to <b>Active.</b></div><div><div>Modifying HA attributes</div><table><thead><tr><th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr></thead><tbody><tr><td>ZombieNOAM1</td><td>Active</td><td>The maximum</td></tr><tr><td>ZombieNOAM2</td><td>Active</td><td>The maximum</td></tr><tr><td>ZombieDRNOAM1</td><td>Active Standby Snare</td><td>The maximum</td></tr></tbody></table></div><div>4. Click <b>OK.</b></div></div></div>	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active	The maximum	ZombieNOAM2	Active	The maximum	ZombieDRNOAM1	Active Standby Snare	The maximum
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active	The maximum												
ZombieNOAM2	Active	The maximum												
ZombieDRNOAM1	Active Standby Snare	The maximum												
43.	<div><div></div><div>NOAM VIP GUI: Restart DSR application</div></div>	<div><div><div>1. Navigate to <b>Status &amp; Manage &gt; Server.</b></div><div><div><div>Status &amp; Manage</div><div>Network Elements</div><div>Server</div><div>HA</div><div>Database</div><div>KPIs</div><div>Processes</div><div>Tasks</div><div>Files</div></div></div></div><div><div>2. Select the recovered standby NOAM server and click <b>Restart.</b></div><div><div>op</div><div>Restart</div><div>Rebo</div></div></div></div>												

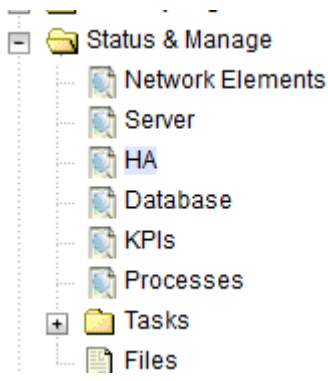
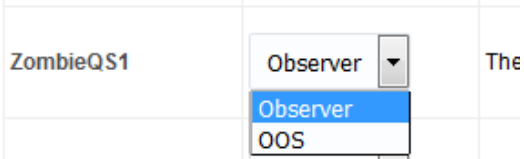
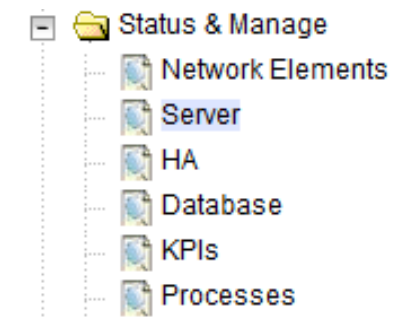
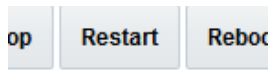
**Procedure 3. Recovery Scenario 3**

44. <input type="checkbox"/>	<b>Active NOAM:</b> Correct the recognized authority table	<ol style="list-style-type: none"> <li>1. Establish an SSH session to the active NOAM and login as <b>admusr</b>.</li> <li>2. Execute this command: <div data-bbox="521 338 1422 537" style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <pre>\$ sudo top.setPrimary - Using my cluster: A1789 - New Primary Timestamp: 11/09/15 20:21:43.418 - Updating A1789.022: &lt;DSR_NOAM_B_hostname&gt; - Updating A1789.144: &lt;DSR_NOAM_A_hostname&gt;</pre> </div> </li> </ol>
45. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Perform Keyexchange with remote import server. SDS only. If DSR, skip to step 47.	<ol style="list-style-type: none"> <li>1. Navigate to <b>SDS &gt; Configuration &gt; Options</b>.   </li> <li>2. Unmark the <b>Remote Import Enabled</b> checkbox.   </li> <li>3. Click <b>Apply</b>.  <b>Note:</b> Navigate to <b>SDS &gt; Configuration &gt; Options</b> again to clear the banner. </li> <li>4. Enter the <b>Remote Import Password</b>.   </li> <li>5. Click <b>Apply</b>.   </li> <li>6. Mark the <b>Remote Import Enabled</b> checkbox.   </li> </ol>

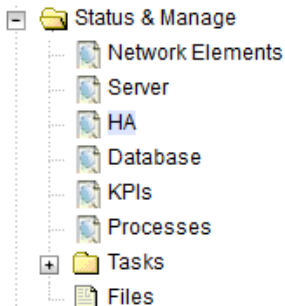
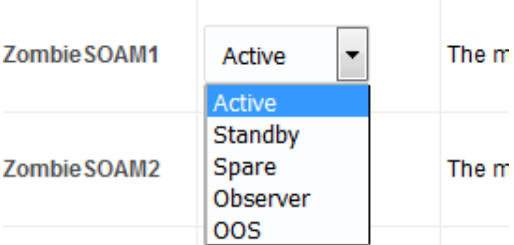
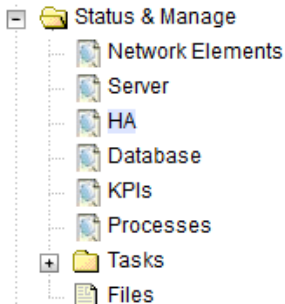
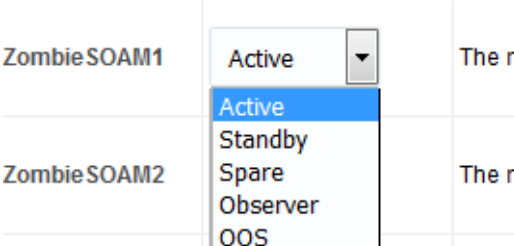
**Procedure 3. Recovery Scenario 3**

46. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Repeat for remote export server. SDS only. If DSR, skip to step 47.	Repeat step 45. for the remote export server.
47. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Perform Keyexchange with export server	<p>1. Navigate to <b>Administration &gt; Remote Servers &gt; Data Export</b>.</p>  <p>2. Click <b>SSH Key Exchange</b>.</p>  <p>3. Type the <b>Password</b> and click <b>OK</b>.</p> 
48. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover query servers. SDS only. If DSR, skip to step 51.	Execute the <b>Configuring SDS Query Servers</b> procedure, steps 1, 4-7, from reference [8].

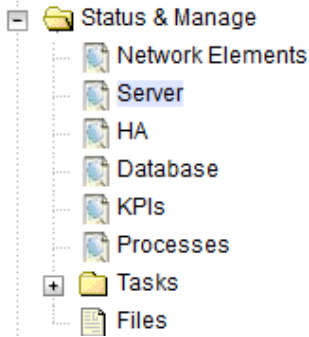

**Procedure 3. Recovery Scenario 3**

49. <input type="checkbox"/>	<b>SDS NOAM VIP GUI:</b> Set HA on query server. SDS only. If DSR, skip to step 51.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>2. Click <b>Edit</b>.</li> <li>3. Select the query server and select <b>Observer</b>.   </li> <li>4. Click <b>OK</b>.</li> </ol>
50. <input type="checkbox"/>	<b>SDS NOAM VIP GUI:</b> Restart SDS application. SDS only. If DSR, skip to step 51.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.   </li> <li>2. Select the recovered query server and click <b>Restart</b>.   </li> </ol>
51. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover the remaining SOAM servers (standby, spare)	<p><b>DSR:</b>  Execute the <b>Configure the SOAM Servers</b> procedure, steps 1-3 and 5-9, from reference [8].</p> <p><b>Note:</b> If you are using NetBackup, also execute step 12.</p> <p><b>SDS:</b>  Execute the <b>Configure the SDS DP SOAM Servers</b> procedure, steps 1-3 and 5-8, from reference [8].</p>

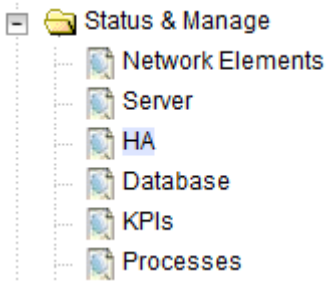
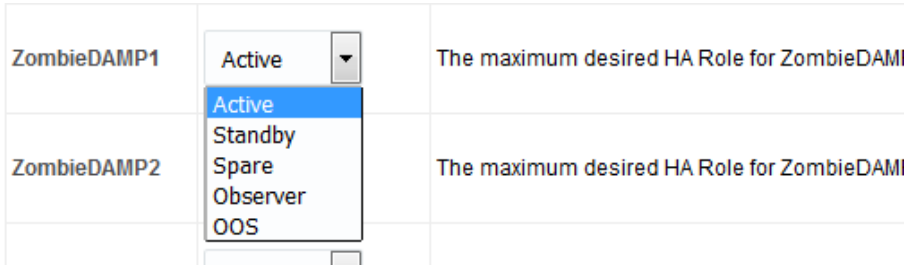
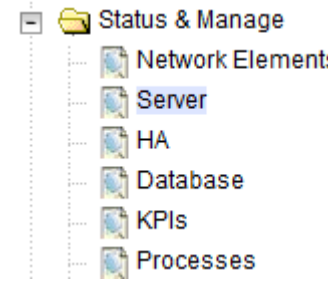

**Procedure 3. Recovery Scenario 3**

52. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set HA on SOAM server	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA.</b>   </li> <li>2. Click <b>Edit.</b></li> <li>3. Select the SOAM server and set it to <b>Active.</b>   </li> <li>4. Click <b>OK.</b></li> </ol>
53. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set HA on the SOAM server	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA.</b>   </li> <li>2. Click <b>Edit.</b></li> <li>3. Select the SOAM server and set it to <b>Active.</b>   </li> <li>4. Click <b>OK.</b></li> </ol>

**Procedure 3. Recovery Scenario 3**

54. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Restart DSR application	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.   </li> <li>2. Select the recovered SOAM server and click <b>Restart</b>.   </li> </ol>
55. <input type="checkbox"/>	Activate PCA feature. DSR only. If SDS, skip this step.	If you have PCA installed in the system being recovered, re-activate PCA by executing the <b>PCA Activation on Active NOAM Network</b> procedure on the recovered active NOAM server and the <b>PCA Activation on Stand By SOAM Network</b> procedure on the recovered standby SOAM from reference [7].
56. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover the C-level servers (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DPs	<p><b>DSR:</b></p> <p>Execute the <b>Configure the MP Servers</b> procedure, steps 1 and 9-13, from reference [8].</p> <p><b>Note:</b> Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.</p> <p><b>SDS:</b></p> <p>Execute the <b>Configure the SDS DP Servers</b> procedure, steps 1 and 5-8, from reference [8],</p> <p>Repeat this step for any remaining failed MP servers.</p>

**Procedure 3. Recovery Scenario 3**

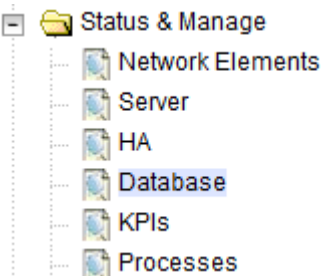

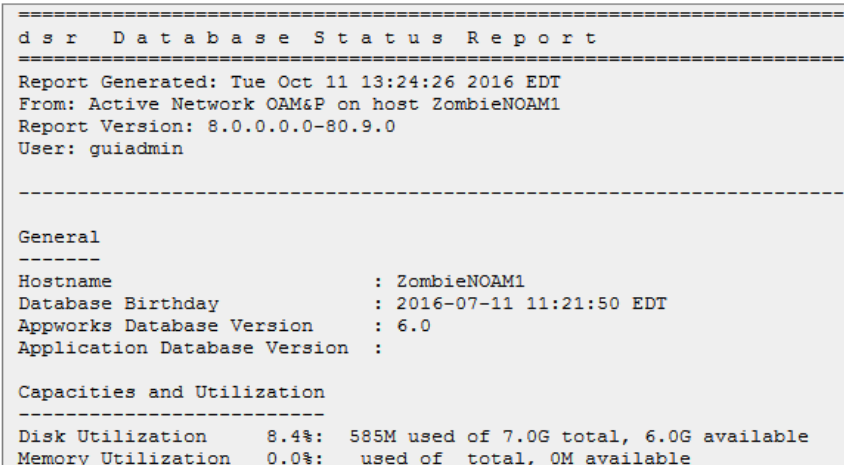
57. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set HA on all C-level servers	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>2. Click <b>Edit</b>.</li> <li>3. For each server whose Max Allowed HA Role is set to OOS, set it to <b>Active</b>.   </li> <li>4. Click <b>OK</b>.</li> </ol>
58. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Restart DSR application on recovered C-level servers	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.   </li> <li>2. Select the recovered C-level servers and click <b>Restart</b>.   </li> </ol>
59. <input type="checkbox"/>	<b>Active NOAM:</b> Perform keyexchange between the active-NOAM and recovered servers	<ol style="list-style-type: none"> <li>1. Establish an SSH session to the active NOAM, login as <b>admusr</b>.</li> <li>2. Perform a keyexchange from the active NOAM to each recovered server:  <pre>\$ keyexchange admusr@&lt;Recovered Server Hostname&gt;</pre> </li> </ol> <p><b>Note:</b> If an export server is configured, perform this step.</p>



**Procedure 3. Recovery Scenario 3**

60. <input type="checkbox"/>	<p><b>Active NOAM:</b> Activate optional features. DSR only. If SDS, then skip to next step.</p>	<p>Establish an SSH session to the active NOAM and login as <b>admusr</b>.</p> <p><b>Note for PCA Feature Activation:</b> If you have PCA installed in the system being recovered, re-activate the PCA by executing the <b>PCA Activation on Active NOAM Server</b> procedure on recovered active NOAM server and the <b>PCA Activation on Standby SOAM Server</b> procedure on the recovered standby SOAM server from [6].</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• If not all SOAM sites are recovered at this point, then repeat the activation for each “new” SOAM site that comes online.</li> <li>• If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature.</li> </ul> <p>Refer to section 1.5 Optional Features to activate any features that were previously activated.</p> <p><b>Note:</b> While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored:</p> <pre>iload#31000{S/W Fault}</pre>
---------------------------------	--	--

**Procedure 3. Recovery Scenario 3**

61. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Fetch and store the database report for the newly restored data and save it	<ol style="list-style-type: none"> <li>Navigate to <b>Status &amp; Manage &gt; Database</b>.   </li> <li>Select the active NOAM server and click <b>Report</b>.   <p>The following screen displays:  <b>Main Menu: Status &amp; Manage -&gt; Database [Report]</b></p>  </li> <li>Click <b>Save</b> and save the report to your local machine.</li> </ol>
------------------------------	---	--

**Procedure 3. Recovery Scenario 3**

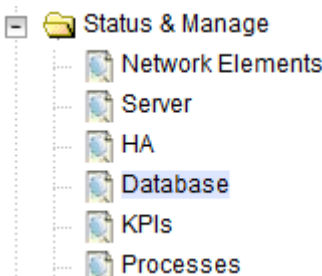
62. <input type="checkbox"/>	<b>Active NOAM:</b> Verify replication between servers	<ol style="list-style-type: none"> <li>1. Log into the active NOAM as <b>admusr</b> using SSH terminal.</li> <li>2. Execute this command:           <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>\$ sudo irepstat -m</pre> </div> <p><b>Example output:</b></p> <pre>-- Policy 0 ActStb [DbReplication] ----- Oahu-DAMP-1 -- Active   BC From Oahu-SOAM-2 Active 0 0.50 ^0.15%cpu 25B/s A=me   CC To Oahu-DAMP-2 Active 0 0.10 0.14%cpu 25B/s A=me Oahu-DAMP-2 -- Stby   BC From Oahu-SOAM-2 Active 0 0.50 ^0.11%cpu 31B/s A=C3642.212   CC From Oahu-DAMP-1 Active 0 0.10 ^0.14 1.16%cpu 31B/s A=C3642.212 Oahu-IPFE-1 -- Active   BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 24B/s A=C3642.212 Oahu-IPFE-2 -- Active   BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 28B/s A=C3642.212 Oahu-NOAM-1 -- Stby   AA From Oahu-NOAM-2 Active 0 0.25 ^0.03%cpu 23B/s Oahu-NOAM-2 -- Active   AA To Oahu-NOAM-1 Active 0 0.25 1%R 0.04%cpu 61B/s   AB To Oahu-SOAM-2 Active 0 0.50 1%R 0.05%cpu 75B/s Oahu-SOAM-1 -- Stby   BB From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 27B/s Oahu-SOAM-2 -- Active   AB From Oahu-NOAM-2 Active 0 0.50 ^0.03%cpu 24B/s   BB To Oahu-SOAM-1 Active 0 0.50 1%R 0.04%cpu 32B/s   BC To Oahu-IPFE-1 Active 0 0.50 1%R 0.04%cpu 21B/s   BC To Oahu-SS7MP-2 Active 0 0.50 1%R 0.04%cpu 21B/s irepstat ( 40 lines) (h)elp (m)erged</pre> </li> </ol>
---------------------------------	--	---

**Procedure 3. Recovery Scenario 3**

63.

NOAM VIP GUI:  
Verify the database states

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



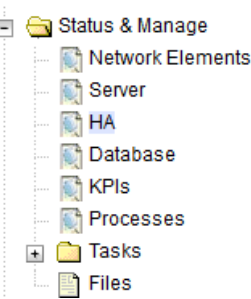
2. Verify the OAM Max HA Role is either **Active** or **Standby** for NOAM and SOAM; Application Max HA Role for MPs is **Active**; and status is **Normal**:

Network Element	Server	Role	OAM Max HA Role
ZombieDRNOAM	ZombieDRNOAM1	Network OAM&P	Active
ZombieNOAM	ZombieNOAM2	Network OAM&P	Standby
ZombieSOAM	ZombieSOAM2	System OAM	N/A
ZombieNOAM	ZombieNOAM1	Network OAM&P	Active
ZombieSOAM	ZombieSOAM1	System OAM	Active
ZombieDRNOAM	ZombieDRNOAM2	Network OAM&P	Standby
ZombieSOAM	ZombieDAMP2	MP	Standby
ZombieSOAM	ZombieSS7MP2	MP	Active
ZombieSOAM	ZombieSS7MP1	MP	Active
ZombieSOAM	ZombieIPFE1	MP	Active
ZombieSOAM	ZombieIPFE2	MP	Active

64.

NOAM VIP GUI:  
Verify the HA status

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

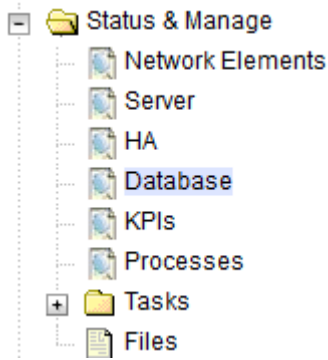
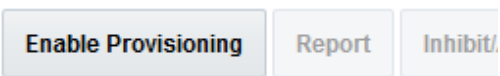
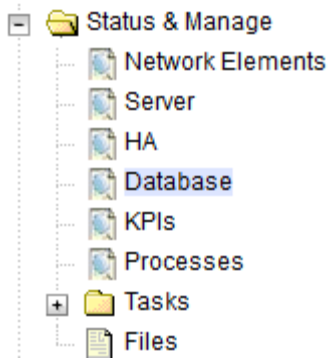

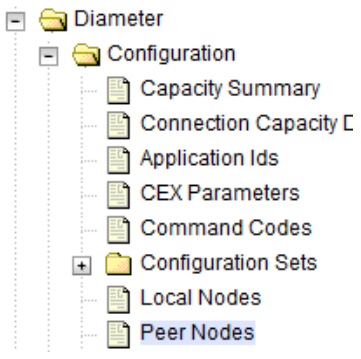


2. Select the row for all of the servers.

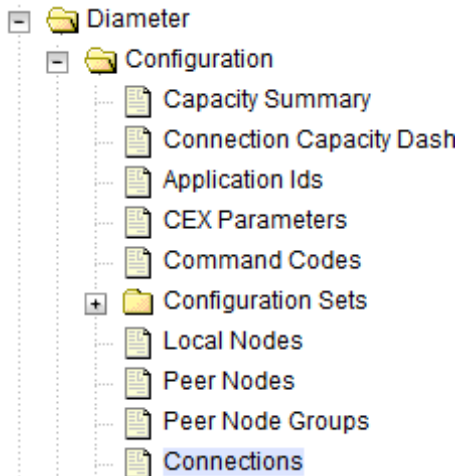
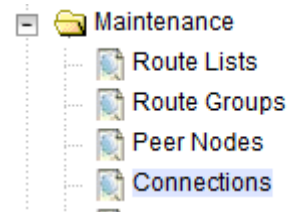
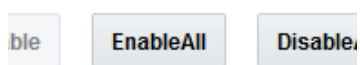
3. Verify the HA Role is either **Active** or **Standby**.

Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role
ZombieNOAM1	Active	N/A	Active
ZombieNOAM2	Standby	N/A	Active
ZombieDRNOAM1	Active	N/A	Active
ZombieDRNOAM2	Standby	N/A	Active
ZombieSOAM1	Active	N/A	Active
ZombieSOAM2	Standby	N/A	Standby

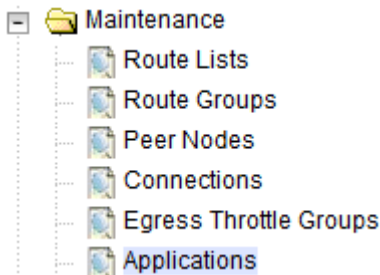
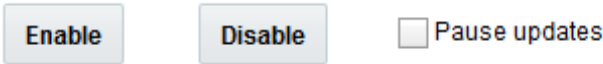
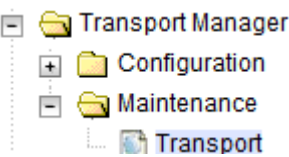

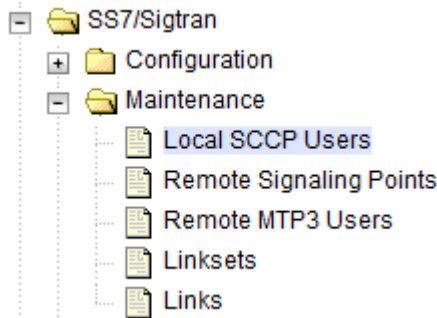

**Procedure 3. Recovery Scenario 3**

65. <input type="checkbox"/>	<b>NOAM GUI:</b> Enable provisioning	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Database</b>.   </li> <li>2. Click <b>Enable Provisioning</b>.   </li> <li>3. Click <b>OK</b>.</li> </ol>
66. <input type="checkbox"/>	<b>SOAM GUI:</b> Enable site provisioning. DSR only. If SDS, then skip to step 75.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Database</b>.   </li> <li>2. Click <b>Enable Site Provisioning</b>.   </li> <li>3. Click <b>OK</b>.</li> </ol>
67. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Verify the peer node information. DSR only. If SDS, then skip to step 75.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Diameter &gt; Configuration &gt; Peer Node</b>.   </li> <li>2. Verify all the peer nodes are shown.</li> </ol>

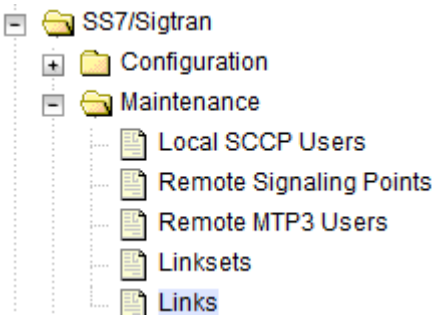

**Procedure 3. Recovery Scenario 3**

68. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Verify the connections information. DSR only. If SDS, then skip to step 75.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Diameter &gt; Configuration &gt; Connections</b>.   </li> <li>2. Verify all the connections are shown.</li> </ol>
69. <input type="checkbox"/>	<b>MP Servers:</b> Disable SCTP Auth Flag (DSR only). DSR only. If SDS, then skip to step 75.	For SCTP connections without DTLS enabled, refer to the <b>Enable/Disable DTLS (SCTP Diameter Connections Only)</b> section in reference [8]. Execute this procedure on all failed MP servers.
70. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Enable connections, if needed. DSR only. If SDS, then skip to step 75.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Diameter &gt; Maintenance &gt; Connections</b>.   </li> <li>2. Select each connection and click <b>Enable</b>. Alternatively, enable all the connections by clicking <b>EnableAll</b>.   </li> <li>3. Verify the Operational State is <b>Available</b>.  <b>Note:</b> If a disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution         </li> </ol>

**Procedure 3. Recovery Scenario 3**

71. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Enable optional features. DSR only. If SDS, then skip to step 75.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Diameter &gt; Maintenance &gt; Applications</b>.   </li> <li>2. Select the optional feature application configured in step 60.</li> <li>3. Click <b>Enable</b>.   </li> </ol>
72. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Re-enable transports, if needed. DSR only. If SDS, then skip to step 75.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Transport Manager &gt; Maintenance &gt; Transport</b>.   </li> <li>2. Select each transport and click <b>Enable</b>.   </li> <li>3. Verify the Operational Status for each transport is <b>Up</b>.</li> </ol>
73. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 75.	<ol style="list-style-type: none"> <li>1. Navigate to <b>SS7/Sigtran &gt; Maintenance &gt; Local SCCP Users</b>.   </li> <li>2. Click the <b>Enable</b> button corresponding to MAPIWF Application Name.   </li> <li>3. Verify the SSN Status is <b>Enabled</b>.</li> </ol>

## Procedure 3. Recovery Scenario 3

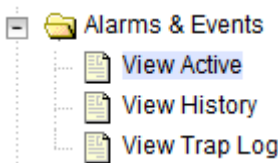
<p>74.</p> <p><input type="checkbox"/></p>	<p><b>SOAM VIP GUI:</b> Re-enable links, if needed. DSR only. If SDS, then skip to step 75.</p>	<ol style="list-style-type: none"> <li>1. Navigate to <b>SS7/Sigtran &gt; Maintenance &gt; Links</b>.   </li> <li>2. Click <b>Enable</b> for each link.   </li> <li>3. Verify the Operational Status for each link is <b>Up</b>.</li> </ol>
<p>75.</p> <p><input type="checkbox"/></p>	<p><b>NOAM VIP:</b> Verify all servers in topology are accessible (RADIUS only)</p>	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>1. Establish an SSH session to the NOAM VIP and login as <b>admusr</b>.</li> <li>2. Check if all the servers in the topology are accessible:</li> </ol> <pre data-bbox="521 982 980 1058" style="background-color: #f0f0f0; padding: 10px;">\$ /usr/TKLC/dpi/bin/ \$ ./sharedKrevo -checkAccess</pre> <p>Example output:</p> <pre data-bbox="516 1115 1435 1619" style="background-color: #2e3436; color: #eeeeec; padding: 10px;">1450112012: [INFO] 'SOAM-2' is accessible. FIPS integrity verification test failed. The authenticity of host 'ipfe (10.240.146.16)' can't be established. RSA key fingerprint is ea:7f:0d:eb:56:4d:de:b1:5b:04:a3:fe:72:4e:c3:52. Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added 'ipfe,10.240.146.16' (RSA) to the list of known hosts . 1450112015: [INFO] 'IPFE' is accessible. FIPS integrity verification test failed. The authenticity of host 'mp-2 (10.240.146.24)' can't be established. RSA key fingerprint is 73:ec:ac:d7:af:d2:78:dd:8e:bf:8e:79:a8:26:a7:b6. Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added 'mp-2,10.240.146.24' (RSA) to the list of known hosts . 1450112017: [INFO] 'MP-2' is accessible. FIPS integrity verification test failed. The authenticity of host 'mp-1 (10.240.146.14)' can't be established. RSA key fingerprint is c5:66:85:6c:1d:c8:9f:78:92:2c:ca:8b:83:9b:ef:99. Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added 'mp-1,10.240.146.14' (RSA) to the list of known hosts . 1450112020: [INFO] 'MP-1' is accessible.</pre> <p><b>Note:</b> If any server is not accessible, stop and contact My Oracle Support (MOS).</p>



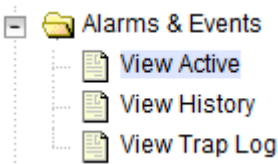
**Procedure 3. Recovery Scenario 3**

76. <input type="checkbox"/>	<b>SOAM VIP:</b> Copy key file to all the servers in topology (RADIUS only)	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>1. Establish an SSH session to any active SOAM that remained intact and operational (Log into an active SOAM server that was not recovered or did not need recovery).</li> <li>2. Login as <b>admusr</b>.</li> <li>3. Check if the existing key file on active SOAM server is valid: <div data-bbox="516 548 1412 632" data-label="Text"> <pre>\$ cd /usr/TKLC/dpi/bin/ \$ ./sharedKrevo -validate</pre> </div> <p><b>Note:</b> If output of above command shows that existing key file is not valid, contact My Oracle Support (MOS).</p> </li> <li>4. Establish an SSH session to the active NOAM, login as <b>admusr</b>.</li> <li>5. Copy the key file to active NOAM: <div data-bbox="516 821 1422 930" data-label="Text"> <pre>\$ cd /usr/TKLC/dpi/bin/ \$ ./sharedKrevo -copyKey -destServer &lt;Active NOAM server name&gt;</pre> </div> </li> </ol>
---------------------------------	---	---

**Procedure 3. Recovery Scenario 3**

<p>77.</p> <p><input type="checkbox"/></p>	<p><b>NOAM VIP:</b> Copy key file to all the servers in topology (RADIUS only)</p>	<ol style="list-style-type: none"> <li>1. Establish an SSH session to any of the active NOAM. Login as <b>admusr</b>.</li> <li>2. Copy the key file to all the servers in the topology: <div data-bbox="565 338 1425 426" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>\$ cd /usr/TKLC/dpi/bin/ \$ ./sharedKrevo -synchronize</pre> </div> <p>Example output:</p> <div data-bbox="565 470 1425 835" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>[admusr@NOAM-1 bin]\$ ./sharedKrevo -synchronize FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203505: [INFO] Key file on Active NOAM and NOAM-2 are same. 1450203505: [INFO] NO NEED to sync key file to NOAM-2. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203506: [INFO] Key file on Active NOAM and SOAM-1 are same. 1450203506: [INFO] NO NEED to sync key file to SOAM-1. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203506: [INFO] Key file on Active NOAM and SOAM-2 are same. 1450203506: [INFO] NO NEED to sync key file to SOAM-2. FIPS integrity verification test failed.</pre> </div> <div data-bbox="565 842 1425 888" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>\$ ./sharedKrevo -updateData</pre> </div> <p>Example output:</p> <div data-bbox="565 932 1425 1220" style="border: 1px solid black; padding: 5px;"> <pre>[admusr@NOAM-1 bin]\$ ./sharedKrevo -updateData 1450203518: [INFO] Updating data on server 'NOAM-1' 1450203519: [INFO] Data updated to 'NOAM-1' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203520: [INFO] Updating data on server 'SOAM-2' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203522: [INFO] 1 rows updated on 'SOAM-2'... 1450203522: [INFO] Data updated to 'SOAM-2'</pre> </div> </li> </ol>
<p>78.</p> <p><input type="checkbox"/></p>	<p><b>SOAM VIP GUI:</b> Examine all alarms</p>	<ol style="list-style-type: none"> <li>1. Navigate to <b>Alarms &amp; Events &gt; View Active</b>. <div data-bbox="542 1283 818 1444" style="border: 1px solid black; padding: 5px; margin: 10px 0;">  </div> </li> <li>2. Examine all active alarms and refer to the on-line help on how to address them.</li> </ol> <p>If needed, contact My Oracle Support (MOS).</p>

**Procedure 3. Recovery Scenario 3**

79. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Examine all alarms	<p>1. Navigate to <b>Alarms &amp; Events &gt; View Active</b>.</p>  <p>2. Examine all active alarms and refer to the on-line help on how to address them.</p> <p>If needed, contact My Oracle Support (MOS).</p>
80. <input type="checkbox"/>	Back up and archive all the databases from the recovered system	Execute the <b>DSR Database Backup</b> procedure to back up the configuration databases.
81. <input type="checkbox"/>	Recover IDIH, if configured	If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.
82. <input type="checkbox"/>	SNMP workaround	<p>Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases:</p> <ol style="list-style-type: none"> <li>1. If SNMP is not configured in DSR/SDS.</li> <li>2. If SNMP is already configured and SNMPv3 is selected as enabled version.</li> </ol>

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

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

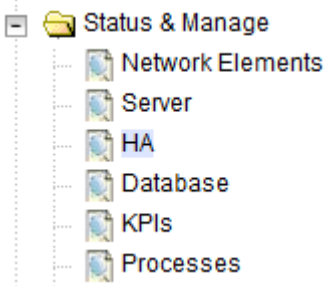

- Recover standby NOAM server by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
- Recover Query Server (if needed) by recovering base hardware and software.
  - Recover the base hardware.
  - Recover the software.
- Recover Standby SOAM server by recovering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

- Recover IDIH if necessary

**Procedure 4. Recovery Scenario 4**

S T E P #	<p>This procedure performs recovery if at least one NOAM server is intact and available and 1 SOAM server is intact and available.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>	
1. <input type="checkbox"/>	Workarounds	<p>Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.</p> <p>Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases:</p> <ol style="list-style-type: none"> <li>1. If SNMP is not configured in DSR.</li> <li>2. If SNMP is already configured and SNMPv3 is selected as enabled version.</li> </ol>
2. <input type="checkbox"/>	Gather required materials	Gather the documents and required materials listed in Required Materials.
3. <input type="checkbox"/>	Replace failed equipment	Work with the hardware vendor to replace the failed equipment.
4. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Login	<ol style="list-style-type: none"> <li>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  <div data-bbox="581 1050 1380 1092" style="border: 1px solid black; padding: 2px; margin: 5px 0;">http://&lt;Primary_NOAM_VIP_IP_Address&gt;</div> </li> <li>2. Login as the <b>guiadmin</b> user:</li> </ol> <div data-bbox="792 1165 1188 1222" style="text-align: center; color: red; font-weight: bold; font-size: 1.2em;">ORACLE®</div> <div data-bbox="539 1270 777 1302" style="text-align: center;">Oracle System Login</div> <div data-bbox="1172 1297 1429 1318" style="text-align: right;">Tue Jun 7 13:49:06 2016 EDT</div> <div data-bbox="701 1360 1263 1707" style="border: 1px solid #ccc; padding: 10px; margin: 10px auto; width: 80%;"> <p style="text-align: center;"><b>Log In</b></p> <p style="text-align: center;">Enter your username and password to log in</p> <p style="text-align: center;">Username: <input style="width: 100px;" type="text"/></p> <p style="text-align: center;">Password: <input style="width: 100px;" type="password"/></p> <p style="text-align: center;"><input type="checkbox"/> Change password</p> <p style="text-align: center;"><input type="button" value="Log In"/></p> </div> <p style="font-size: 0.8em; margin-top: 10px;">Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.</p> <hr style="border: 0; border-top: 1px solid #ccc; margin: 10px 0;"/> <p style="font-size: 0.7em; text-align: center;">Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</p> <p style="font-size: 0.7em; text-align: center;">Copyright © 2010, 2016, <a href="#">Oracle</a> and/or its affiliates. All rights reserved.</p>

**Procedure 4. Recovery Scenario 4**

<p>5. <input type="checkbox"/></p>	<p><b>Active NOAM:</b> Set failed servers to OOS</p>	<ol style="list-style-type: none"> <li>Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>Click <b>Edit</b>.</li> <li>Set the Max Allowed HA Role option to <b>OOS</b> for the failed servers.  <b>Modifying HA attributes</b>  <table border="1" data-bbox="535 766 1112 1134"> <thead> <tr> <th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td><td>Active</td><td>The maximum des</td></tr> <tr> <td>ZombieNOAM2</td><td>OOS</td><td>The maximum des</td></tr> <tr> <td>ZombieDRNOAM1</td><td>OOS</td><td>The maximum des</td></tr> </tbody> </table> </li> <li>Click <b>OK</b>.   </li> </ol>	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active	The maximum des	ZombieNOAM2	OOS	The maximum des	ZombieDRNOAM1	OOS	The maximum des
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active	The maximum des												
ZombieNOAM2	OOS	The maximum des												
ZombieDRNOAM1	OOS	The maximum des												
<p>6. <input type="checkbox"/></p>	<p><b>Recover PMAC and PMAC TVOE Host:</b> Configure BIOS settings and update firmware</p>	<ol style="list-style-type: none"> <li>Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]: <ul style="list-style-type: none"> <li><b>HP DL380 Gen8:</b> Configure HP Gen 8 Server BIOS Settings</li> <li><b>Oracle X5-2/Netra X5-2/X6-2/X7-2:</b> Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings</li> <li><b>HP DL380 Gen9:</b> Configure HP Gen9 Server BIOS Settings</li> </ul> </li> <li>Verify and/or upgrade server firmware by executing the <b>Upgrade Rack Mount Server Firmware</b> procedure from reference [8].</li> </ol>												

**Procedure 4. Recovery Scenario 4**

7. <input type="checkbox"/>	<b>Recover PMAC, TVOE Hosts, and Switch:</b> Backups available	<p>If the PMAC is located on the failed rack mount server, execute this step; otherwise skip to step 10.</p> <p>This step assumes TVOE and PMAC backups are available. If backups are <b>NOT</b> available, <b>skip this step</b>.</p> <ol style="list-style-type: none"> <li>1. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.</li> <li>2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup.</li> <li>3. Proceed to step 9.</li> </ol>
8. <input type="checkbox"/>	<b>Recover PMAC, TVOE Hosts, and Switch:</b> Backups NOT available	<p>If the PMAC is located on the failed rack mount server, execute this step; otherwise skip to step 10.</p> <p>This step assumes TVOE and PMAC backups are <b>NOT</b> available. If the TVOE and PMAC have already been restored, <b>skip this step</b>.</p> <p>Execute these procedures from reference [8]:</p> <ul style="list-style-type: none"> <li>• <b>Install and Configure TVOE on First RMS (PMAC Host)</b></li> <li>• <b>Install PMAC</b></li> <li>• <b>Initialize the PMAC Application</b></li> </ul>
9. <input type="checkbox"/>	Configure PMAC (no backup)	<p>If PMAC backup was <b>NOT</b> restored in step 7. , execute this step; otherwise, skip this step.</p> <p>Execute these procedures from reference [8]:</p> <ul style="list-style-type: none"> <li>• <b>Configure PMAC Server (NetBackup Only)</b></li> <li>• <b>Add RMS to the PMAC Inventory</b></li> </ul>
10. <input type="checkbox"/>	Install/Configure additional rack mount servers	<p><b>Note:</b> If TVOE backups are available, refer Appendix G Restore TVOE Configuration from Backup Media; otherwise, execute this step.</p> <p>If TVOE backups were <b>NOT</b> performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step.</p> <ol style="list-style-type: none"> <li>1. Execute these procedures from reference [8]: <ul style="list-style-type: none"> <li>• <b>Install TVOE on Additional Rack Mount Servers</b></li> <li>• <b>Configure TVOE on Additional Rack Mount Servers</b></li> </ul> </li> <li>2. Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]: <ul style="list-style-type: none"> <li>• <b>HP DL380 Gen8:</b> Configure HP Gen 8 Server BIOS Settings</li> <li>• <b>Oracle X5-2/Netra X5-2/X6-2/X7-2:</b> Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings</li> <li>• <b>HP DL380 Gen9:</b> Configure HP Gen9 Server BIOS Settings</li> </ul> </li> <li>3. Verify and/or upgrade server firmware by executing the <b>Upgrade Rack Mount Server Firmware</b> procedure from reference [8].</li> </ol>

**Procedure 4. Recovery Scenario 4**

11. <input type="checkbox"/>	Determine VM placement and socket pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 only)	HP DL380 GEN 8, <b>skip this step.</b> Determine VM placement and pinning by following section 3.1, item 14.
12. <input type="checkbox"/>	Deploy redundant PMAC, if required	Refer to the <b>Deploy Redundant PMAC (Optional)</b> procedure to re-deploy and configure any redundant PMACs previously configured.
13. <input type="checkbox"/>	<b>PMAC:</b> Determine if the fdconfig file exists from the initial deployment	<ol style="list-style-type: none"> <li>Type: <div data-bbox="591 590 1086 651" data-label="Text"> <pre>[admusr@melbourne-pmac-1 ~]\$ ll /usr/TKLC/smac/etc/fdc/</pre> </div> </li> <li>Examine the results and verify if the <b>rms config file &lt;hostname&gt;.cfg</b> exists.</li> </ol> <p><b>Note:</b> There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS.</p> <ol style="list-style-type: none"> <li>Skip to step 15.</li> </ol>
14. <input type="checkbox"/>	Create fdconfig backup file, if it does not already exist	<p>Execute this step <b>ONLY</b> If the fdconfig backup file does <b>NOT</b> exist.</p> <p>Create the needed file(s) by executing the <b>Virtual Machine/Network Fast Deployment</b> section from reference [8].</p> <p style="text-align: center;"><b>WARNING</b></p> <p>It is very important to ensure the file(s) created only affects the TVOE server(s) and the guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.</p>
15. <input type="checkbox"/>	<b>PMAC:</b> Load ISOs into PMAC, if not done already	If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the <b>Virtual Machine/Network Fast Deployment</b> section from reference [8].
16. <input type="checkbox"/>	<b>PMAC:</b> Edit/Update configuration file	<p>Edit the fdconfig file to include only the required/failed servers.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Comment out configuration items that are not needed.</li> <li>Create a separate configuration file for EACH rack mount server being deployed.</li> <li>The Cabinet ID in the config file needs to match the cabinet already defined in PMAC.</li> </ul> <p>The following items are mandatory:</p> <ul style="list-style-type: none"> <li>siteName</li> <li>tpdIso</li> <li>dsrIso (if DSR VMs are being configured)</li> <li>sdsIso (if SDS VMs are being configured)</li> <li>NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured)</li> </ul>

**Procedure 4. Recovery Scenario 4**

		<ul style="list-style-type: none"> <li>• XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured)</li> <li>• XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured)</li> <li>• DSRNOAM1XMIIPADDRESS (if DSRNOAM1 is being configured)</li> <li>• DSRNOAM2XMIIPADDRESS (if DSRNOAM2 is being configured)</li> <li>• DSRDRNOAM1XMIIPADDRESS (if DSRDRNOAM1 is being configured)</li> <li>• DSRDRNOAM2XMIIPADDRESS (if DSRDRNOAM2 is being configured)</li> <li>• SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured)</li> <li>• SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured)</li> <li>• SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured)</li> <li>• SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured)</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].</li> <li>• Comment out SDS and DSR profile items if corresponding products are not used.</li> <li>• For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9, refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].</li> <li>• VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName.</li> <li>• VM locations should not be changed from their <b>RMSx</b> format. Each RMS should correspond to a separate rack mount server.</li> </ul> <p style="text-align: center;"><b>WARNING</b></p> <p>Ensure the file(s) created only affect the TVOE server(s) and guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.</p>
17.	<input type="checkbox"/> <b>PMAC:</b> Copy the backed up fdconfig file to the RMS directory	<p>Copy the fdconfig backup file to the RMS directory.</p> <pre>\$ sudo cp /usr/TKLC/smac/etc/fdc/&lt;backup_fdc_file&gt; /usr/TKLC/smac/etc/RMS/</pre>



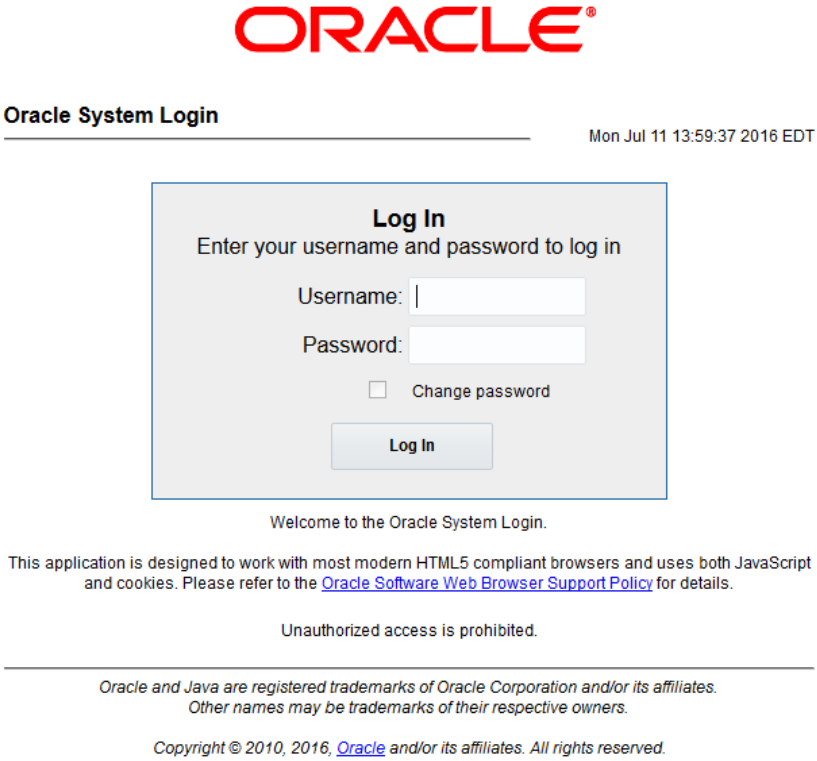
**Procedure 4. Recovery Scenario 4**

18. <input type="checkbox"/>	<b>PMAC:</b> Execute the config.sh script	<p>Execute <b>config.sh</b> against the modified backup config file.</p> <p><b>Note:</b> If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>\$ sudo ./config.sh &lt;config file&gt;</pre> </div> <p>Example output:</p> <pre>[admusr@5010441PMAC RMS]\$ sudo ./config.sh rms.cfg Validating cfg file... Successful validation of cfg file. Added Cabinet 101 to Fast Deployment File. Added Zombie_TVOE1 to Fast Deployment File. Added Zombie_TVOE2 to Fast Deployment File. Added xmi(bond0.4) to Fast Deployment File. Added imi(bond0.3) to Fast Deployment File. Added rep(bond1.10) to Fast Deployment File. Added xsi1(bond1.6) to Fast Deployment File. Added xsi2(bond1.7) to Fast Deployment File. Added xsi3(bond1.8) to Fast Deployment File. Added xsi4(bond1.9) to Fast Deployment File. Added xsi5(bond1.11) to Fast Deployment File. Added xsi6(bond1.12) to Fast Deployment File. Added xsi7(bond1.13) to Fast Deployment File. Added xsi8(bond1.14) to Fast Deployment File. Added xsi9(bond1.15) to Fast Deployment File. Added xsi10(bond1.16) to Fast Deployment File. Added xsi11(bond1.17) to Fast Deployment File. Added xsi12(bond1.18) to Fast Deployment File. Added xsi13(bond1.19) to Fast Deployment File. Added xsi14(bond1.20) to Fast Deployment File. Added xsi15(bond1.21) to Fast Deployment File. Added xsi16(bond1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRDRNOAM1 to Fast Deployment File. Added Zombie_DSRDRNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSDRNOAM1 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_DSRSOAM1 to Fast Deployment File. Added Zombie_DSRSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM1 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDAMP2 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_DSRIPFE2 to Fast Deployment File. Added Zombie_SSDPSV1 to Fast Deployment File. Added Zombie_SSDPSV2 to Fast Deployment File. Validating Fast Deployment File..... Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!! [admusr@5010441PMAC RMS]\$</pre>
---------------------------------	---	--

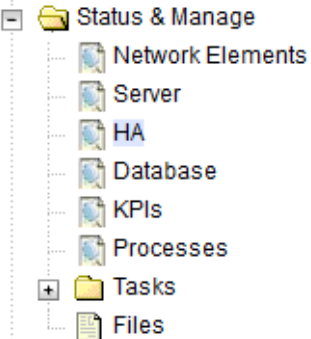
**Procedure 4. Recovery Scenario 4**

19. <input type="checkbox"/>	<b>PMAC:</b> Execute fast deployment	<p>With the file generated from the config.sh script, execute the following command to start fast deployment:</p> <pre>\$ screen \$ sudo fdconfig config --file=&lt;fd_config.xml&gt;</pre> <p><b>Note:</b> This is a long duration command. If the screen command was run before executing the fdconfig, perform a <b>screen -dr</b> to resume the screen session in the event of a terminal timeout, etc.</p>																																																															
20. <input type="checkbox"/>	<b>PMAC GUI:</b> Monitor the configuration	<p>1. If not already done, establish a GUI session on the PMAC server.</p> <p>2. Navigate to <b>Task Monitoring</b>.</p> <div></div> <p>3. Monitor the configuration to completion:</p> <div><p>Main Menu: Task Monitoring</p><p>Filter*</p><table><thead><tr><th>ID</th><th>Task</th><th>Target</th><th>Status</th><th>State</th><th>Task Output</th><th>Running Time</th><th>Start Time</th><th>Progress</th></tr></thead><tbody><tr><td>925</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_SDSRNOAM1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:04</td><td>2016-07-11 11:27:35</td><td>100%</td></tr><tr><td>924</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_SDSNOAM1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:04</td><td>2016-07-11 11:27:34</td><td>100%</td></tr><tr><td>923</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_DSRPF1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:06</td><td>2016-07-11 11:26:43</td><td>100%</td></tr><tr><td>922</td><td>Accept</td><td>RMS: pc5010439 Guest: Zombie_DSRDAMP2</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:05</td><td>2016-07-11 11:26:43</td><td>100%</td></tr><tr><td>921</td><td>Accept</td><td>RMS: pc5010441 Guest: Zombie_DSRDAMP1</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:05</td><td>2016-07-11 11:26:43</td><td>100%</td></tr><tr><td>920</td><td>Accept</td><td>RMS: pc5010439 Guest: Zombie_DSRDAMP2</td><td>Success</td><td>COMPLETE</td><td>N/A</td><td>0:01:06</td><td>2016-07-11 11:26:42</td><td>100%</td></tr></tbody></table></div> <p><b>Note:</b> If a failure occurs with fdconfig, logs can be accessed in <b>/var/TKLC/log/fdconfig/fdconfig.log</b> file.</p> <pre>[admusr@melbourne-pmac-1 fdconfig]\$ sudo fdconfig dumpsteps -- file=deploy_melbourne_20170329T202458_701b.fdcdb Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb" Here are the steps that were generated ----- begin ----- Dump of DB steps: NUM PHS DLY INFRA ID SVRTYPE CMD ELEMENT PRE STATE TO BGTS COMMAND TEXT ----- 1 1 0 pmac Fast_Deployment 0 21 0 Complete 300 0 Check PM&amp;C is available 2 1 0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet 3 1 0 pmac Fast_Deployment 0 3 melbourne_RMS3 1 Skipped 900 0 Add Rms 4 2 0 pmac Fast_Deployment 1</pre> <p>4. Restart the fdconfig after a failure has occurred and has been resolved:</p> <pre>\$ sudo fdconfig restart -- file=deploy_melbourne_20170329T202458_701b.fdcdb</pre>	ID	Task	Target	Status	State	Task Output	Running Time	Start Time	Progress	925	Accept	RMS: pc5010441 Guest: Zombie_SDSRNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:35	100%	924	Accept	RMS: pc5010441 Guest: Zombie_SDSNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:34	100%	923	Accept	RMS: pc5010441 Guest: Zombie_DSRPF1	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:43	100%	922	Accept	RMS: pc5010439 Guest: Zombie_DSRDAMP2	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%	921	Accept	RMS: pc5010441 Guest: Zombie_DSRDAMP1	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%	920	Accept	RMS: pc5010439 Guest: Zombie_DSRDAMP2	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:42	100%
ID	Task	Target	Status	State	Task Output	Running Time	Start Time	Progress																																																									
925	Accept	RMS: pc5010441 Guest: Zombie_SDSRNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:35	100%																																																									
924	Accept	RMS: pc5010441 Guest: Zombie_SDSNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:34	100%																																																									
923	Accept	RMS: pc5010441 Guest: Zombie_DSRPF1	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:43	100%																																																									
922	Accept	RMS: pc5010439 Guest: Zombie_DSRDAMP2	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%																																																									
921	Accept	RMS: pc5010441 Guest: Zombie_DSRDAMP1	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%																																																									
920	Accept	RMS: pc5010439 Guest: Zombie_DSRDAMP2	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:42	100%																																																									

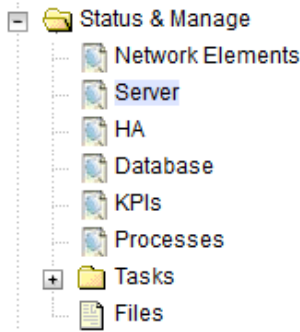

**Procedure 4. Recovery Scenario 4**

21. <input type="checkbox"/>	<b>PMAC:</b> Repeat for each rack mount server configuration file	Repeat steps 13. -20. for each rack mount server/configuration file, if required.
22. <input type="checkbox"/>	<b>PMAC:</b> Back up FDC file	1. Copy the updated fdc file to the fdc backup directory: <pre>\$ sudo cp /usr/TKLC/smac/etc/RMS/&lt;fdc_file&gt; /usr/TKLC/smac/etc/fdc/</pre> 2. Change permissions: <pre>\$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/&lt;fdc_file&gt;</pre>
23. <input type="checkbox"/>	Perform CPU pinning	Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the <b>CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only)</b> procedure from reference [8].
24. <input type="checkbox"/>	<b>NOAM GUI:</b> Login If the failed server is not OAM, then skip to step 47.	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: <pre>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</pre> 2. Login as the <b>guiadmin</b> user: <div data-bbox="560 934 1372 1690">  </div>

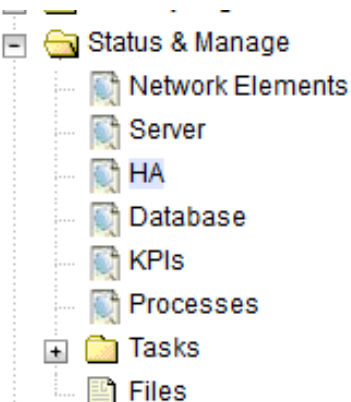
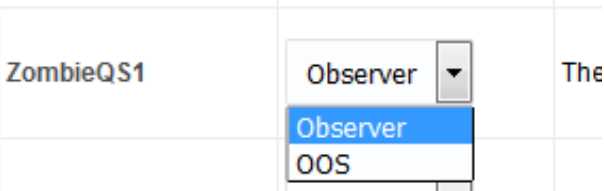
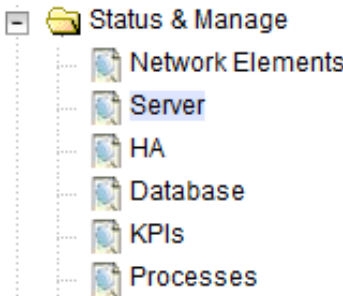

**Procedure 4. Recovery Scenario 4**

25. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover standby NOAM, if needed	Install the second NOAM server: <b>DSR:</b> Execute the <b>Configure the Second NOAM Server</b> procedure, steps 1 and 3-6, from reference [8]. <b>SDS:</b> Execute the <b>Configure the Second SDS NOAM Server</b> procedure, steps 1 and 3-6, from reference [8].												
26. <input type="checkbox"/>	Install NetBackup client (optional)	If NetBackup is used, execute the <b>Install NetBackup Client (Optional)</b> procedure from reference [8].												
27. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set HA on standby NOAM	<ol style="list-style-type: none"> <li>Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>Click <b>Edit</b>.</li> <li>Select the standby NOAM server and set it to <b>Active</b>.  <b>Modifying HA attributes</b>  <table border="1" data-bbox="545 1167 1084 1478"> <thead> <tr> <th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td><td>Active ▼</td><td>The maximum</td></tr> <tr> <td>ZombieNOAM2</td><td>Active ▼</td><td>The maximum</td></tr> <tr> <td>ZombieDRNOAM1</td><td>Active ▼</td><td>The maximum</td></tr> </tbody> </table> </li> <li>Click <b>OK</b>.</li> </ol>	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active ▼	The maximum	ZombieNOAM2	Active ▼	The maximum	ZombieDRNOAM1	Active ▼	The maximum
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active ▼	The maximum												
ZombieNOAM2	Active ▼	The maximum												
ZombieDRNOAM1	Active ▼	The maximum												

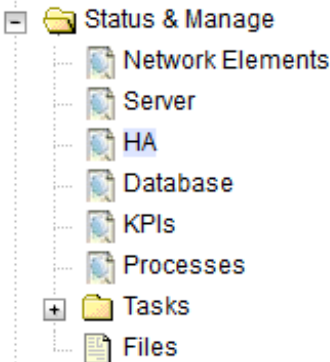
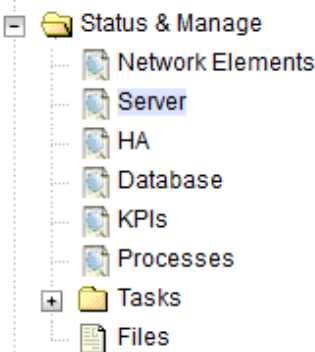

**Procedure 4. Recovery Scenario 4**

28. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Restart DSR application	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.   </li> <li>2. Select the recovered standby NOAM server and click <b>Restart</b>.   </li> </ol>
29. <input type="checkbox"/>	<b>Active NOAM:</b> Correct the recognized authority table	<ol style="list-style-type: none"> <li>1. Establish an SSH session to the active NOAM and login as <b>admusr</b>.</li> <li>2. Execute this command:  <pre data-bbox="591 863 1435 1052"> \$ sudo top.setPrimary - Using my cluster: A1789 - New Primary Timestamp: 11/09/15 20:21:43.418 - Updating A1789.022: &lt;DSR_NOAM_B_hostname&gt; - Updating A1789.144: &lt;DSR_NOAM_A_hostname&gt; </pre> </li> </ol>
30. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover query servers. SDS only. If DSR, skip to step 33.	Execute the <b>Configuring SDS Query Servers</b> procedure, steps 1 and 4-7, from reference [8].

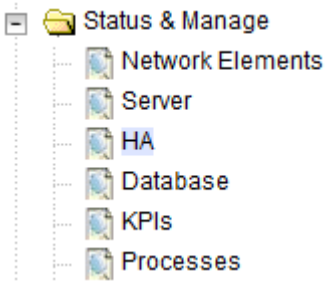
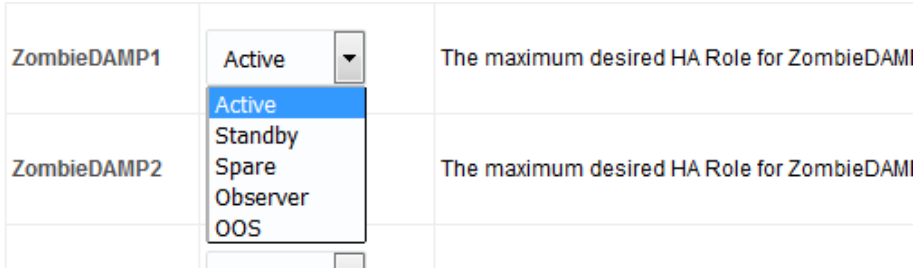
**Procedure 4. Recovery Scenario 4**

31. <input type="checkbox"/>	<b>SDS NOAM VIP GUI:</b> Set HA on query server. SDS only. If DSR, skip to step 33.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>2. Click <b>Edit</b>.</li> <li>3. Select the query server and select <b>Observer</b>.   </li> <li>4. Click <b>OK</b>.</li> </ol>
32. <input type="checkbox"/>	<b>SDS NOAM VIP GUI:</b> Restart SDS application. SDS only. If DSR, skip to step 33.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.   </li> <li>2. Select the recovered query server and click <b>Restart</b>.   </li> </ol>
33. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover the SOAM servers ( <b>Standby, Spare</b> — Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only)	<p><b>DSR:</b>          Execute the <b>Configure the SOAM Servers</b> procedure, steps 1-3 and 5-9, from reference [8].</p> <p><b>Note:</b> If you are using NetBackup, also execute step 12.</p> <p><b>SDS:</b>          Execute the <b>Configure the SDS DP SOAM Servers</b> procedure, steps 1-3 and 5-8, from reference [8].</p>

**Procedure 4. Recovery Scenario 4**

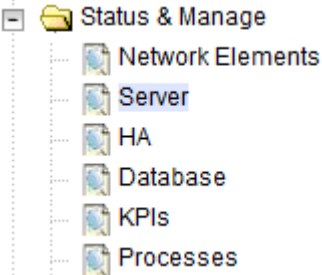

34. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set HA on standby NOAM	<ol style="list-style-type: none"> <li>Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>Click <b>Edit</b>.</li> <li>Select the standby NOAM server and set it to <b>Active</b>.  <b>Modifying HA attributes</b>  <table border="1" data-bbox="542 827 1052 1121"> <thead> <tr> <th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td><td>Active</td><td>The maximum</td></tr> <tr> <td>ZombieNOAM2</td><td>Active</td><td>The maximum</td></tr> <tr> <td>ZombieDRNOAM1</td><td>Active Standby Spare</td><td>The maximum</td></tr> </tbody> </table> </li> <li>Click <b>OK</b>.</li> </ol>	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active	The maximum	ZombieNOAM2	Active	The maximum	ZombieDRNOAM1	Active Standby Spare	The maximum
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active	The maximum												
ZombieNOAM2	Active	The maximum												
ZombieDRNOAM1	Active Standby Spare	The maximum												
35. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Restart DSR application	<ol style="list-style-type: none"> <li>Navigate to <b>Status &amp; Manage &gt; Server</b>.   </li> <li>Select the recovered standby NOAM server and click <b>Restart</b>.   </li> </ol>												
36. <input type="checkbox"/>	Activate PCA feature. DSR only. If SDS, skip this step.	If you have PCA installed in the system being recovered, re-activate PCA by executing the <b>PCA Activation on Active NOAM Network</b> procedure on the recovered standby NOAM server and the <b>PCA Activation on Stand By SOAM Network</b> procedure on the recovered standby SOAM from reference [7].												

**Procedure 4. Recovery Scenario 4**

37. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover the C-level servers (DA-MPs, SBRs, IPFE, SS7-MP, and SDS DP)	<b>DSR:</b> Execute the <b>Configure the MP Servers</b> procedure, steps 1 and 9-13, from reference [8].  <b>Note:</b> Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.  <b>SDS — Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only:</b> Execute the <b>Configure the SDS DP Servers</b> procedure, steps 1 and 5-8, from reference [8], Repeat this step for any remaining failed MP servers.
38. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set HA on all C-level servers	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>2. Click <b>Edit</b>.</li> <li>3. For each server whose Max Allowed HA Role is set to OOS, set it to <b>Active</b>.   </li> <li>4. Click <b>OK</b>.</li> </ol>



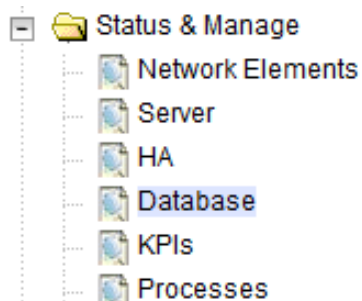
**Procedure 4. Recovery Scenario 4**

39. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Restart DSR application on recovered C-level servers	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.   </li> <li>2. Select the recovered C-level servers and click <b>Restart</b>.   </li> </ol>
40. <input type="checkbox"/>	<b>Active NOAM:</b> Perform keyexchange between the active-NOAM and recovered servers	<ol style="list-style-type: none"> <li>1. Establish an SSH session to the active NOAM, login as <b>admusr</b>.</li> <li>2. Perform a keyexchange from the active NOAM to each recovered server:  <pre>\$ keyexchange admusr@&lt;Recovered Server Hostname&gt;</pre> </li> </ol> <p><b>Note:</b> If an export server is configured, perform this step.</p>
41. <input type="checkbox"/>	<b>Active NOAM:</b> Activate optional features. DSR only. If SDS, then skip step 43.	<p>Establish an SSH session to the active NOAM and login as <b>admusr</b>.</p> <p><b>Note for PCA Feature Activation:</b></p> <p>If you have PCA installed in the system being recovered, re-activate the PCA by executing the <b>PCA Activation on Active NOAM Server</b> procedure on recovered active NOAM server and the <b>PCA Activation on Standby SOAM Server</b> procedure on the recovered standby SOAM server from [6].</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• If not all SOAM sites are recovered at this point, then repeat the activation for each “new” SOAM site that comes online.</li> <li>• If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature.</li> </ul> <p>Refer to section 1.5 Optional Features to activate any features that were previously activated.</p> <p><b>Note:</b> While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored:</p> <pre>iload#31000{S/W Fault}</pre>
42. <input type="checkbox"/>	<b>MP Servers:</b> Disable SCTP Auth Flag (DSR only). DSR only. If SDS, then skip step 43.	<p>For SCTP connections without DTLS enabled, refer to the <b>Enable/Disable DTLS (SCTP Diameter Connections Only)</b> section in reference [8].</p> <p>Execute this procedure on all failed MP servers.</p>

**Procedure 4. Recovery Scenario 4**

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

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



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



The following screen displays:

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

```
=====
d s r   D a t a b a s e   S t a t u s   R e p o r t
=====
Report Generated: Tue Oct 11 13:24:26 2016 EDT
From: Active Network OAM&P on host ZombieNOAM1
Report Version: 8.0.0.0.0-80.9.0
User: guiadmin

-----

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

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

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

**Procedure 4. Recovery Scenario 4**

44. <input type="checkbox"/>	<b>Active NOAM:</b> Verify replication between servers	<ol style="list-style-type: none"> <li>1. Log into the active NOAM as <b>admusr</b> using SSH terminal.</li> <li>2. Execute this command: <div data-bbox="578 338 1438 386" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> \$ sudo irepstat -m </div> </li> </ol> <p>Example output:</p> <pre> -- Policy 0 ActStb [DbReplication] ----- Oahu-DAMP-1 -- Active   BC From Oahu-SOAM-2  Active   0    0.50 ^0.15%cpu 25B/s  A=me   CC To   Oahu-DAMP-2  Active   0    0.10  0.14%cpu 25B/s  A=me Oahu-DAMP-2 -- Stby   BC From Oahu-SOAM-2  Active   0    0.50 ^0.11%cpu 31B/s  A=C3642.212   CC From Oahu-DAMP-1  Active   0    0.10 ^0.14 1.16%cpu 31B/s A=C3642.212 Oahu-IPFE-1 -- Active   BC From Oahu-SOAM-2  Active   0    0.50 ^0.03%cpu 24B/s  A=C3642.212 Oahu-IPFE-2 -- Active   BC From Oahu-SOAM-2  Active   0    0.50 ^0.03%cpu 28B/s  A=C3642.212 Oahu-NOAM-1 -- Stby   AA From Oahu-NOAM-2  Active   0    0.25 ^0.03%cpu 23B/s Oahu-NOAM-2 -- Active   AA To   Oahu-NOAM-1  Active   0    0.25 1%R 0.04%cpu 61B/s   AB To   Oahu-SOAM-2  Active   0    0.50 1%R 0.05%cpu 75B/s Oahu-SOAM-1 -- Stby   BB From Oahu-SOAM-2  Active   0    0.50 ^0.03%cpu 27B/s Oahu-SOAM-2 -- Active   AB From Oahu-NOAM-2  Active   0    0.50 ^0.03%cpu 24B/s   BB To   Oahu-SOAM-1  Active   0    0.50 1%R 0.04%cpu 32B/s   BC To   Oahu-IPFE-1  Active   0    0.50 1%R 0.04%cpu 21B/s   BC To   Oahu-SS7MP-2 Active   0    0.50 1%R 0.04%cpu 21B/s irepstat ( 40 lines) (h)elp (m)erged </pre>
---------------------------------	--	---

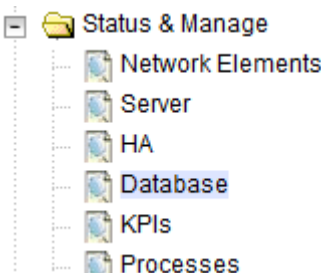
**Procedure 4. Recovery Scenario 4**

45.

☐

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

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



2. Verify the OAM Max HA Role as shown.

Role	Server Type	Expected HA Role(s)
Network OAM&P	NO	Active/Standby
SYSTEM OAM	SOAM	Active/Standby/Spare
MP	DA MP(s) IPFE(s) SS7MP(s)	Active
MP	SBR(s)	Active/Standby/Spare

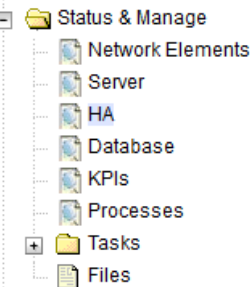
3. Verify the Status and OAM Repl Status is **Normal** and **Repl Status=Allowed.**

46.

☐

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

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

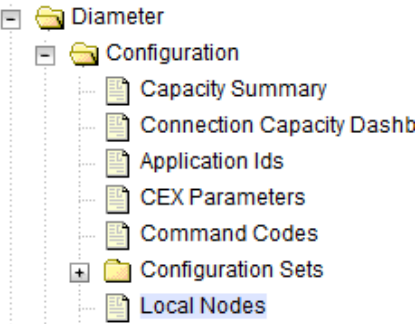
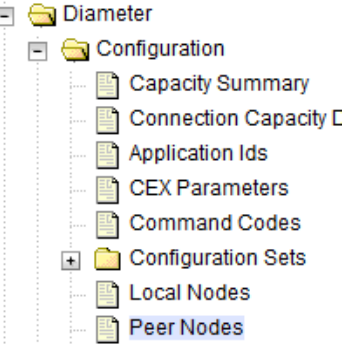
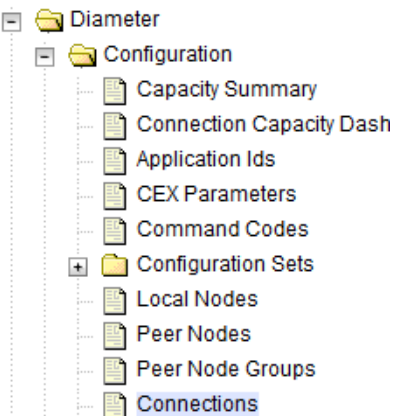


2. Select the row for all of the servers.

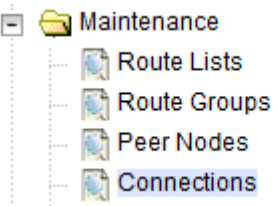
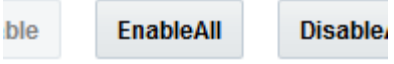
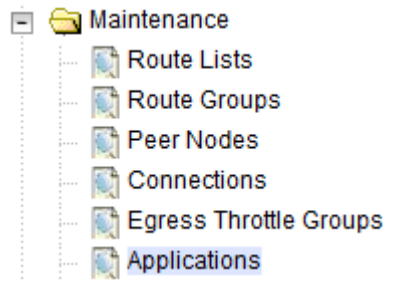
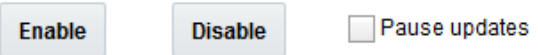
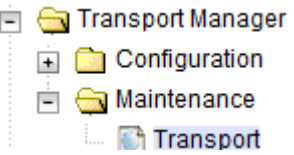
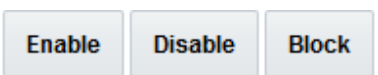
3. Verify the HA Role is either **Active** or **Standby**.

Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role
ZombieNOAM1	Active	N/A	Active
ZombieNOAM2	Standby	N/A	Active
ZombieDRNOAM1	Active	N/A	Active
ZombieDRNOAM2	Standby	N/A	Active
ZombieSOAM1	Active	N/A	Active
ZombieSOAM2	Standby	N/A	Standby

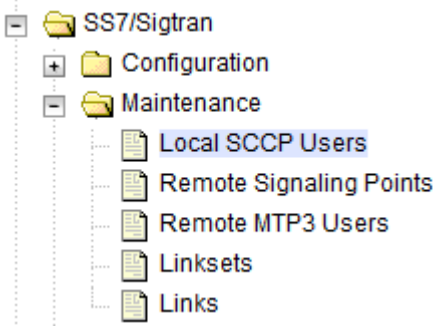
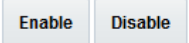
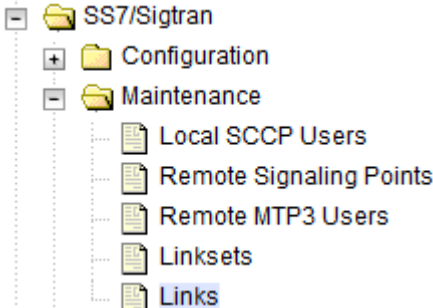

**Procedure 4. Recovery Scenario 4**

47. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Verify the local node information. DSR only. If SDS, then skip to step 56.	1. Navigate to <b>Diameter &gt; Configuration &gt; Local Node</b> .  2. Verify all the local nodes are shown.
48. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Verify the peer node information. DSR only. If SDS, then skip to step 56.	1. Navigate to <b>Diameter &gt; Configuration &gt; Peer Node</b> .  2. Verify all the peer nodes are shown.
49. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Verify the connections information. DSR only. If SDS, then skip to step 56.	3. Navigate to <b>Diameter &gt; Configuration &gt; Connections</b> .  4. Verify all the connections are shown.

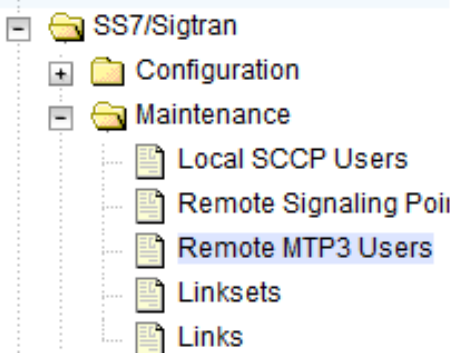

**Procedure 4. Recovery Scenario 4**

50. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Enable connections, if needed. DSR only. If SDS, then skip to step 56.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Diameter &gt; Maintenance &gt; Connections</b>.   </li> <li>2. Select each connection and click <b>Enable</b>. Alternatively, enable all the connections by clicking <b>EnableAll</b>.   </li> <li>3. Verify the Operational State is <b>Available</b>.  <b>Note:</b> If a disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution </li> </ol>
51. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Enable optional features. DSR only. If SDS, then skip to step 56.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Diameter &gt; Maintenance &gt; Applications</b>.   </li> <li>2. Select the optional feature application configured in step 72.</li> <li>3. Click <b>Enable</b>.   </li> </ol>
52. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Re-enable transports, if needed. DSR only. If SDS, then skip to step 56.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Transport Manager &gt; Maintenance &gt; Transport</b>.   </li> <li>2. Select each transport and click <b>Enable</b>.   </li> <li>3. Verify the Operational Status for each transport is <b>Up</b>.</li> </ol>

**Procedure 4. Recovery Scenario 4**

53. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 56.	<ol style="list-style-type: none"> <li>1. Navigate to <b>SS7/Sigtran &gt; Maintenance &gt; Local SCCP Users</b>.   </li> <li>2. Click the <b>Enable</b> button corresponding to MAPIWF Application Name.   </li> <li>3. Verify the SSN Status is <b>Enabled</b>.</li> </ol>
54. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Re-enable links, if needed. DSR only. If SDS, then skip to step 56.	<ol style="list-style-type: none"> <li>1. Navigate to <b>SS7/Sigtran &gt; Maintenance &gt; Links</b>.   </li> <li>2. Click <b>Enable</b> for each link.   </li> <li>3. Verify the Operational Status for each link is <b>Up</b>.</li> </ol>

**Procedure 4. Recovery Scenario 4**

55. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Reset remote MTP3 users, if needed. DSR only. If SDS, then skip to step 56.	<ol style="list-style-type: none"> <li>1. Navigate to <b>SS7/Sigtran &gt; Maintenance &gt; Remote MTP3 Users</b>.   </li> <li>2. Click Reset for each record, if needed.   </li> </ol>
56. <input type="checkbox"/>	<b>NOAM VIP:</b> Verify all servers in topology are accessible (RADIUS only)	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>1. Establish an SSH session to the NOAM VIP and login as <b>admusr</b>.</li> <li>2. Check if all the servers in the topology are accessible:</li> </ol> <pre>\$ /usr/TKLC/dpi/bin/ \$ ./sharedKrevo -checkAccess</pre> <p>Example output:</p> <pre>[admusr@NOAM-2 bin]\$ ./sharedKrevo -checkAccess FIPS integrity verification test failed. 1450723403: [INFO] 'NOAM-1' is accessible. FIPS integrity verification test failed. 1450723403: [INFO] 'SOAM-1' is accessible. FIPS integrity verification test failed. 1450723403: [INFO] 'SOAM-2' is accessible. FIPS integrity verification test failed. 1450723404: [INFO] 'IPFE' is accessible. FIPS integrity verification test failed. 1450723404: [INFO] 'MP-2' is accessible. FIPS integrity verification test failed. 1450723404: [INFO] 'MP-1' is accessible. [admusr@NOAM-2 bin]\$</pre> <p><b>Note:</b> If any server is not accessible, stop and contact My Oracle Support (MOS).</p>
57. <input type="checkbox"/>	<b>NOAM VIP:</b> Copy key file to all the servers in topology (RADIUS only)	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>1. Check if existing key file on active NOAM (the NOAM, which is intact and was not recovered) server is valid:</li> </ol>



**Procedure 4. Recovery Scenario 4**

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

Example output:

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

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

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

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

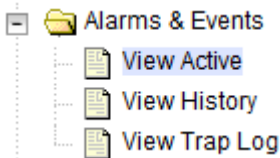
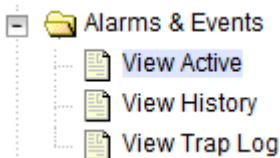
Example output:

```
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722733: [INFO] Synched key to IPFE
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722734: NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722735: [INFO] Synched key to MP-2
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722736: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450722738: [INFO] Synched key to MP-1
[admusr@NOAM-2 bin]$
```

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

Example output:

## Procedure 4. Recovery Scenario 4

		<pre>[admusr@NOAM-1 bin]\$ ./sharedKrevo -updateData 1450203518: [INFO] Updating data on server 'NOAM-1' 1450203519: [INFO] Data updated to 'NOAM-1' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203520: [INFO] Updating data on server 'SOAM-2' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203522: [INFO] 1 rows updated on 'SOAM-2'... 1450203522: [INFO] Data updated to 'SOAM-2'</pre> <p><b>Note:</b> If any errors display, stop and contact My Oracle Support (MOS).</p>
58. <input type="checkbox"/>	<b>SOAM VIP GUI:</b> Examine all alarms	<ol style="list-style-type: none"> <li>1. Navigate to <b>Alarms &amp; Events &gt; View Active</b>.   </li> <li>2. Examine all active alarms and refer to the on-line help on how to address them.</li> </ol> <p>If needed, contact My Oracle Support (MOS).</p>
59. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Examine all alarms	<ol style="list-style-type: none"> <li>1. Navigate to <b>Alarms &amp; Events &gt; View Active</b>.   </li> <li>2. Examine all active alarms and refer to the on-line help on how to address them.</li> </ol> <p>If needed, contact My Oracle Support (MOS).</p>
60. <input type="checkbox"/>	Restart oampAgent, if needed	<p><b>Note:</b> If <b>10012: The responder for a monitored table failed to respond to a table change</b> alarm displays, the oampAgent needs to be restarted.</p> <ol style="list-style-type: none"> <li>1. Establish an SSH session to each server that has the alarm.</li> <li>2. Login admusr</li> <li>3. Execute the following commands:</li> </ol> <pre>\$ sudo pm.set off oampAgent \$ sudo pm.set on oampAgent</pre>
61. <input type="checkbox"/>	Back up and archive all the databases from the recovered system	Execute the <b>DSR Database Backup</b> procedure to back up the configuration databases.
62. <input type="checkbox"/>	Recover IDIH	If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.

## 4.5 Recovery Scenario 5 (Both NOAM Servers Failed with DR-NOAM Available)

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

- Switch DR NOAM from secondary to primary
- Recover the failed NOAM servers by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
  - The database is intact at the newly active NOAM server and does not require restoration
- If applicable, recover any failed SOAM and MP servers by recovering base hardware and software
  - Recover the base hardware
  - Recover the software
  - The database is intact at the active NOAM server and does not require restoration at the SOAM and MP servers
- Recover IDIH if necessary

### Procedure 5. Recovery Scenario 5

S T E P #		This procedure performs recovery if both NOAM servers have failed but a DR NOAM is available. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.
1. <input type="checkbox"/>	Workarounds	Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist. Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases: 1. If SNMP is not configured in DSR. 2. If SNMP is already configured and SNMPv3 is selected as enabled version.
2. <input type="checkbox"/>	Gather required materials	Gather the documents and required materials listed in Required Materials.
3. <input type="checkbox"/>	Switch DR NOAM to primary	Refer to [13] DSR/SDS NOAM Failover User's Guide.

**Procedure 5. Recovery Scenario 5**

4. <input type="checkbox"/>	Recover failed SOAMs	<p>If ALL SOAM servers have failed, execute Procedure 2.</p> <p>If ALL NOAM servers have failed, execute:</p> <ol style="list-style-type: none"> <li>1. Procedure 4, steps 4. through 14.</li> <li>2. Perform keyexchange between the newly active NOAM and the recovered NOAM PMAC.</li> </ol> <p>From a terminal window connection on the active NOAM as the <b>admusr</b> user, exchange SSH keys for <b>admusr</b> between the active NOAM and the recovered NOAM's PMAC server using the keyexchange utility, using the management IP address for the PMAC server.</p> <p>When asked for the password, enter the password for the <b>admusr</b> user of the PMAC server.</p> <pre>\$ keyexchange admusr@&lt;Recovered_Servers_PMAC_IP Address&gt;</pre> <p><b>Note:</b> If keyexchange fails, edit <b>/home/admusr/.ssh/known_hosts</b> and remove blank lines. Retry the keyexchange commands.</p> <ol style="list-style-type: none"> <li>3. Use the PMAC GUI to determine the control network IP address of the recovered VMs.</li> <li>4. Navigate to <b>Software Inventory</b>.</li> <li>5. Perform a keyexchange between the recovered PMAC and the recovered guests:</li> </ol> <p>From a terminal window connection on the recovered PMAC as the <b>admusr</b> user, exchange SSH keys for <b>admusr</b> between the PMAC and the recovered VM guests using the keyexchange utility, using the control network IP addresses for the VM guests.</p> <p>When asked for the password, enter the password for the <b>admusr</b> user of the VM guest.</p> <pre>\$ keyexchange admusr@&lt;Recovered_VM_control_IP Address&gt;</pre> <p><b>Note:</b> If keyexchange fails, edit <b>/home/admusr/.ssh/known_hosts</b> and remove blank lines. Retry the keyexchange commands.</p> <ol style="list-style-type: none"> <li>6. Procedure 4, steps 15. through 19. for each NOAM.</li> </ol>
5. <input type="checkbox"/>	Perform keyexchange between active NOAM and recovered NOAMs	<p>Perform a keyexchange between the newly active NOAM and the recovered NOAM servers:</p> <ol style="list-style-type: none"> <li>8. From a terminal window connection on the active NOAM as the <b>admusr</b> user, exchange SSH keys for <b>admusr</b> between the active NOAM and the recovered NOAM servers using the keyexchange utility, using the host names of the recovered NOAMs.</li> <li>9. When prompted for the password, enter the password for the <b>admusr</b> user of the recovered NOAM servers.</li> </ol> <pre>\$ keyexchange admusr@&lt;Recovered_NOAM Hostname&gt;</pre>

**Procedure 5. Recovery Scenario 5**

6. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Recover standby/spare SOAM and C-level servers	If necessary, refer to Procedure 3 to recover any standby or Spare SOAMs as well as any C-Level servers.
7. <input type="checkbox"/>	<b>Recovered NOAM Servers:</b> Activate optional features	<p>Map-Diameter Interworking (MAP-IWF) and/or Policy and Charging Application (PCA) Only</p> <p>Activate the features Map-Diameter Interworking (MAP-IWF) and Policy and Charging Application (PCA) as follows:</p> <p><b>For PCA:</b></p> <p>Establish SSH sessions to the all the recovered NOAM servers and login as <b>admusr</b>. Refer [7] and execute <b>PCA Activation on Standby NOAM Server</b> on all recovered NOAM servers to re-activate PCA.</p> <p><b>For MAP-IWF:</b></p> <p>Establish SSH session to the recovered active NOAM, login as <b>admusr</b>. Refer to [5] to activate Map-Diameter Interworking (MAP-IWF).</p> <p><b>Note:</b> While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored:</p> <pre>iload#31000{S/W Fault}</pre> <p><b>Note:</b> If any of the MPs are failed and recovered, then restart these MP servers after activation of the feature.</p>
8. <input type="checkbox"/>	<b>NOAM VIP:</b> Copy key file to all the servers in topology (RADIUS only)	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>1. Check if existing key file on active NOAM (the NOAM, which is intact and was not recovered) server is valid: <div data-bbox="532 1224 1425 1310" data-label="Text"> <pre>\$ cd /usr/TKLC/dpi/bin/ \$ ./sharedKrevo -validate</pre> </div> <p><b>Note:</b> If output of above command shows that existing key file is not valid, contact My Oracle Support (MOS).</p> </li> <li>2. Copy the key file from active DR NOAM to recovered NOAMs. <div data-bbox="483 1451 1425 1528" data-label="Text"> <pre>\$ ./sharedKrevo -copyKey -destServer &lt;First NOAM server&gt; \$ ./sharedKrevo -copyKey -destServer &lt;Second NOAM server&gt;</pre> </div> </li> </ol>

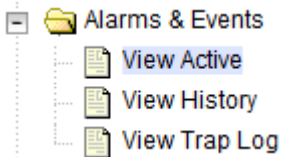
**Procedure 5. Recovery Scenario 5**

9. <input type="checkbox"/>	<b>Primary NOAM:</b> Modify DSR OAM process	<ol style="list-style-type: none"> <li>1. Establish an SSH session to the primary NOAM, login as <b>admusr</b>.</li> <li>2. Retrieve the cluster ID of the recovered NOAM:             <div data-bbox="532 338 1435 493" data-label="Text"> <pre>\$ sudo iqt -fClusterID TopologyMapping where "NodeID='&lt;DR_NOAM_Host_Name&gt;' " Server_ID      NodeID ClusterID 1 Oahu-DSR-NOAM-2 A1055</pre> </div> </li> <li>3. Execute this command to start the DSR OAM process on the recovered NOAM:             <div data-bbox="532 577 1435 653" data-label="Text"> <pre>\$ echo "&lt;clusterID&gt; DSROAM_Proc Yes"   iload -ha -xun -fcluster -fresource -foptional HaClusterResourceCfg</pre> </div> </li> </ol>
10. <input type="checkbox"/>	Switch DR NOAM back to secondary	Once the system has been recovered, refer to [13] DSR/SDS NOAM Failover User's Guide.

**Procedure 5. Recovery Scenario 5**

11. <input type="checkbox"/>	<b>NOAM VIP:</b> Verify all servers in topology are accessible (RADIUS only).  DSR only. If SDS, then skip to the next step.	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>1. Establish an SSH session to the NOAM VIP and login as <b>admusr</b>.</li> <li>2. Check if all the servers in the topology are accessible: <pre>\$ /usr/TKLC/dpi/bin/ \$ ./sharedKrevo -checkAccess</pre> <p><b>Note:</b> If any server is not accessible, stop and contact My Oracle Support (MOS).</p> </li> <li>3. Copy the key file to all the servers in the topology: <pre>\$ ./sharedKrevo -synchronize</pre> <p>Example output:</p> <pre>FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722733: [INFO] Synched key to IPFE FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722734: NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722735: [INFO] Synched key to MP-2 FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722736: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722738: [INFO] Synched key to MP-1 [admusr@NOAM-2 bin]\$</pre> <pre>\$ ./sharedKrevo -updateData</pre> <p>Example output:</p> <pre>[admusr@NOAM-1 bin]\$ ./sharedKrevo -updateData 1450203518: [INFO] Updating data on server 'NOAM-1' 1450203519: [INFO] Data updated to 'NOAM-1' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203520: [INFO] Updating data on server 'SOAM-2' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203522: [INFO] 1 rows updated on 'SOAM-2'... 1450203522: [INFO] Data updated to 'SOAM-2'</pre> <p><b>Note:</b> If any errors display, stop and contact My Oracle Support (MOS).</p> </li> </ol>
------------------------------	---	---

**Procedure 5. Recovery Scenario 5**

12. <input type="checkbox"/>	<b>Recovered Servers:</b> Verify alarms	<p>1. Navigate to <b>Alarms &amp; Events &gt; View Active</b>.</p>  <p>2. Verify the recovered servers are not contributing to any active alarms (Replication, Topology misconfiguration, database impairments, NTP, etc.)</p>
13. <input type="checkbox"/>	Recover IDIH	If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.

**4.6 Recovery Scenario 6 (Database Recovery)****4.6.1 Recovery Scenario 6: Case 1**

For a partial outage with

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

**Notes:**


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

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

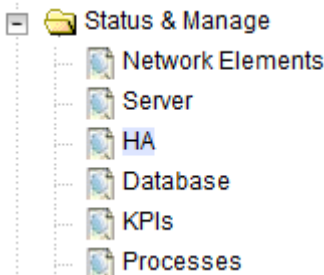
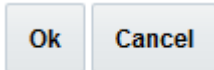
<b>STEP #</b>	<p>This procedure performs recovery if at least one NOAM server is available, but all SOAM servers in a site have failed. This includes any SOAM server that is in another location.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>	
1. <input type="checkbox"/>	Workarounds	Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.



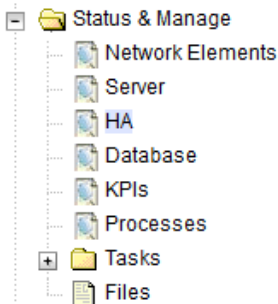
**Procedure 6. Recovery Scenario 6 (Case 1)**

2.	<b>NOAM VIP GUI:</b> Login	<div data-bbox="516 247 1430 310"><p>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:</p></div> <div data-bbox="565 323 1369 369"><p><code>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</code></p></div> <div data-bbox="516 382 902 411"><p>2. Login as the <b>guiadmin</b> user:</p></div> <div data-bbox="776 441 1166 499"></div> <div data-bbox="526 550 763 579"><p>Oracle System Login</p></div> <div data-bbox="1166 575 1406 596"><p>Tue Jun 7 13:49:06 2016 EDT</p></div> <div data-bbox="688 634 1247 978"><div data-bbox="688 634 1247 978"><p><b>Log In</b></p><p>Enter your username and password to log in</p><p>Username: <input type="text"/></p><p>Password: <input type="password"/></p><p><input type="checkbox"/> Change password</p><p><input type="button" value="Log In"/></p></div></div> <div data-bbox="548 991 1386 1037"><p>Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.</p></div> <div data-bbox="630 1054 1299 1100"><p>Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</p></div> <div data-bbox="688 1121 1243 1142"><p>Copyright © 2010, 2016, <a href="#">Oracle</a> and/or its affiliates. All rights reserved.</p></div>
----	-------------------------------	--

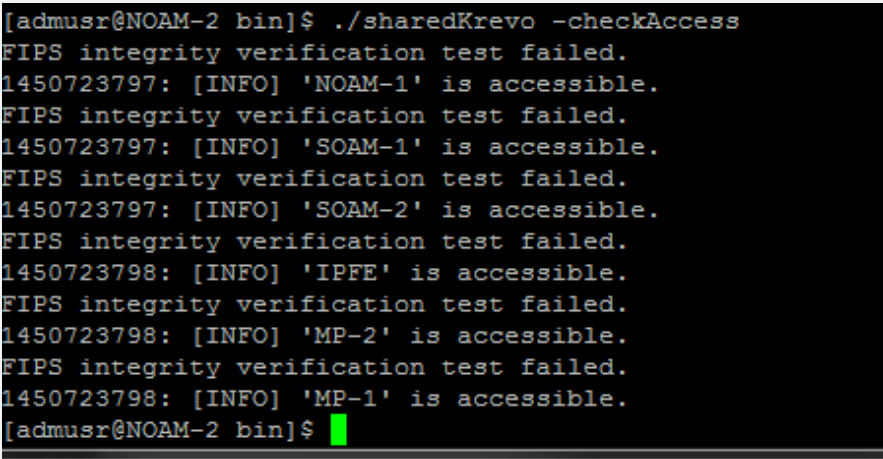
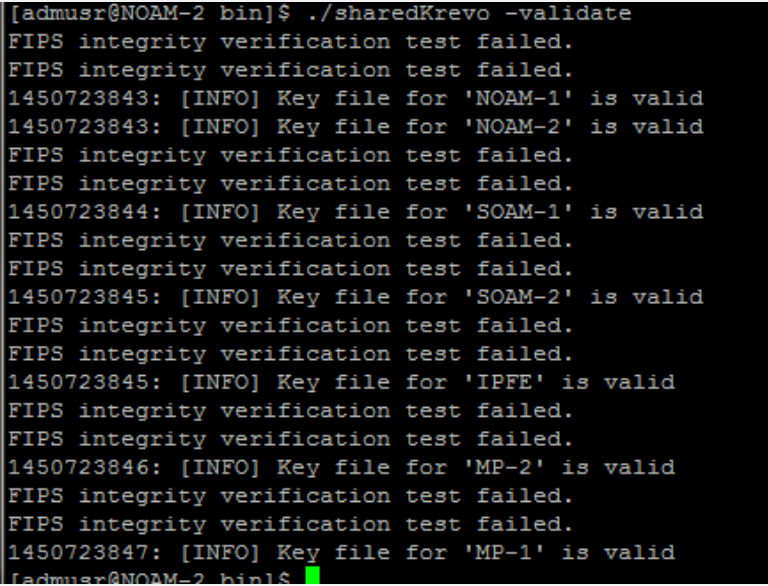
**Procedure 6. Recovery Scenario 6 (Case 1)**

3. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set failed servers to OOS	<ol style="list-style-type: none"> <li>Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>Select <b>Edit</b>.  <b>Modifying HA attributes</b>  <table border="1" data-bbox="521 709 1057 1052"> <thead> <tr> <th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td><td>Active</td><td>The maximum des</td></tr> <tr> <td>ZombieNOAM2</td><td>OOS</td><td>The maximum des</td></tr> <tr> <td>ZombieDRNOAM1</td><td>OOS</td><td>The maximum des</td></tr> </tbody> </table> </li> <li>Set the Max Allowed HA Role option to <b>OOS</b> for the failed servers.</li> <li>Click <b>OK</b>.   </li> </ol>	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active	The maximum des	ZombieNOAM2	OOS	The maximum des	ZombieDRNOAM1	OOS	The maximum des
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active	The maximum des												
ZombieNOAM2	OOS	The maximum des												
ZombieDRNOAM1	OOS	The maximum des												
4. <input type="checkbox"/>	<b>Server in Question:</b> Login	Establish an SSH session to the server in question. Login as <b>admusr</b> .												
5. <input type="checkbox"/>	<b>Server in Question:</b> Change runlevel to 3	Bring the system to runlevel 3. <pre>\$ sudo init 3</pre>												
6. <input type="checkbox"/>	<b>Server in Question:</b> Recover system	Execute this command and follow the instructions appearing in the console prompt. <pre>\$ sudo /usr/TKLC/appworks/sbin/backout_restore</pre>												
7. <input type="checkbox"/>	<b>Server in Question:</b> Change runlevel to 4	Bring the system back to runlevel 4. <pre>\$ sudo init 6</pre>												

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

<p>8.</p> <p><input type="checkbox"/></p>	<p><b>Server in Question:</b> Verify the server</p>	<p>Verify if the processes are up and running.</p> <pre>\$ sudo pm.getprocs</pre> <p>Example output:</p> <pre>A 5139 cmha Up 12/21 13:16:25 1 cmha A 5140 cmplatalarm Up 12/21 13:16:25 1 cmplatalarm A 5143 cmsnmpsa Up 12/21 13:16:25 1 cmsnmpsa -R 1.3.6.1.4.1.3 23.5.3.28.1 A 5145 cmsoapa Up 12/21 13:16:25 1 cmsoapa A 9969 eclipseHelp Up 12/21 13:16:39 1 eclipseHelp A 5149 idbsvc Up 12/21 13:16:25 1 idbsvc -M10 -ME204 -D40 - DE820 -W1 -S2 A 6149 idbunlock Up 12/21 13:16:36 1 idbunlock -f A 5151 inetmerge Up 12/21 13:16:25 1 inetmerge A 5155 inetrep Up 12/21 13:16:25 1 inetrep A 5160 oampAgent Up 12/21 13:16:25 1 oampAgent A 5164 pm.watchdog Up 12/21 13:16:25 1 pm.watchdog A 5167 raclerk Up 12/21 13:16:25 1 raclerk -r 6000 A 5171 re.portmap Up 12/21 13:16:25 1 re.portmap -c100 A 5174 statclerk Up 12/21 13:16:25 1 statclerk -s -0 A 5177 vipmgr Up 12/21 13:16:25 1 vipmgr A -1 AstateInit Done 12/21 13:16:36 1 AstateInit A -1 auditPTask Done 12/21 13:16:36 1 auditPeriodicTask A -1 auditTasks Done 12/21 13:16:36 1 auditDefunctTasks A -1 guiReqMapLoad Done 12/21 13:16:25 1 guiReqMapLoad A -1 mkdbhooks Done 12/21 13:16:25 1 mkdbhooks [root@MP-1 adminr]#</pre>												
<p>9.</p> <p><input type="checkbox"/></p>	<p><b>NOAM VIP GUI:</b> Set failed servers to active</p>	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.</li> </ol>  <ol style="list-style-type: none"> <li>2. Click <b>Edit</b>.</li> <li>3. Select the failed server and set it to <b>Active</b>.</li> </ol> <p><b>Modifying HA attributes</b></p> <table border="1"> <thead> <tr> <th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td><td>Active</td><td>The maximum</td></tr> <tr> <td>ZombieNOAM2</td><td>Active</td><td>The maximum</td></tr> <tr> <td>ZombieDRNOAM1</td><td>Active Standby Snare</td><td>The maximum</td></tr> </tbody> </table> <ol style="list-style-type: none"> <li>4. Click <b>OK</b>.</li> </ol>	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active	The maximum	ZombieNOAM2	Active	The maximum	ZombieDRNOAM1	Active Standby Snare	The maximum
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active	The maximum												
ZombieNOAM2	Active	The maximum												
ZombieDRNOAM1	Active Standby Snare	The maximum												

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

10. <input type="checkbox"/>	<b>NOAM VIP:</b> Verify all servers in topology are accessible (RADIUS only)	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>1. Establish an SSH session to the NOAM VIP and login as <b>admusr</b>.</li> <li>2. Check if all the servers in the Topology are accessible:</li> </ol> <pre>\$ cd /usr/TKLC/dpi/bin/ \$ ./sharedKrevo -checkAccess</pre> 
11. <input type="checkbox"/>	<b>NOAM VIP:</b> Copy key file to all the servers in topology (RADIUS only)	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>1. Check if existing key file on active NOAM (The NOAM which is intact and was not recovered) server is valid:</li> </ol> <pre>\$ ./sharedKrevo -validate</pre>  <p>If output of above command shows the existing key file is not valid, contact My Oracle Support (MOS).</p>

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


		<p>2. Copy the key file to all the servers in the Topology:</p> <pre> \$ ./sharedKrevo -synchronize FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722733: [INFO] Synched key to IPFE FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722734: NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722735: [INFO] Synched key to MP-2 FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722736: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722738: [INFO] Synched key to MP-1 [admusr@NOAM-2 bin]\$  \$ ./sharedKrevo -updateData [admusr@NOAM-1 bin]\$ ./sharedKrevo -updateData 1450203518: [INFO] Updating data on server 'NOAM-1' 1450203519: [INFO] Data updated to 'NOAM-1' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203520: [INFO] Updating data on server 'SOAM-2' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203522: [INFO] 1 rows updated on 'SOAM-2'... 1450203522: [INFO] Data updated to 'SOAM-2' </pre> <p><b>Note:</b> If any errors are present, stop and contact My Oracle Support (MOS).</p>
12.	<input type="checkbox"/> Backup and archive all the databases from the recovered system	Execute DSR Database Backup to back up the Configuration databases.

## 4.6.2 Recovery Scenario 6: Case 2

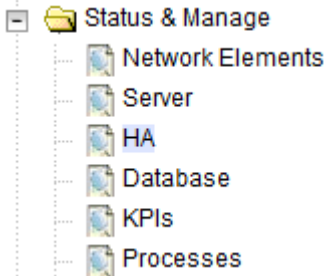
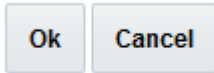
For a partial outage with:

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

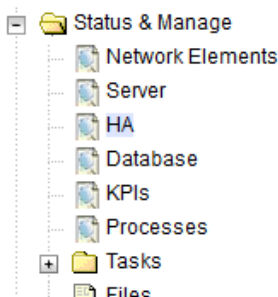
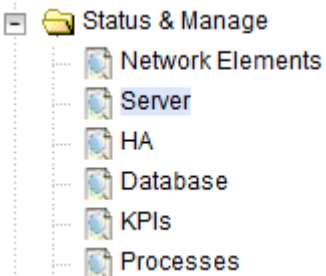

### Procedure 7. Recovery Scenario 6 (Case 2)

STEP #	<p>This procedure performs recovery if at least one NOAM server is available, but all SOAM servers in a site have failed. This includes any SOAM server that is in another location.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>	
1. <input type="checkbox"/>	Workarounds	Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.
2. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Login	<p>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:</p> <div data-bbox="565 877 1369 926" style="border: 1px solid black; padding: 2px;"> <code>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</code> </div> <p>2. Login as the <b>guiadmin</b> user:</p> <div data-bbox="526 995 1417 1707">  </div>

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

3. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set failed servers to OOS	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>2. Click <b>Edit</b>.  <b>Modifying HA attributes</b>  <table border="1" data-bbox="522 718 1058 1058"> <thead> <tr> <th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td><td>Active</td><td>The maximum des</td></tr> <tr> <td>ZombieNOAM2</td><td>OOS</td><td>The maximum des</td></tr> <tr> <td>ZombieDRNOAM1</td><td>OOS</td><td>The maximum des</td></tr> </tbody> </table> </li> <li>3. Set the Max Allowed HA Role option to <b>OOS</b> for the failed servers.</li> <li>4. Click <b>OK</b>.   </li> </ol>	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active	The maximum des	ZombieNOAM2	OOS	The maximum des	ZombieDRNOAM1	OOS	The maximum des
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active	The maximum des												
ZombieNOAM2	OOS	The maximum des												
ZombieDRNOAM1	OOS	The maximum des												
4. <input type="checkbox"/>	<b>Server in Question:</b> Login	Establish an SSH session to the server in question. Login as <b>admusr</b> .												
5. <input type="checkbox"/>	<b>Server in Question:</b> Stop httpd service	Stop the httpd service. <pre>\$ sudo bash -l</pre> Stop the HTTPD service before the database is down and start the HTTPD service after the database has started. <pre>\$ service httpd stop</pre>												
6. <input type="checkbox"/>	<b>Server in Question:</b> Take server out of service	Take the server out of service. <pre>\$ prod.clobber</pre>												
7. <input type="checkbox"/>	<b>Server in Question:</b> Take server to DbUp state and start the application	Take the server to Dbup and start the DSR application. <pre>\$ prod.start</pre>												

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

8. <input type="checkbox"/>	<b>Server in Question:</b> Start httpd service	<ol style="list-style-type: none"> <li>1. Start the httpd service.  <pre>\$ service httpd start</pre> </li> <li>2. Exit out of root.  <pre>\$ exit</pre> </li> </ol>												
9. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Set failed servers to active	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.   </li> <li>2. Click <b>Edit</b> at the bottom of the screen.</li> <li>3. Select the failed server and set it to <b>Active</b>.  <b>Modifying HA attributes</b>  <table border="1" data-bbox="527 976 998 1249"> <thead> <tr> <th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td><td>Active ▼</td><td>The maximum</td></tr> <tr> <td>ZombieNOAM2</td><td>Active ▼</td><td>The maximum</td></tr> <tr> <td>ZombieDRNOAM1</td><td>Active ▼ Standby Snare</td><td>The maximum</td></tr> </tbody> </table> </li> <li>4. Click <b>OK</b>.</li> </ol>	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active ▼	The maximum	ZombieNOAM2	Active ▼	The maximum	ZombieDRNOAM1	Active ▼ Standby Snare	The maximum
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active ▼	The maximum												
ZombieNOAM2	Active ▼	The maximum												
ZombieDRNOAM1	Active ▼ Standby Snare	The maximum												
10. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Restart DSR application	<ol style="list-style-type: none"> <li>1. Navigate to <b>Status &amp; Manage &gt; Server</b>.   </li> <li>2. Select each recovered server and click <b>Restart</b>.   </li> </ol>												



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

11. <input type="checkbox"/>	<b>Server in Question:</b> Verify the server state	<ol style="list-style-type: none"> <li>Verify the processes are up and running:  <pre>\$ sudo pm.getprocs</pre> <p>Example output:</p> <pre>A 5139 cmha Up 12/21 13:16:25 1 cmha A 5140 cmplatalarm Up 12/21 13:16:25 1 cmplatalarm A 5143 cmsnmpsa Up 12/21 13:16:25 1 cmsnmpsa -R 1.3.6.1.4.1.3 23.5.3.28.1 A 5145 cmsopa Up 12/21 13:16:25 1 cmsopa A 9969 eclipseHelp Up 12/21 13:16:39 1 eclipseHelp A 5149 idbsvc Up 12/21 13:16:25 1 idbsvc -M10 -ME204 -D40 - DE820 -W1 -S2 A 6149 idbunlock Up 12/21 13:16:36 1 idbunlock -f A 5151 inetmerge Up 12/21 13:16:25 1 inetmerge A 5155 inetrep Up 12/21 13:16:25 1 inetrep A 5160 oampAgent Up 12/21 13:16:25 1 oampAgent A 5164 pm.watchdog Up 12/21 13:16:25 1 pm.watchdog A 5167 raclerk Up 12/21 13:16:25 1 raclerk -r 6000 A 5171 re.portmap Up 12/21 13:16:25 1 re.portmap -c100 A 5174 statclerk Up 12/21 13:16:25 1 statclerk -s -0 A 5177 vipmgr Up 12/21 13:16:25 1 vipmgr A -1 AstateInit Done 12/21 13:16:36 1 AstateInit A -1 auditPTask Done 12/21 13:16:36 1 auditPeriodicTask A -1 auditTasks Done 12/21 13:16:36 1 auditDefunctTasks A -1 guiReqMapLoad Done 12/21 13:16:25 1 guiReqMapLoad A -1 mkdbhooks Done 12/21 13:16:25 1 mkdbhooks [root@MP-1 admusr]#</pre> </li> <li>Verify if replication channels are up and running:  <pre>\$ sudo irepstat</pre> <p>Example output:</p> <pre>-- Policy 0 ActStb [DbReplication] ----- BC From SOAM-2 Active 0 0.50 ^0.04%cpu 34B/s A=C2713.145 CC From MP-2 Active 0 0.20 ^0.05 1.57%cpu 35B/s A=C2713.145  -- Policy 1001 DSR_SLDB_Policy [] ----- 1 CC From MP-2 Active 0 0.20 ^0.06 1.51%cpu 35B/s A=C2713.145</pre> </li> <li>Verify if merging channels are up and running:  <pre>\$ sudo inetmstat</pre> <p>Example output:</p> <pre>nodeId InetMerge State dir dSeq dTime updTime info SOAM-1 Standby To 0 0.00 13:19:33 SOAM-2 Active To 0 0.00 13:19:33</pre> </li> </ol>
12. <input type="checkbox"/>	<b>NOAM VIP:</b> Verify all servers in topology are accessible (RADIUS Only). DSR only. If SDS, skip to step 14.	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>Establish an SSH session to the NOAM VIP and login as <b>admusr</b>.</li> <li>Check if all the servers in the Topology are accessible:  <pre>\$ cd /usr/TKLC/dpi/bin/ \$ ./sharedKrevo -checkAccess</pre> </li> </ol>

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

13. <input type="checkbox"/>	<b>NOAM VIP:</b> Copy key file to all the servers in topology (RADIUS Only)	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>1. Check if existing key file on active NOAM (the NOAM which is intact and was not recovered) server is valid: <div data-bbox="565 426 1425 510" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>\$ cd /usr/TKLC/dpi/bin/ \$ ./sharedKrevo -validate</pre> </div> <p>If output shows the existing key file is not valid, contact My Oracle Support (MOS).</p> </li> <li>2. Copy the key file to all the servers in the topology: <div data-bbox="532 636 1425 1581" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>\$ ./sharedKrevo -synchronize FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722733: [INFO] Synched key to IPFE FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722734: NOAM-2 and MP-2 key files differ. Sync NOAM-2 key file to MP-2. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722735: [INFO] Synched key to MP-2 FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722736: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722738: [INFO] Synched key to MP-1 [admusr@NOAM-2 bin]\$  \$ ./sharedKrevo -updateData [admusr@NOAM-1 bin]\$ ./sharedKrevo -updateData 1450203518: [INFO] Updating data on server 'NOAM-1' 1450203519: [INFO] Data updated to 'NOAM-1' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203520: [INFO] Updating data on server 'SOAM-2' FIPS integrity verification test failed. FIPS integrity verification test failed. 1450203522: [INFO] 1 rows updated on 'SOAM-2'... 1450203522: [INFO] Data updated to 'SOAM-2'</pre> </div> </li> </ol> <p><b>Note:</b> If any errors are present, stop and contact My Oracle Support (MOS).</p>
14. <input type="checkbox"/>	Backup and archive all the databases from the recovered system	Execute DSR Database Backup to back up the Configuration databases.

## 5. Resolve User Credential Issues after Database Restore

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


### 5.1 Restore a Deleted User

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

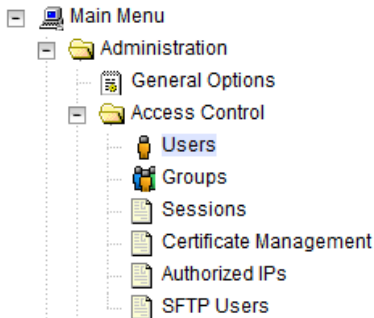

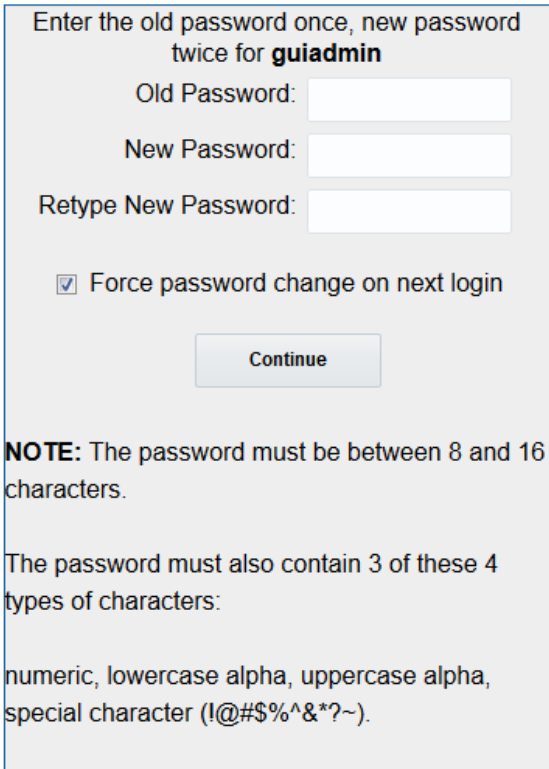
These users were removed before creation of the backup and archive file. They are reintroduced by system restoration of that file.

### 5.2 Keep a Restored User

#### Procedure 8. Keep Restored User


S T E P #	Perform this procedure to keep users restored by system restoration. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. <input type="checkbox"/>	<b>Before Restoration:</b> Notify affected users before restoration	Contact each user affected before the restoration and notify them that you will reset their password during this maintenance operation.
2. <input type="checkbox"/>	<b>After Restoration:</b> Log into the NOAM VIP	<p>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">http://&lt;Primary_NOAM_VIP_IP_Address&gt;</div> <p>2. Login as the <b>guiadmin</b> user:</p> <div style="text-align: center; margin: 20px 0;">  </div> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p><b>Oracle System Login</b> <span style="float: right;">Tue Jun 7 13:49:06 2016 EDT</span></p> <div style="text-align: center; margin-top: 20px;"> <p><b>Log In</b></p> <p>Enter your username and password to log in</p> <p>Username: <input style="width: 150px;" type="text"/></p> <p>Password: <input style="width: 150px;" type="password"/></p> <p><input type="checkbox"/> Change password</p> <p><input type="button" value="Log In"/></p> </div> </div>

**Procedure 8. Keep Restored User**

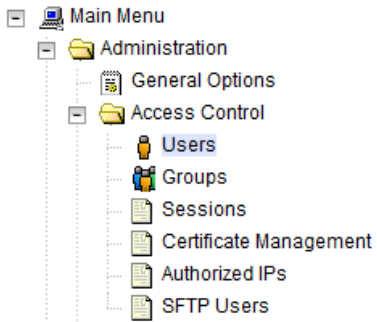


<p>3. <input type="checkbox"/></p>	<p><b>After Restoration:</b> Reset user passwords</p>	<ol style="list-style-type: none"> <li>1. Navigate to <b>Administration &gt; Access Control &gt; Users</b>.   </li> <li>2. Select the user.</li> <li>3. Click <b>Change Password</b>.   </li> <li>4. Type a new password.   </li> <li>5. Click <b>Continue</b>.</li> </ol>
------------------------------------	---	--

## 5.3 Remove a Restored User

### Procedure 9. Remove the Restored User

S T E P #	<p>Perform this procedure to remove users restored by system restoration</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>
1. <input type="checkbox"/>	<p><b>After Restoration:</b> Log into the NOAM VIP</p> <ol style="list-style-type: none"> <li>Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:               <div data-bbox="532 541 1333 590" style="border: 1px solid black; padding: 2px; margin: 5px 0;">                 http://&lt;Primary_NOAM_VIP_IP_Address&gt;               </div> </li> <li>Login as the <b>guiadmin</b> user:</li> </ol> <div data-bbox="483 659 1442 1423" style="text-align: center;">  <p>The screenshot shows the Oracle System Login page. At the top is the Oracle logo in red. Below it is the text 'Oracle System Login' followed by a horizontal line. To the right of the line is the date and time 'Tue Jun 7 13:49:06 2016 EDT'. In the center is a light gray box with a blue border containing the 'Log In' form. The form has the title 'Log In' and the instruction 'Enter your username and password to log in'. It includes fields for 'Username:' and 'Password:', a 'Change password' checkbox, and a 'Log In' button. Below the form box, there is a disclaimer: 'Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.' At the bottom, there is a footer with trademark information and a copyright notice: 'Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.'</p> </div>

**Procedure 9. Remove the Restored User**

2. <input type="checkbox"/>	<b>After Restoration:</b> Reset user passwords	<ol style="list-style-type: none"> <li>1. Navigate to <b>Administration &gt; Access Control &gt; Users</b>.   </li> <li>2. Select the user.</li> <li>3. Click <b>Delete</b>.     Delete selected users?   </li> <li>4. Click <b>OK</b> to confirm.</li> </ol>
-----------------------------	---	--

**5.4 Restore a Modified User**

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

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

**Before Restoration:**

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

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

**After Restoration:**

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


**5.5 Restore an Archive that Does Not Contain a Current User**

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

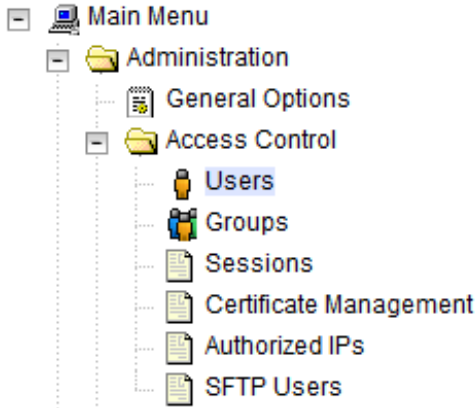
- User 'testuser' exists in current database but not in the selected backup file.

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

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


<b>S T E P #</b>	<p>Perform this procedure to remove users restored by system restoration.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>	
1. <input type="checkbox"/>	<b>Before Restoration:</b> Notify affected users before restoration	Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.
2. <input type="checkbox"/>	<b>Before Restoration:</b> Log into the NOAM VIP	<ol style="list-style-type: none"> <li>Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:  <div data-bbox="565 653 1369 699" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <code>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</code> </div> </li> <li>Login as the <b>guiadmin</b> user:</li> </ol> <div data-bbox="526 772 1429 1491" style="text-align: center;">  <p>The screenshot shows the Oracle System Login page. At the top is the Oracle logo. Below it is the title 'Oracle System Login' and a timestamp 'Tue Jun 7 13:49:06 2016 EDT'. A central box contains the 'Log In' form with fields for 'Username' and 'Password', a 'Change password' checkbox, and a 'Log In' button. At the bottom, there is a disclaimer: 'Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.' followed by trademark information and a copyright notice: 'Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.'</p> </div>

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

<p>3. <input type="checkbox"/></p>	<p><b>Before Restoration:</b> Record user settings</p>	<p>1. Navigate to <b>Administration &gt; Access Control &gt; Users</b>.</p>  <p>2. Under each affected user, record the following:</p> <ul style="list-style-type: none"><li>• Username</li><li>• Account status</li><li>• Remote Auth</li><li>• Local Auth</li><li>• Concurrent Logins Allowed</li><li>• Inactivity Limit</li><li>• Comment</li><li>• Groups</li></ul>
------------------------------------	--	--



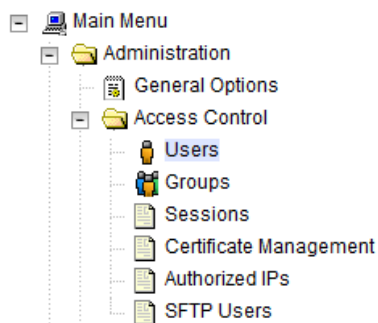
**Procedure 10. Restore an Archive That Does Not Contain a Current User**

<div>4.</div> <div><input type="checkbox"/></div>	<b>After Restoration:</b> Login	<div>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: <div>http://&lt;Primary_NOAM_VIP_IP_Address&gt;</div></div> <div>2. Login as the <b>guiadmin</b> user:</div> <div></div>
---	------------------------------------	---

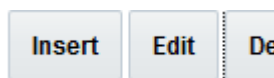
**Procedure 10. Restore an Archive That Does Not Contain a Current User**

5. ☐ After restoration:  
recreate affected  
user

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



2. Click **Insert**.



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

**Adding new user**

Username *	<input type="text"/>	Select long
Group *	admin	Select
Authentication Options	<input type="checkbox"/> Allow Remote Authentication <input checked="" type="checkbox"/> Allow Local Authentication	Select *Admin action [Default]
Access Options	<input checked="" type="checkbox"/> Allow GUI Access <input checked="" type="checkbox"/> Allow MMI Access	Select
Access Allowed	<input checked="" type="checkbox"/> Account Enabled	Is the
Maximum Concurrent Logins	0	The
Session Inactivity Limit	120	The
Comment *	<input type="text"/>	Con

4. Click **OK**.

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

6. <input type="checkbox"/>	<b>After Restoration:</b> Repeat for additional users	Repeat step 5 to recreate additional users.
7. <input type="checkbox"/>	<b>After Restoration:</b> Reset the passwords	See Procedure 8 for resetting passwords for a user.

**6. IDIH Disaster Recovery**

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

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

```

</infrastructure>
</infrastructures>
<servers>
.....
.
    <tvoeguest id="ORA">
        <infrastructure>localPMAC</infrastructure>
        </postdeploy>
    </scripts>
</tvoeguest
.....
.
    <tvoeguest id="MED">
        <infrastructure>localPMAC</infrastructure>
        <!--Specify which Rack Mount Server TVOE Host the Mediation
server will be placed -->
        <tvoehost>mgmtsrvrtvove2</tvoehost>
        <name>MED</name>


```

**Disaster Recovery Scenarios**

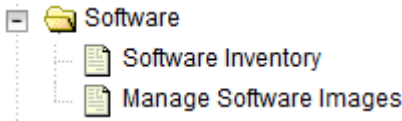
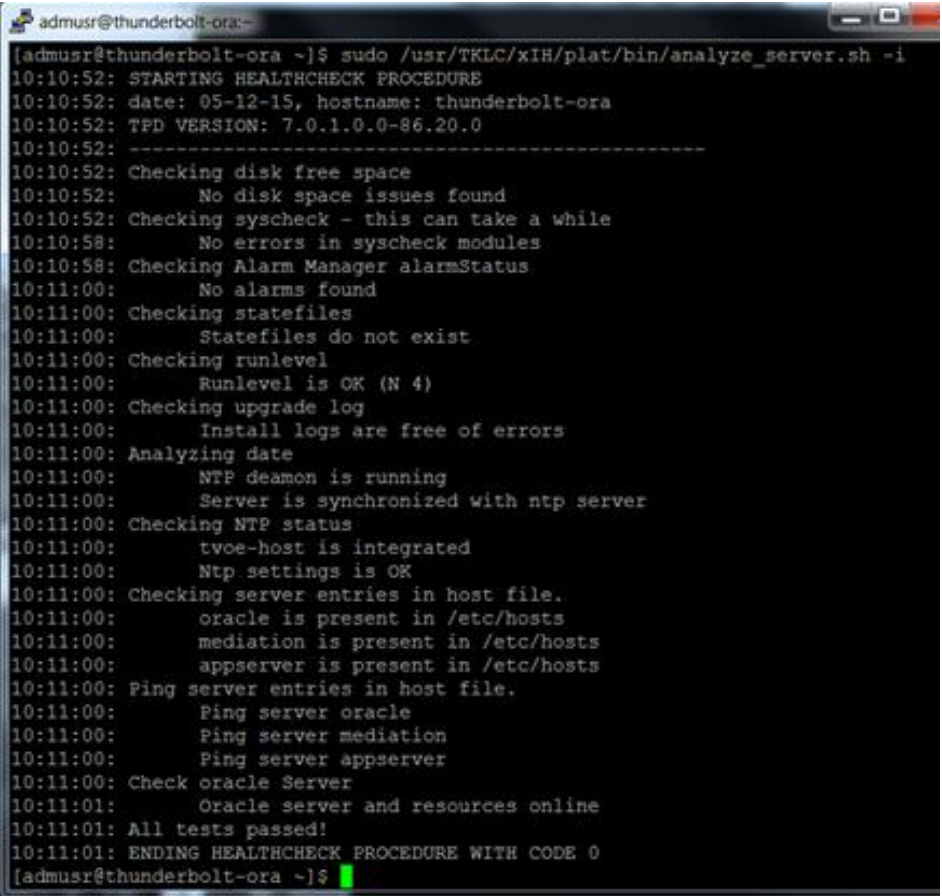
Disaster Recovery Scenario	fdconfig file to use
Server containing Oracle database server	Install fdconfig xml
Server containing Application Server	Upgrade/Disaster Recovery xml

Server containing Mediation Server	Upgrade/Disaster Recovery xml
------------------------------------	-------------------------------


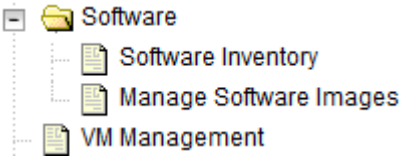
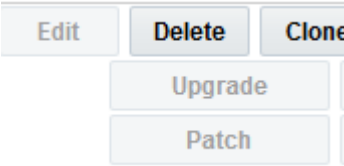
**Procedure 11. IDIH Disaster Recovery Preparation**

<b>S T E P #</b>	<p>This procedure performs disaster recovery preparation steps for the IDIH.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>
1. <input type="checkbox"/>	<p><b>PMAC GUI:</b> Login</p> <p>1. Open web browser and enter:</p> <div data-bbox="532 548 1333 594" style="border: 1px solid black; padding: 2px; margin: 5px 0;">http://&lt;PMAC_Mgmt_Network_IP&gt;</div> <p>2. Login as <b>pmacadmin</b> user:</p> <div data-bbox="483 667 1442 1423" style="text-align: center;">  <p><b>Oracle System Login</b></p> <p>Tue Jun 7 13:49:06 2016 EDT</p> <div data-bbox="667 877 1268 1247" style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 80%;"> <p><b>Log In</b></p> <p>Enter your username and password to log in</p> <p>Username: <input style="width: 100px;" type="text"/></p> <p>Password: <input style="width: 100px;" type="password"/></p> <p><input type="checkbox"/> Change password</p> <p><input type="button" value="Log In"/></p> </div> <p>Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.</p> <hr/> <p><i>Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</i></p> <p><i>Copyright © 2010, 2016, <a href="#">Oracle</a> and/or its affiliates. All rights reserved.</i></p> </div>

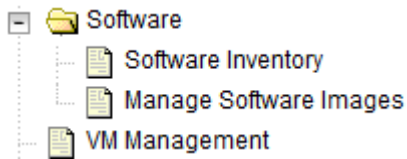
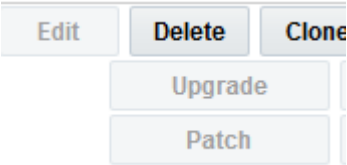

## Procedure 11. IDIH Disaster Recovery Preparation

2. <input type="checkbox"/>	<b>PMAC GUI:</b> Verify necessary IDIH images are available	<ol style="list-style-type: none"> <li>1. Navigate to <b>Software &gt; Manage Software Images</b>.   </li> <li>2. Verify the current IDIH TVOE, TPD, Oracle, Application and Mediation images are listed.</li> <li>3. Verify these values match the name in the &lt;software&gt; &lt;/software&gt; section in the <b>hostname-upgrade_xx-xx-xx.xml</b> file.</li> </ol> <p><b>Note:</b> If the necessary software images are not available, follow the instructions from the <b>Load Application and TPD ISO onto PMAC Server</b> procedure and steps 1-4 of <b>IDIH Configuration</b> from [8] to acquire and transfer the images.</p>
3. <input type="checkbox"/>	<b>Oracle Guest:</b> Login	Establish an SSH session to the Oracle guest, login as <b>admusr</b> .
4. <input type="checkbox"/>	<b>Oracle Guest:</b> Perform database health check	Perform a database health check: <pre>\$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i</pre> <p>Example output:</p> 

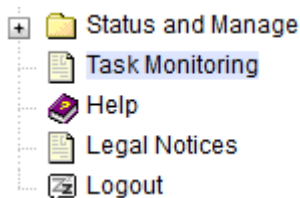
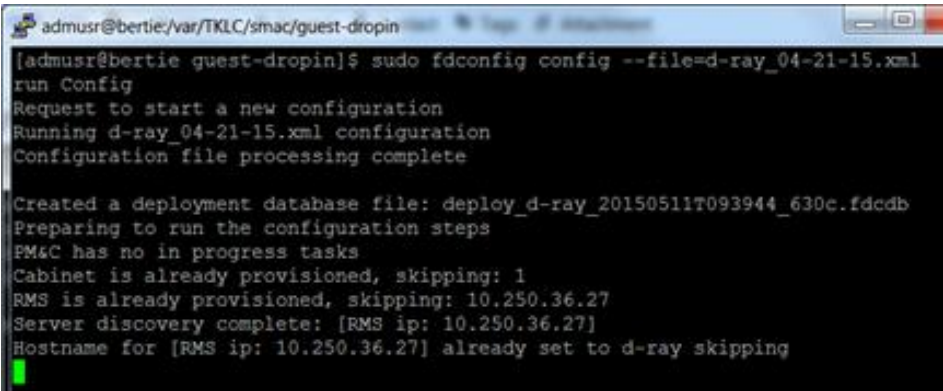
**Procedure 12. IDIH Disaster Recovery (Re-Install Mediation and Application Servers)**

STEP #	<p>This procedure performs disaster recovery for the IDIH by re-installing the mediation and application servers.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>	
<p>1.</p> <p><input type="checkbox"/></p>	<p><b>PMAC GUI: Login</b></p>	<p>1. Open web browser and enter:</p> <div data-bbox="553 478 1357 531" style="border: 1px solid black; padding: 2px;"> <p>http://&lt;PMAC_Mgmt_Network_IP&gt;</p> </div> <p>2. Login as <b>pmacadmin</b> user:</p>  <p>Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.</p> <p>Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</p> <p>Copyright © 2010, 2016, <a href="#">Oracle</a> and/or its affiliates. All rights reserved.</p>
<p>2.</p> <p><input type="checkbox"/></p>	<p>Remove existing application server</p>	<p>1. Navigate to <b>Main Menu &gt; VM Management</b>.</p>  <p>2. Select the application guest.</p> <p>3. Click <b>Delete</b>.</p> 

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

3. <input type="checkbox"/>	Remove existing mediation server	<ol style="list-style-type: none"> <li>1. Navigate to <b>Main Menu &gt; VM Management</b>.   </li> <li>2. Select the Mediation guest.</li> <li>3. Click <b>Delete</b>.   </li> </ol>
4. <input type="checkbox"/>	<b>PMAC:</b> Establish SSH session and login	Establish an SSH session to the PMAC, login as <b>admusr</b> .
5. <input type="checkbox"/>	<b>PMAC:</b> Re-install the mediation and application servers	<p>Execute this command (Enter your upgrade file):</p> <pre>\$ cd /var/TKLC/smac/guest-dropin \$ screen \$ sudo fdconfig config --file=&lt;hostname-upgrade_xx-xx-xx&gt;.xml</pre> <div style="text-align: center;">  <p><b>Warning</b></p> <p>If you run the fdconfig without <b>upgrade</b> in the XML filename, the database is destroyed and you lose all of the existing data.</p> <p><b>Note:</b> <b>Note:</b> This is a long duration command (45-90 minutes). If the screen command was run before executing the fdconfig, perform a <b>screen -dr</b> to resume the screen session in the event of a terminal timeout etc.</p> </div>


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

6. <input type="checkbox"/>	<b>PMAC GUI:</b> Monitor the configuration	<ol style="list-style-type: none"> <li>1. If not already done, establish a GUI session on the PMAC server.</li> <li>2. Navigate to <b>Task Monitoring</b>.   </li> <li>3. Monitor the IDIH configuration to completion.            Alternatively, you can monitor the fdconfig status through the command line after executing the fdconfig command:            Example:            </li> </ol>
-----------------------------	---	---



## Appendix A. DSR Database Backup

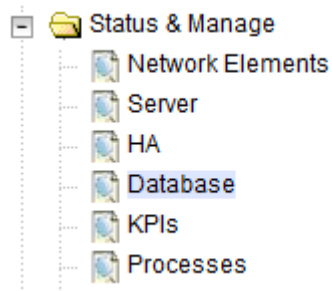
### Procedure 13. DSR Database Backup

S T E P #	<p>This procedure backs up the provision and configuration information from an NOAM or SOAM server after the disaster recovery is complete.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>
<p>1. <input type="checkbox"/></p>	<p><b>NOAM/SOAM VIP: Login</b></p> <ol style="list-style-type: none"> <li>Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server. Open the web browser and enter a URL of: <div data-bbox="532 632 1386 680" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <code>http://&lt;Primary_NOAM/SOAM_VIP_IP_Address&gt;</code> </div> </li> <li>Login as the <b>guiadmin</b> user:</li> </ol> <div data-bbox="483 743 1448 1507" style="text-align: center;">  <p>The screenshot shows the Oracle System Login page. At the top is the Oracle logo. Below it is the title 'Oracle System Login' and a timestamp 'Tue Jun 7 13:49:06 2016 EDT'. A central box contains a 'Log In' form with fields for 'Username' and 'Password', a 'Change password' checkbox, and a 'Log In' button. At the bottom, there is a disclaimer: 'Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.' followed by trademark and copyright information.</p> </div>

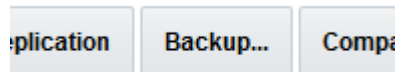
**Procedure 13. DSR Database Backup**

2. **NOAM/SOAM VIP:** Backup configuration data for the system

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



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



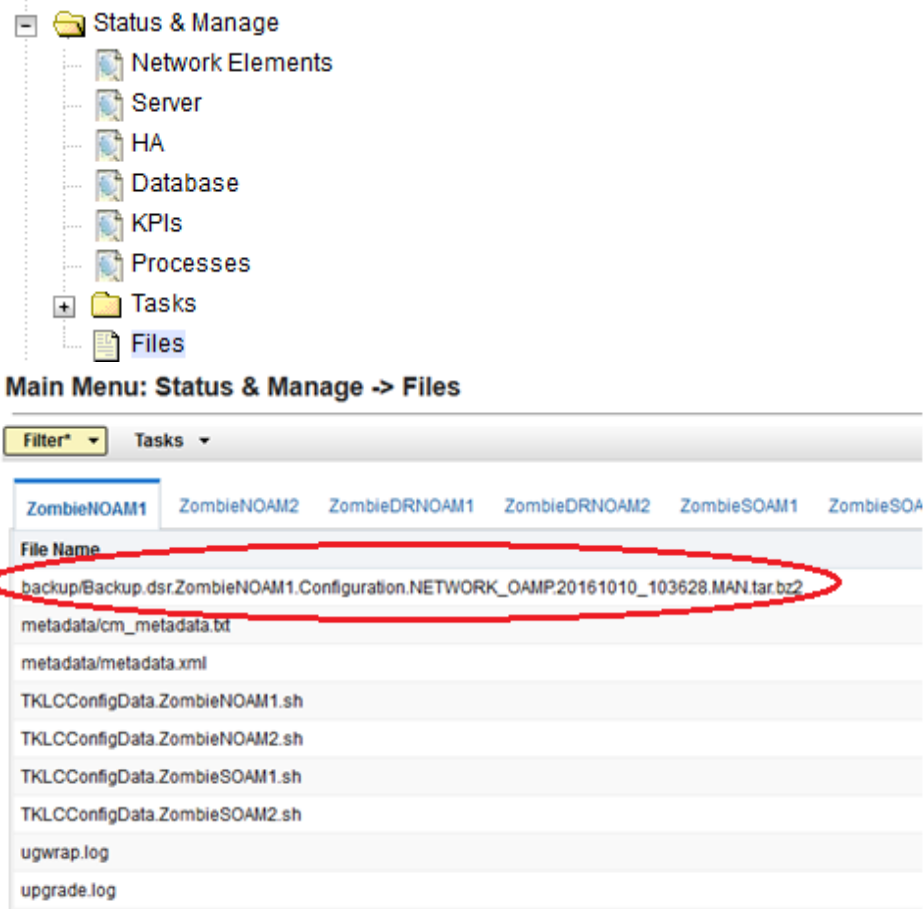
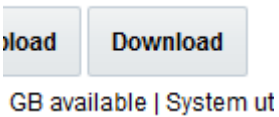
3. Make sure that the **Configuration** checkbox is marked.

**Database Backup**

Field	Value
<b>Server: ZombieNOAM1</b>	
Select data for backup	<input type="checkbox"/> Provisioning <input checked="" type="checkbox"/> Configuration
Compression *	<input type="radio"/> gzip <input checked="" type="radio"/> bzip2 <input type="radio"/> none
Archive Name *	Backup.dsr.ZombieNOAM1.Configuration.NETV
Comment	<input type="text"/>
<input type="button" value="Ok"/> <input type="button" value="Cancel"/>	

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

**Procedure 13. DSR Database Backup**

<p>3. <input type="checkbox"/></p>	<p><b>NOAM/SOAM VIP:</b> Verify the backup file existence</p>	<p>1. Navigate to <b>Status &amp; Manage &gt; Files</b>.</p>  <p>2. Select the active NOAM or SOAM tab.</p> <p>3. The files on this server display. Verify the existence of the backup file.</p>
<p>4. <input type="checkbox"/></p>	<p><b>NOAM/SOAM VIP:</b> Download the file to a local machine</p>	<p>1. From the previous step, select the backup file.</p> <p>2. Click <b>Download</b>.</p>  <p>3. Click <b>OK</b> to confirm the download.</p>
<p>5. <input type="checkbox"/></p>	<p>Upload the image to secure location</p>	<p>Transfer the backed up image saved in the previous step to a secure location where the server backup files are located in case of system disaster recovery.</p>
<p>6. <input type="checkbox"/></p>	<p>Backup active SOAM</p>	<p>Repeat steps 2 through 5 to back up the active SOAM.</p>

**Procedure 13. DSR Database Backup**

7. <input type="checkbox"/>	Take Secured backup of key file (RADIUS only)	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> <li>1. Log into ssh shell of active NOAM server using user <b>admusr</b>.</li> <li>2. Take secure backup of updated key file <b>RADIUS shared secret encryption key</b> for disaster scenarios.</li> <li>3. Encrypt the key file before backing up to secure customer setup: <div data-bbox="527 514 917 562" data-label="Text"> <pre>\$ ./sharedKrevo -encr</pre> </div> </li> <li>4. Copy the encrypted key file to secure customer setup: <div data-bbox="527 619 1437 697" data-label="Text"> <pre>\$ sudo scp /var/TKLC/db/filemgmt/DpiKf.bin.encr user@&lt;customer IP&gt;:&lt;path of customer setup&gt;</pre> </div> </li> </ol> <p><b>Note:</b> The operator must strictly control access to the backed up key file. If the operator needs to encrypt this key file further using operator specified encryption techniques, the operator is recommended to do so; however, the operator is responsible to decrypt this file using operator-specific decryption techniques and copy the resulting <b>DpiKf.bin.encr</b> file securely to the file management folder if the key file needs to be restored for disaster recovery. Once the key file is backed up to the operator-provided server and path, it is the responsibility of the operator to ensure access to the backed up key file is extremely selective and restricted.</p>
--------------------------------	---	--

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

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

<b>S T E P #</b>	<p>This procedure recovers a failed aggregation (4948E/4948E-F) switch.</p> <p><b>Prerequisites:</b></p> <ul style="list-style-type: none"> <li>• A copy of the networking xml configuration files</li> <li>• A copy of HP miscellaneous firmware DVD or ISO</li> <li>• IP address and hostname of the failed switch</li> <li>• Rack mount position of the failed switch</li> </ul> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>
<b>1.</b> <input type="checkbox"/>	<p><b>Recover failed Aggregation Switches:</b> Cisco 4948E/4948E-F</p> <ol style="list-style-type: none"> <li>1. Log into the PMAC using SSH as <b>admusr</b>.</li> <li>2. Remove the old SSH key of the switch from the PMAC by executing this command from a PMAC command shell: <div data-bbox="553 852 1161 905" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>sudo ssh-keygen -R &lt;4948_switch_IP&gt;</pre> </div> </li> <li>3. Refer to the Replace a failed 4948/4948E/4948E-F switch (c-Class System) (netConfig) procedure in reference [2] to replace a failed aggregation switch. <p><b>Note:</b> You need a copy of the HP Misc Firmware DVD or ISO (or firmware file obtained from the appropriate hardware vendor) and the original networking XML files custom for this installation. These are either stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.</p> <p><b>Note:</b> Copy the switch appropriate init file and use it for respective switch:</p> <p>Older platform init files may not work on platform 7.2 systems. Copy the switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy <b>switch1A_4948_4948E_init.xml</b>.</p> </li> <li>4. The templates can be found using the following method: <p>From the PMAC CLI:</p> <div data-bbox="553 1415 1424 1467" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>df   grep -I DSR</pre> </div> <p><b>Sample output:</b></p> <pre>/var/TKLC/smac/image/repository/DSR- 8.4.0.0.0_84.9.0-x86_64.iso 1118514 1118514 0 100% /usr/TKLC/smac/html/TPD/DSR- 8.4.0.0.0_84.9.0-x86_64 /var/TKLC/smac/image/repository/DSR- 8.4.0.0.0_84.9.0-x86_64.iso 1118372 1118372 0 100% /usr/TKLC/smac/html/TPD/DSR- 8.4.0.0.0_84.9.0-x86_64 /var/TKLC/smac/image/repository/DSR- 8.4.0.0.0_84.9.0-x86_64.iso</pre> </li> </ol>

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

	<pre>1117976 1117976 0 100% /usr/TKLC/smac/html/TPD/DSR-8.4.0.0.0_84.9.0-x86_64</pre> <p>5. Determine the applicable directory of the DSR release being recovered.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>cd usr/TKLC/smac/html/TPD/&lt;DSR Release dir&gt;/upgrade/overlay/</pre> </div> <p>Example:</p> <pre>cd /usr/TKLC/smac/html/TPD/DSR- 8.4.0.0.0_84.9.0-x86_64 /upgrade/overlay/</pre> <p>6. Locate the DSR_NetConfig_Templates.zip file.</p> <p>Example:</p> <pre>\$ ll total 286 -r--r--r-- 1 root root 611 Feb 21 19:18 change_ilo_admin_passwd.xml -r--r--r-- 1 root root 107086 Feb 21 19:18 DSR_NetConfig_Templates.zip -r--r--r-- 1 root root 11642 Feb 21 19:18 DSR_NOAM_FD_Blade.xml -r--r--r-- 1 root root 13346 Feb 21 19:18 DSR_NOAM_FD_RMS.xml dr-xr-xr-x 2 root root 2048 Feb 21 19:18 RMS -r--r--r-- 1 root root 812 Feb 21 19:18 SAMPLE-NetworkElement.xml -r--r--r-- 1 root root 2309 Feb 21 19:20 TRANS.TBL -r-xr-xr-x 1 root root 2186 Feb 21 19:18 TVOEcfig.sh -r-xr-xr-x 1 root root 598 Feb 21 19:18 TVOEcfile.sh -r--r--r-- 1 root root 128703 Feb 21 19:18 UpgradeHCplugin.php-ovl -r--r--r-- 1 root root 19658 Feb 21 19:18 upgradeHealthCheck-ovl</pre> <p>7. Unzip the DSR_NetConfig_Templates.zip file and retrieve the required switch init file.</p> <p>Example:</p> <pre>\$ unzip DSR_NetConfig_Templates.zip</pre> <p>8. Edit the desired file with site specific details. The existing file from original deployment /usr/TKLC/smac/etc/switch/xml can be used as a reference.</p> <p>9. Copy the new init file to the /usr/TKLC/smac/etc/switch/xml dir.</p> <p>Example:</p> <pre>\$ cp &lt;switch_xml_file&gt; /usr/TKLC/smac/etc/switch/xml/</pre>
--	---

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

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

STEP #	This procedure inhibits A and B level replication on all C-level servers of this site. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.																																														
1. <input type="checkbox"/>	<b>Active NOAM:</b> Login	Log into the active NOAM server using SSH as <b>admusr</b> .																																													
2. <input type="checkbox"/>	<b>Active NOAM:</b> Inhibit replication on all C-level servers	<div>Execute this command:</div> <div><pre>\$ for i in \$(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='&lt;SOAM Site_NE name of the site&gt;'); do iset -finhibitRepPlans='A B' NodeInfo where "nodeName='\$i'; done</pre></div> <div><b>Note:</b> SOAM Site_NE name of the site can be found out by logging into the active NOAM GUI and navigating to <b>Configuration &gt; Server Groups</b>.</div> <div>The following figure shows more details, for example, if ServerSO1 belongs to the site being recovered, then siteId is SO_HPC03.</div> <div>Main Menu: Configuration -&gt; Servers</div> <div><div>Filter* Info*</div><table><thead><tr><th>Hostname</th><th>Role</th><th>System ID</th><th>Server Group</th><th>Network Element</th></tr></thead><tbody><tr><td>ZombieNOAM1</td><td>Network OAM&amp;P</td><td></td><td>ZombieNOAM</td><td>ZombieNOAM</td></tr><tr><td>ZombieNOAM2</td><td>Network OAM&amp;P</td><td></td><td>ZombieNOAM</td><td>ZombieNOAM</td></tr><tr><td>ZombieDRNOAM1</td><td>Network OAM&amp;P</td><td></td><td>ZombieDRNOAM</td><td>ZombieDRNOAM</td></tr><tr><td>ZombieDRNOAM2</td><td>Network OAM&amp;P</td><td></td><td>ZombieDRNOAM</td><td>ZombieDRNOAM</td></tr><tr><td>ZombieSOAM1</td><td>System OAM</td><td></td><td>ZombieSOAM</td><td>ZombieSOAM</td></tr><tr><td>ZombieSOAM2</td><td>System OAM</td><td></td><td>ZombieSOAM</td><td>ZombieSOAM</td></tr><tr><td>ZombieDAMP1</td><td>MP</td><td></td><td>ZombieDAMP</td><td>ZombieSOAM</td></tr><tr><td>ZombieDAMP2</td><td>MP</td><td></td><td>ZombieDAMP</td><td>ZombieSOAM</td></tr></tbody></table></div>	Hostname	Role	System ID	Server Group	Network Element	ZombieNOAM1	Network OAM&P		ZombieNOAM	ZombieNOAM	ZombieNOAM2	Network OAM&P		ZombieNOAM	ZombieNOAM	ZombieDRNOAM1	Network OAM&P		ZombieDRNOAM	ZombieDRNOAM	ZombieDRNOAM2	Network OAM&P		ZombieDRNOAM	ZombieDRNOAM	ZombieSOAM1	System OAM		ZombieSOAM	ZombieSOAM	ZombieSOAM2	System OAM		ZombieSOAM	ZombieSOAM	ZombieDAMP1	MP		ZombieDAMP	ZombieSOAM	ZombieDAMP2	MP		ZombieDAMP	ZombieSOAM
Hostname	Role	System ID	Server Group	Network Element																																											
ZombieNOAM1	Network OAM&P		ZombieNOAM	ZombieNOAM																																											
ZombieNOAM2	Network OAM&P		ZombieNOAM	ZombieNOAM																																											
ZombieDRNOAM1	Network OAM&P		ZombieDRNOAM	ZombieDRNOAM																																											
ZombieDRNOAM2	Network OAM&P		ZombieDRNOAM	ZombieDRNOAM																																											
ZombieSOAM1	System OAM		ZombieSOAM	ZombieSOAM																																											
ZombieSOAM2	System OAM		ZombieSOAM	ZombieSOAM																																											
ZombieDAMP1	MP		ZombieDAMP	ZombieSOAM																																											
ZombieDAMP2	MP		ZombieDAMP	ZombieSOAM																																											
3. <input type="checkbox"/>	<b>Active NOAM:</b> Verify replication has been Inhibited	<div>After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.</div> <div>Verify replication inhibition on MPs by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site, for example, Site SO_HPC03 is set as <b>A B</b>.</div> <div><pre>\$ iqt NodeInfo</pre></div> <div>Example output:</div> <table><thead><tr><th>nodeId</th><th>nodeName</th><th>hostName</th><th>nodeCapability</th><th>inhibitRepPlans</th><th>siteId</th></tr></thead><tbody><tr><td>A1386.099</td><td>NO1</td><td>NO1</td><td>Active</td><td></td><td>NO_HPC03</td></tr><tr><td>B1754.109</td><td>SO1</td><td>SO1</td><td>Active</td><td></td><td>SO_HPC03</td></tr><tr><td>C2254.131</td><td>MP2</td><td>MP2</td><td>Active</td><td>A B</td><td>SO_HPC03</td></tr><tr><td>C2254.233</td><td>MP1</td><td>MP1</td><td>Active</td><td>A B</td><td>SO_HPC03</td></tr></tbody></table>	nodeId	nodeName	hostName	nodeCapability	inhibitRepPlans	siteId	A1386.099	NO1	NO1	Active		NO_HPC03	B1754.109	SO1	SO1	Active		SO_HPC03	C2254.131	MP2	MP2	Active	A B	SO_HPC03	C2254.233	MP1	MP1	Active	A B	SO_HPC03															
nodeId	nodeName	hostName	nodeCapability	inhibitRepPlans	siteId																																										
A1386.099	NO1	NO1	Active		NO_HPC03																																										
B1754.109	SO1	SO1	Active		SO_HPC03																																										
C2254.131	MP2	MP2	Active	A B	SO_HPC03																																										
C2254.233	MP1	MP1	Active	A B	SO_HPC03																																										

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

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

STEP #	This procedure un-inhibits A and B level replication on all C-level servers of this site. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.																																														
1. <input type="checkbox"/>	<b>Active NOAM:</b> Login	Log into the active NOAM server using SSH as <b>admusr</b> .																																													
2. <input type="checkbox"/>	<b>Active NOAM:</b> Un-Inhibit replication on all C-level servers	<div>Execute this command:</div> <div><pre>\$ for i in \$(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='&lt;SOAM_Site_NE_name&gt;'); do iset -finhibitRepPlans=' ' NodeInfo where "nodeName='\$i'; done</pre></div> <div><b>Note:</b> SOAM Site NE name of the site can be found out by logging into the active NOAM GUI and navigating to <b>Configuration &gt; Server Groups</b>.</div> <div>Please see the snapshot below for more details, for example, if ServerSO1 belongs to the site being recovered, then siteID is SO_HPC03.</div> <div>Main Menu: Configuration -&gt; Servers</div> <div><div>Filter* Info*</div><table><thead><tr><th>Hostname</th><th>Role</th><th>System ID</th><th>Server Group</th><th>Network Element</th></tr></thead><tbody><tr><td>ZombieNOAM1</td><td>Network OAMP</td><td></td><td>ZombieNOAM</td><td>ZombieNOAM</td></tr><tr><td>ZombieNOAM2</td><td>Network OAMP</td><td></td><td>ZombieNOAM</td><td>ZombieNOAM</td></tr><tr><td>ZombieDRNOAM1</td><td>Network OAMP</td><td></td><td>ZombieDRNOAM</td><td>ZombieDRNOAM</td></tr><tr><td>ZombieDRNOAM2</td><td>Network OAMP</td><td></td><td>ZombieDRNOAM</td><td>ZombieDRNOAM</td></tr><tr><td>ZombieSOAM1</td><td>System OAM</td><td></td><td>ZombieSOAM</td><td>ZombieSOAM</td></tr><tr><td>ZombieSOAM2</td><td>System OAM</td><td></td><td>ZombieSOAM</td><td>ZombieSOAM</td></tr><tr><td>ZombieOAMP1</td><td>MP</td><td></td><td>ZombieOAMP</td><td>ZombieSOAM</td></tr><tr><td>ZombieOAMP2</td><td>MP</td><td></td><td>ZombieOAMP</td><td>ZombieSOAM</td></tr></tbody></table></div>	Hostname	Role	System ID	Server Group	Network Element	ZombieNOAM1	Network OAMP		ZombieNOAM	ZombieNOAM	ZombieNOAM2	Network OAMP		ZombieNOAM	ZombieNOAM	ZombieDRNOAM1	Network OAMP		ZombieDRNOAM	ZombieDRNOAM	ZombieDRNOAM2	Network OAMP		ZombieDRNOAM	ZombieDRNOAM	ZombieSOAM1	System OAM		ZombieSOAM	ZombieSOAM	ZombieSOAM2	System OAM		ZombieSOAM	ZombieSOAM	ZombieOAMP1	MP		ZombieOAMP	ZombieSOAM	ZombieOAMP2	MP		ZombieOAMP	ZombieSOAM
Hostname	Role	System ID	Server Group	Network Element																																											
ZombieNOAM1	Network OAMP		ZombieNOAM	ZombieNOAM																																											
ZombieNOAM2	Network OAMP		ZombieNOAM	ZombieNOAM																																											
ZombieDRNOAM1	Network OAMP		ZombieDRNOAM	ZombieDRNOAM																																											
ZombieDRNOAM2	Network OAMP		ZombieDRNOAM	ZombieDRNOAM																																											
ZombieSOAM1	System OAM		ZombieSOAM	ZombieSOAM																																											
ZombieSOAM2	System OAM		ZombieSOAM	ZombieSOAM																																											
ZombieOAMP1	MP		ZombieOAMP	ZombieSOAM																																											
ZombieOAMP2	MP		ZombieOAMP	ZombieSOAM																																											
3. <input type="checkbox"/>	<b>Active NOAM:</b> Verify replication has been Inhibited	<div>After executing above steps to un-inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.</div> <div>Verify replication inhibition on MPs by analyzing NodeInfo output. The InhibitRepPlans field for all the MP servers for the selected site, for example, Site SO_HPC03 is set as <b>A B</b>.</div> <div><pre>\$ sudo iqt NodeInfo</pre></div> <div>Example output:</div> <div><table><thead><tr><th>nodeId</th><th>nodeName</th><th>hostName</th><th>nodeCapability</th><th>inhibitRepPlans</th><th>siteId</th></tr></thead><tbody><tr><td>A1386.099</td><td>NO1</td><td>NO1</td><td>Active</td><td></td><td>NO_HPC03</td></tr><tr><td>B1754.109</td><td>SO1</td><td>SO1</td><td>Active</td><td></td><td>SO_HPC03</td></tr><tr><td>C2254.131</td><td>MP2</td><td>MP2</td><td>Active</td><td>A B</td><td>SO_HPC03</td></tr><tr><td>C2254.233</td><td>MP1</td><td>MP1</td><td>Active</td><td>A B</td><td>SO_HPC03</td></tr></tbody></table></div>	nodeId	nodeName	hostName	nodeCapability	inhibitRepPlans	siteId	A1386.099	NO1	NO1	Active		NO_HPC03	B1754.109	SO1	SO1	Active		SO_HPC03	C2254.131	MP2	MP2	Active	A B	SO_HPC03	C2254.233	MP1	MP1	Active	A B	SO_HPC03															
nodeId	nodeName	hostName	nodeCapability	inhibitRepPlans	siteId																																										
A1386.099	NO1	NO1	Active		NO_HPC03																																										
B1754.109	SO1	SO1	Active		SO_HPC03																																										
C2254.131	MP2	MP2	Active	A B	SO_HPC03																																										
C2254.233	MP1	MP1	Active	A B	SO_HPC03																																										



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

### Procedure 17. Inhibit A and B Level Replication on C-level Servers

STEP #

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

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

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

1.

Active NOAM: Login

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

2.

Active NOAM: Inhibit replication on all C-level servers

Execute the script from **/usr/TKLC/dsr/tools/InhibitReplication.sh**, if available.

If the **/usr/TKLC/dsr/tools/** path does not have the **InhibitReplication.sh** script, then use this manual command.

```
/usr/TKLC/dsr/tools/InhibitReplication.sh - replication=inhibit --SO_SG_Name=<SOAM server group name>
```

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

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

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

For example, if SOAM1 belongs to the site being recovered, then the server group is SO\_SG.

DRNO_SG	A	NONE	DSR (active/standby pair)	1	<div>Network Element: DSR_DR_NO_NE</div> <table> <tr> <th>Server</th> <th>Node HA Pref</th> <th>VIPs</th> </tr> <tr> <td>DRNOAM1</td> <td></td> <td></td> </tr> <tr> <td>DRNOAM2</td> <td></td> <td></td> </tr> </table>	Server	Node HA Pref	VIPs	DRNOAM1			DRNOAM2		
Server	Node HA Pref	VIPs												
DRNOAM1														
DRNOAM2														
NO_SG	A	NONE	DSR (active/standby pair)	1	<div>Network Element: DSR_NO_NE</div> <table> <tr> <th>Server</th> <th>Node HA Pref</th> <th>VIPs</th> </tr> <tr> <td>NOAM1</td> <td></td> <td></td> </tr> <tr> <td>NOAM2</td> <td></td> <td></td> </tr> </table>	Server	Node HA Pref	VIPs	NOAM1			NOAM2		
Server	Node HA Pref	VIPs												
NOAM1														
NOAM2														
SO_SG	B	NO_SG	DSR (active/standby pair)	1	<div>Network Element: DSR_SO_NE</div> <table> <tr> <th>Server</th> <th>Node HA Pref</th> <th>VIPs</th> </tr> <tr> <td>SOAM1</td> <td></td> <td></td> </tr> <tr> <td>SOAM2</td> <td></td> <td></td> </tr> </table>	Server	Node HA Pref	VIPs	SOAM1			SOAM2		
Server	Node HA Pref	VIPs												
SOAM1														
SOAM2														

Procedure 17. Inhibit A and B Level Replication on C-level Servers

3. <div></div>	<b>Active NOAM:</b> Verify replication has been inhibited	<p>After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled.</p> <p>Verify replication inhibition on MPs by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO_SG is set as <b>A B</b>.</p> <p>Execute this command:</p> <div><pre>\$ iqt NodeInfo</pre></div> <p>Example output:</p> <table><tr><th>nodeId</th><th>nodeName</th><th>hostName</th><th>nodeCapability</th><th>inhibitRepPlans</th><th>siteId</th></tr><tr><td colspan="6">excludeTables</td></tr><tr><td>A1386.099</td><td>NO1</td><td>NO1</td><td>Active</td><td></td><td>NO_HPC03</td></tr><tr><td>B1754.109</td><td>SO1</td><td>SO1</td><td>Active</td><td></td><td>SO_HPC03</td></tr><tr><td>C2254.131</td><td>MP2</td><td>MP2</td><td>Active</td><td>A B</td><td>SO_HPC03</td></tr><tr><td>C2254.233</td><td>MP1</td><td>MP1</td><td>Active</td><td>A B</td><td>SO_HPC03</td></tr></table>	nodeId	nodeName	hostName	nodeCapability	inhibitRepPlans	siteId	excludeTables						A1386.099	NO1	NO1	Active		NO_HPC03	B1754.109	SO1	SO1	Active		SO_HPC03	C2254.131	MP2	MP2	Active	A B	SO_HPC03	C2254.233	MP1	MP1	Active	A B	SO_HPC03
nodeId	nodeName	hostName	nodeCapability	inhibitRepPlans	siteId																																	
excludeTables																																						
A1386.099	NO1	NO1	Active		NO_HPC03																																	
B1754.109	SO1	SO1	Active		SO_HPC03																																	
C2254.131	MP2	MP2	Active	A B	SO_HPC03																																	
C2254.233	MP1	MP1	Active	A B	SO_HPC03																																	

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

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

STEP#

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

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

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

1.

Active NOAM: Login

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

2.

Active NOAM: Un-Inhibit replication on all C-level servers

Execute the script from **/usr/TKLC/dsr/tools/InhibitReplication.sh**, if available.

If the **/usr/TKLC/dsr/tools/** path does not have the **InhibitReplication.sh** script, then use this manual command.

```
/usr/TKLC/dsr/tools/InhibitReplication.sh - replication=allow --SO_SG_Name=<SOAM server group name>
```

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

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

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

For example, if SOAM1 belongs to the site being recovered, then the server group is SO\_SG.

DRNO_SG	A	NONE	DSR (active/standby pair)	1	<div>Network Element: DSR_DR_NO_NE<table><tr><td>Server</td><td>Node HA Pref</td><td>VIPs</td></tr><tr><td>DRNOAM1</td><td></td><td></td></tr><tr><td>DRNOAM2</td><td></td><td></td></tr></table></div>	Server	Node HA Pref	VIPs	DRNOAM1			DRNOAM2		
Server	Node HA Pref	VIPs												
DRNOAM1														
DRNOAM2														
NO_SG	A	NONE	DSR (active/standby pair)	1	<div>Network Element: DSR_NO_NE<table><tr><td>Server</td><td>Node HA Pref</td><td>VIPs</td></tr><tr><td>NOAM1</td><td></td><td></td></tr><tr><td>NOAM2</td><td></td><td></td></tr></table></div>	Server	Node HA Pref	VIPs	NOAM1			NOAM2		
Server	Node HA Pref	VIPs												
NOAM1														
NOAM2														
SO_SG	B	NO_SG	DSR (active/standby pair)	1	<div>Network Element: DSR_SO_NE<table><tr><td>Server</td><td>Node HA Pref</td><td>VIPs</td></tr><tr><td>SOAM1</td><td></td><td></td></tr><tr><td>SOAM2</td><td></td><td></td></tr></table></div>	Server	Node HA Pref	VIPs	SOAM1			SOAM2		
Server	Node HA Pref	VIPs												
SOAM1														
SOAM2														

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

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

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

Verify replication inhibition on MPs by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO\_SG is set as **A B**.

Execute this command:

```
$ sudo iqt NodeInfo
```

Example output:

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

## Appendix G. Restore TVOE Configuration from Backup Media

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

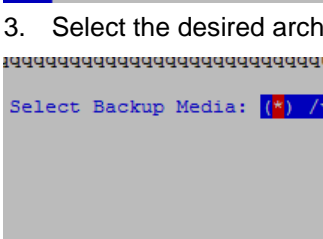
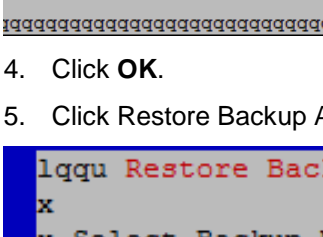
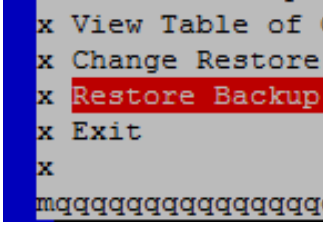
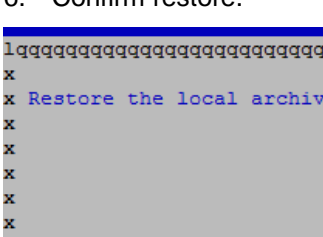
S T E P #	This procedure provides steps to restore the TVOE application configuration from backup media. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. <input type="checkbox"/>	Install TVOE application	<ul style="list-style-type: none"> <li>• If the PMAC is <b>NOT</b> hosted on the failed rack mount server, execute <b>IPM Servers Using PMAC Application</b> from reference [8].</li> <li>• If the PMAC is hosted on the failed rack mount server, execute <b>Installing TVOE on the Management Server</b> from reference [8].</li> </ul>
2. <input type="checkbox"/>	Establish network connectivity	<ul style="list-style-type: none"> <li>• If the PMAC is <b>NOT</b> hosted on the failed rack mount server, <b>skip this step</b>.</li> <li>• If the PMAC is hosted on the failed rack mount server, execute <b>TVOE Network Configuration</b>, steps 1-11, from reference [8].</li> </ul> <p><b>Note:</b> The IP address configured on the TVOE must be one accessible through the network of the machine currently holding the TVOE Backup ISO image. This could be a NetBackup master server, a customer PC, etc.</p>
3. <input type="checkbox"/>	Restore TVOE backup ISO image to the TVOE host (NetBackup)	<p>If using NetBackup to restore the TVOE backup ISO image, then execute this step; otherwise, skip this step.</p> <ol style="list-style-type: none"> <li>1. Execute <b>Application NetBackup Client Installation Procedures</b> from reference [8].</li> <li>2. Interface with the NetBackup master server and initiate a restore of the TVOE backup ISO image.</li> </ol> <p><b>Note:</b> Once restored, the ISO image is in <b>/var/TKLC/bkp/</b> on the TVOE server.</p>

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

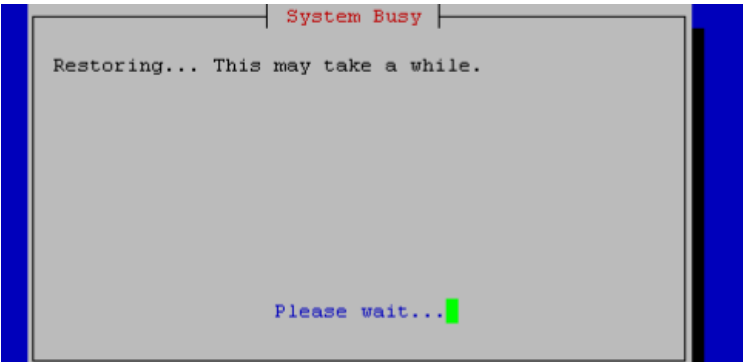
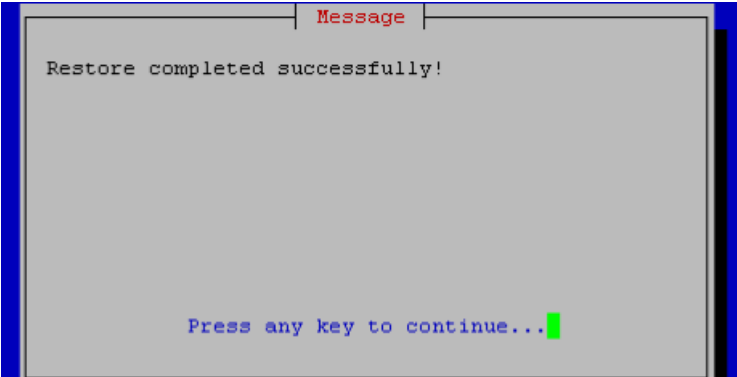
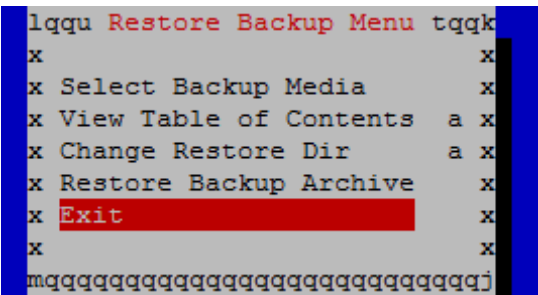
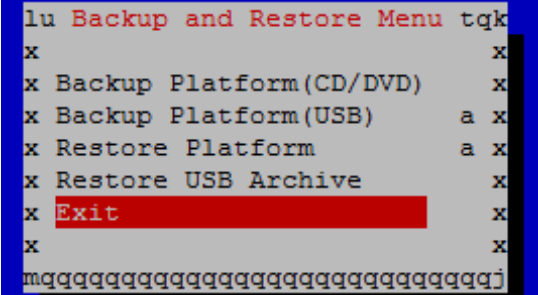
4. <input type="checkbox"/>	Transfer TVOE backup ISO image to the TVOE host	<p>Restore TVOE backup ISO using SCP.</p> <p>Using the IP of the TVOE host, transfer the backup ISO image to the TVOE.</p> <p><b>Linux:</b></p> <p>From the command line of a Linux machine use this command to copy the backup ISO image to the TVOE host:</p> <pre># scp &lt;path_to_image&gt; tvoexfer@&lt;TVOE_IP&gt;:backup/</pre> <p>where &lt;path_to_image&gt; is the path to the backup ISO image on the local system and &lt;TVOE_IP&gt; is the TVOE IP address.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• If the IP is an IPv4 address, then &lt;TVOE_IP&gt; is a normal dot-decimal notation (for example, 10.240.6.170).</li> <li>• If the IP is an IPv6 link local address, then &lt;TVOE_IP&gt; needs to be scoped. For example, <b>[fe80::21e:bff:fe76:5e1c%control]</b> where control is the name of the interface on the machine initiating the transfer and it must be on the same link as the interface on the TVOE host.</li> <li>• The control IP address of the TVOE can be used if the TVOE is NOT hosting the PMAC. This method requires first transferring the backup file to the PMAC, and then to the TVOE host.</li> </ul> <p><b>IPv4 Example:</b></p> <pre># scp /path/to/image.iso tvoexfer@10.240.6.170:backup/</pre> <p><b>IPv6 Example:</b></p> <pre># scp /path/to/image.iso tvoexfer@[fe80::21e:bff:fe76:5e1c%control]:backup/</pre> <p><b>Windows:</b></p> <p>Use WinSCP to copy the Backup ISO image into the <b>/var/TKLC/bkp</b> directory. Refer to [8], the Using WinSCP procedure, to copy the backup image to the customer system.</p>
5. <input type="checkbox"/>	<b>TVOE Server:</b> Login	Establish an SSH session to the TVOE server and login as <b>admusr</b> .

## Procedure 19. Restore TVOE Configuration from Backup Media

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

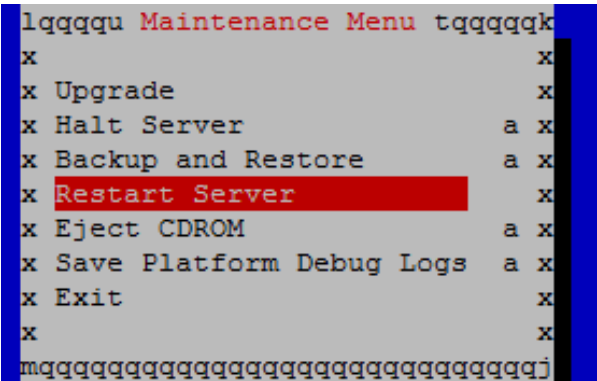
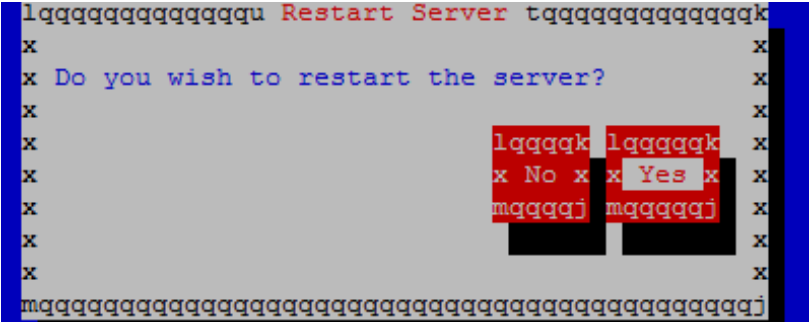
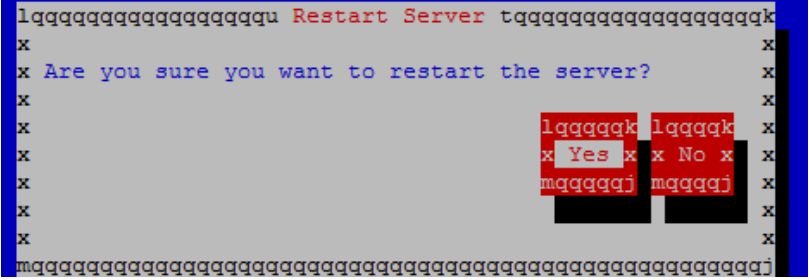
```
$ sudo su - platcfg
```
  2. Navigate to **Maintenance > Backup and Restore > Restore Platform .> Select Backup Media.**

  3. Select the desired archive.
 
  4. Click **OK**.
  5. Click **Restore Backup Archive**.
 
  6. Confirm restore.
 

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

<p>7.</p> <p><input type="checkbox"/></p>	<p>Monitor TVOE backup process</p>	<p>1. Wait for the restore to complete.</p>  <p><b>Note:</b> This typically takes less than 5 minutes.</p>  <p>2. <b>Exit</b> platcfg.</p>
<p>8.</p> <p><input type="checkbox"/></p>	<p><b>TVOE Server:</b> Exit restore backup menu</p>	<p>Exit the Restore Backup Menu.</p>  



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

<p>9. <input type="checkbox"/></p>	<p><b>TVOE Server:</b> Restart</p>	<ol style="list-style-type: none"> <li>Restart the TVOE server.   </li> <li>Click <b>Yes</b> to restart.   </li> <li>Confirm restart.   </li> </ol>
------------------------------------	--	--

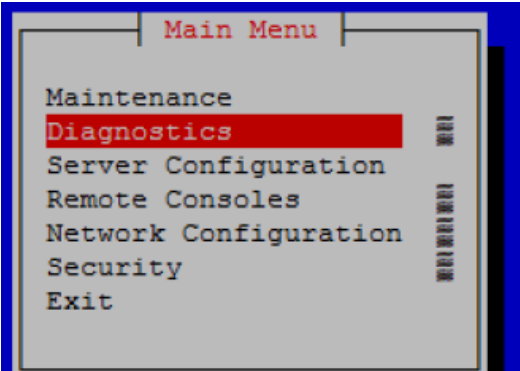
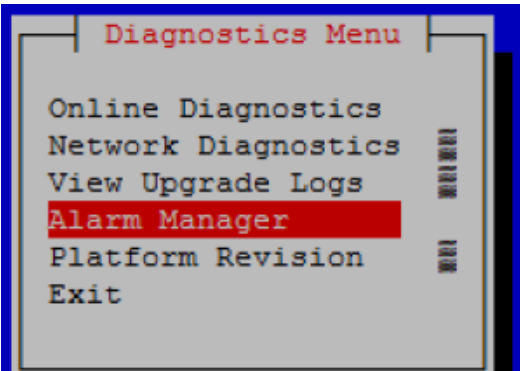
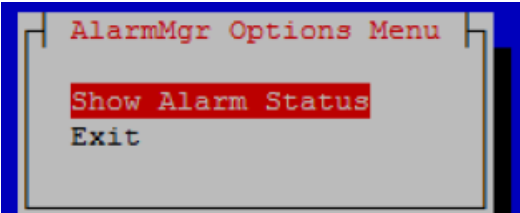
**Procedure 19. Restore TVOE Configuration from Backup Media**

10. <input type="checkbox"/>	<b>TVOE Server:</b> Wait for restart to successfully complete	<pre> 1401715649: Upstart Job TKLChpacucli: started #####  1401715649: Upstart Job alarmMgr: started #####  1401715649: Upstart Job tpdProvd: started #####  Oracle Linux Server release 6.5 Kernel 2.6.32-431.11.2.el6prere17.0.0.0_86.3.0.x86_64 on an x86_64  1401715649: Upstart Job syscheck: started #####  1401715650: Upstart Job TKLCsnmp-subagent: started #####  1401715651: Upstart Job ntdMgr: started #####  Oracle Linux Server release 6.5 Kernel 2.6.32-431.11.2.el6prere17.0.0.0_86.3.0.x86_64 on an x86_64  hostname71e968a495e6 login: █ </pre>
11. <input type="checkbox"/>	<b>TVOE Server:</b> Verify storage pools are active	<ol style="list-style-type: none"> <li>1. Login as <b>admusr</b>.</li> <li>2. Verify all storage pools are listed and are in the active state:</li> </ol> <pre> \$ sudo virsh -c "qemu:///system" pool-list  [admusr@5010441-TVOE ~]\$ sudo virsh -c "qemu:///system" pool-list Name                               State    Autostart ----- vsguests                           active   yes  [admusr@5010441-TVOE ~]\$ █ </pre> <p><b>Note:</b> If any storage pools are missing or inactive, contact My Oracle Support (MOS).</p>

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

12. <input type="checkbox"/>	<b>TVOE Server:</b> Enable HIDS (Optional)	<p><b>Note:</b> Enabling HIDS is optional. This step is skipped if HIDS is not required to be enabled.</p> <p>When enabling HIDS, update the baseline so the restored files are not reported as being tampered with. Execute these commands from the TVOE host remote console to enable HIDS and update the baseline:</p> <pre>\$ /usr/TKLC/plat/bin/hidsMgr -initialize LOG: HIDS monitoring has been Initialized HIDS baseline has been initialized \$ /usr/TKLC/plat/bin/hidsMgr --enable HIDS monitoring has successfully been enabled <b>New State: ENABLED</b> \$ /usr/TKLC/plat/bin/hidsMgr --update --all HIDS baseline has successfully been updated</pre>
---------------------------------	--	---

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


13.	<b>TVOE Server:</b> Verify alarms <input type="checkbox"/>	<ol style="list-style-type: none"><li>1. Verify alarms: <div data-bbox="505 289 898 340" style="border: 1px solid black; padding: 2px;"><code>\$ sudo su - platcfg</code></div></li><li>2. Click <b>Diagnostics</b>. The screenshot shows a 'Main Menu' with a list of options: Maintenance, Diagnostics (highlighted in red), Server Configuration, Remote Consoles, Network Configuration, Security, and Exit. A vertical bar on the right side of the menu indicates the current selection.</li><li>3. Click <b>Alarm Manager</b>. The screenshot shows a 'Diagnostics Menu' with a list of options: Online Diagnostics, Network Diagnostics, View Upgrade Logs, Alarm Manager (highlighted in red), Platform Revision, and Exit. A vertical bar on the right side of the menu indicates the current selection.</li><li>4. Click <b>Show Alarm Status</b>. The screenshot shows an 'AlarmMgr Options Menu' with a list of options: Show Alarm Status (highlighted in red) and Exit. A vertical bar on the right side of the menu indicates the current selection.</li></ol> <p>If there are any failures, contact My Oracle Support (MOS).</p>
-----	--	--

## Appendix H. Restore PMAC from Backup

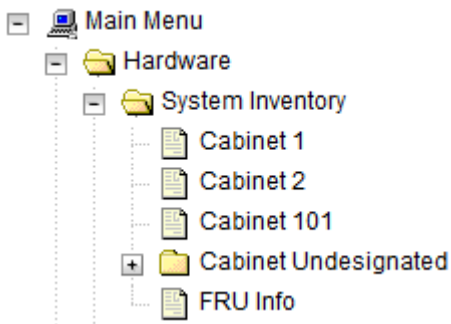
### Procedure 20. Restore PMAC from Backup Media

<b>S T E P #</b>	<p>This procedure provides steps to restore the PMAC application configuration from backup media.</p> <p><b>Prerequisite:</b> TVOE management server has been restored.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>	
1. <input type="checkbox"/>	Deploy the PMAC guest	Execute <b>Install PMAC</b> from reference [8].
2. <input type="checkbox"/>	<b>PMAC:</b> Login	Establish an SSH session to the PMAC server and login as <b>admusr</b> .
3. <input type="checkbox"/>	Restore PMAC Backup image to the PMAC host	<p>From the remote backup location, copy the backup file to the deployed PMAC. There are too many possible backup scenarios to cover them all here.</p> <p>This example is a simple scp from a redundant PMAC backup location. If using IPv6 addresses, the command requires shell escapes, for example,</p> <pre>admusr@[&lt;ipV6addr&gt;]:/&lt;file&gt;</pre> <p><b>Note:</b> Execute the scp command from the recovered PMAC and the backup file is pulled/retrieved from the backup location.</p> <div data-bbox="483 957 1425 1066" style="border: 1px solid black; padding: 5px;"> <pre>\$ sudo /usr/bin/scp -p \ admsur@&lt;remoteserver&gt;:/var/TKLC/smac/backup/*.pef \ /var/TKLC/smac/backup/</pre> </div> <p><b>Note:</b> It is important to copy the correct backup file to use in the restore. The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PMAC before the restoration of the data.</p>
4. <input type="checkbox"/>	<b>PMAC:</b> Verify no Alarms are present	<p>Verify no alarms are present.</p> <div data-bbox="483 1297 1425 1352" style="border: 1px solid black; padding: 5px;"> <pre>\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre> </div>
5. <input type="checkbox"/>	Restore the PMAC Data from Backup	<p>1. Restore the PMAC data from backup.</p> <div data-bbox="483 1415 1425 1499" style="border: 1px solid black; padding: 5px;"> <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm restore PM&amp;C Restore been successfully initiated as task ID 1</pre> </div> <p>2. Check the status of the background task.</p> <div data-bbox="483 1554 1425 1608" style="border: 1px solid black; padding: 5px;"> <pre>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</pre> </div> <p><b>Note:</b> The result eventually displays PMAC Restore successful.</p>

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

6. <input type="checkbox"/>	<b>PMAC GUI:</b> Login	<ol style="list-style-type: none"> <li>1. Open web browser and navigate to the PMAC GUI.</li> <li>2. Login as <b>PMACadmin</b> user:  <div data-bbox="483 338 1040 386" style="border: 1px solid black; padding: 2px; margin: 5px 0;">           https://&lt;pmac_network_ip&gt;         </div>  </li> </ol>
7. <input type="checkbox"/>	<b>PMAC GUI:</b> Verify restore task completed	<ol style="list-style-type: none"> <li>1. Navigate to <b>Task Monitoring</b>.</li> <li>2. Verify the restore background task completed successfully.</li> </ol> <p><b>Note:</b> After the restore is complete, you should see <b>Add Enclosure</b> tasks start for all previously provisioning servers. These should be allowed to complete before continuing.</p> <p><b>Note:</b> After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior. ISO images are added in the next step.</p>

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

8. <input type="checkbox"/>	<b>PMAC GUI:</b> Verify system inventory	1. Navigate to <b>Hardware &gt; System Inventory</b> .  2. Verify previously provisioned enclosures are present.
9. <input type="checkbox"/>	<b>PMAC:</b> Verify PMAC	Perform a system health check on the PMAC. <pre>\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre> This command should return no output on a healthy system. <pre>\$ sudo /usr/TKLC/smac/bin/sentry status</pre> All processes should be running, displaying output similar to the following: PM&C Sentry Status ----- sentryd started: Mon Jul 23 17:50:49 2012 Current activity mode: ACTIVE Process PID Status StartTS NumR ----- smacTalk 9039 running Tue Jul 24 12:50:29 2012 2 smacMon 9094 running Tue Jul 24 12:50:29 2012 2 hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2 snmpEventHandler 9176 running Tue Jul 24 12:50:29 2012 2 Fri Aug 3 13:16:35 2012 Command Complete.
10. <input type="checkbox"/>	<b>PMAC:</b> Add ISO images to the PMAC	Re-add any needed ISO images to the PMAC by executing procedure <b>Load DSR, SDS (Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only), and TPD ISOs to the PMAC Server</b> from reference [8] for all required ISO images.

**Procedure 21. Restore PMAC from Backup Server**

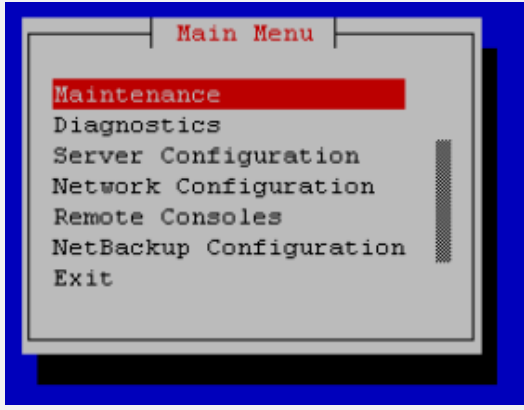
STEP #	<p>This procedure provides steps to restore the PMAC application configuration from backup server.</p> <p><b>Prerequisite:</b> TVOE management server has been restored.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>	
1. <input type="checkbox"/>	Deploy the PMAC guest	<p>Execute <b>Install PMAC</b> from reference [8].</p> <p><b>Note:</b> This procedure is for restoring from a NetBackup server, so specify the appropriate options when deploying PMAC for use with NetBackup.</p>
2. <input type="checkbox"/>	<b>PMAC TVOE Host:</b> Login	Establish an SSH session to the PMAC TVOE Host, login as <b>admusr</b> .
3. <input type="checkbox"/>	<b>PMAC TVOE Host:</b> Log into PMAC guest console	<p>1. On the TVOE host, execute this command:</p> <pre>\$sudo virsh list</pre> <p>This produces a listing of currently running virtual machines.</p> <pre>[admusr@Oahu-TVOE-1 ~]\$ sudo virsh list Id      Name                               State ----- 1       Oahu-PMAC                         running</pre> <p>2. Find the VM name for your PMAC and note its ID number in the first column.</p>
4. <input type="checkbox"/>	Connect to console of the VM using the VM number obtained in step 3	<p>On the TVOE host, execute this command:</p> <pre>\$sudo virsh console &lt;PMAC-VMID&gt;</pre> <p>Where PMAC-VMID is the VM ID you obtained in step 3:</p> <pre>[admusr@Oahu-TVOE-1 ~]\$ sudo virsh console 1 Connected to domain Oahu-PMAC Escape character is ^]  Oracle Linux Server release 6.7 Kernel 2.6.32-573.3.1.el6prere17.0.3.0.0_86.37.0.x86_64 on an x86_64  Oahu-PMAC login: █</pre> <p>You are now connected to the PMAC guest console.</p> <p>If you wish to return to the TVOE host, you can exit the session by pressing <b>CTRL + ]</b>.</p>



**Procedure 21. Restore PMAC from Backup Server**

5. <input type="checkbox"/>	<b>PMAC:</b> Prepare PMAC guest to transfer the appropriate backup from backup server. Disable iptables, and enable the TPD platcfg backup configuration menus	<p>Execute these commands on the PMAC.</p> <pre> \$ sudo /sbin/service iptables stop iptables: Flushing firewall rules: [ OK ] iptables: Setting chains to policy ACCEPT: filter [ OK ] \$ sudo /usr/TKLC/smac/etc/services/netbackup start Modified menu NBConfig -- show Set the following menus: NBConfig to visible=1 Modified menu NBInit -- show Set the following menus: NBInit to visible=1 Modified menu NBDeInit -- show Set the following menus: NBDeInit to visible=1 Modified menu NBInstall -- show Set the following menus: NBInstall to visible=1 Modified menu NBVerifyEnv -- show Set the following menus: NBVerifyEnv to visible=1 Modified menu NBVerify -- show Set the following menus: NBVerify to visible=1= </pre>
-----------------------------	--	---


**Procedure 21. Restore PMAC from Backup Server**

6.	<b>PMAC:</b> Verify the TPD platcfg backup menus are visible, then exit the TPD platcfg Utility	<p>Verify the TPD platcfg backup menus are visible.</p> <pre>\$ sudo /bin/su - platcfg</pre>  <p><b>Note:</b> In the example image above of the TPD platcfg utility Main Menu the backup menu is identified as <b>NetBackup Configuration</b>.</p>
7.	<b>PMAC:</b> Verify the iptables rules are disabled on the PMAC guest	<p>Verify the iptables rules are disabled on the PMAC guest.</p> <pre>\$ sudo /sbin/iptables -nL INPUT (policy ACCEPT) target prot opt source destination Chain FORWARD (policy ACCEPT) target prot opt source destination Chain OUTPUT (policy ACCEPT) target prot opt source destination</pre>
8.	<b>PMAC:</b> Install backup utility client software on the PMAC guest	<p>Execute <b>PMAC NetBackup Client Installation and Configuration</b> from reference [8] starting at step 4.</p> <p><b>Note:</b> The <b>Initialize PMAC Application</b> and <b>Configure PMAC Application</b> prerequisites can be ignored.</p>
9.	Backup server: verify appropriate PMAC backup exists	<p>This step is likely executed by customer IT personnel.</p> <ol style="list-style-type: none"> <li>1. Log into the backup server as the appropriate user using the user password.</li> <li>2. Execute the appropriate commands to verify the PMAC backup exists for the desired date.</li> </ol> <p><b>Note:</b> The actions and commands required to verify the PMAC backups exist and the commands required to perform backup and restore on the backup server are the responsibility of the site customer.</p> <p><b>Note:</b> It is important to select the correct backup file to use in the restore. The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PMAC before the restoration of the data.</p>

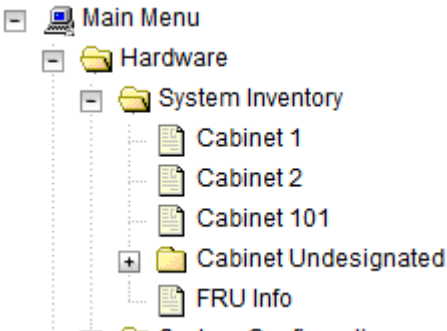
**Procedure 21. Restore PMAC from Backup Server**

10. <input type="checkbox"/>	<b>Backup Server:</b> Verify appropriate PMAC backup exists	<p>This step is likely executed by customer IT personnel.</p> <ol style="list-style-type: none"> <li>1. Log into the backup server as the appropriate user using the user password.</li> <li>2. Execute the appropriate commands to verify the PMAC backup exists for the desired date.</li> <li>3. Execute the appropriate commands to restore the PMAC management server backup for the desired date.</li> </ol> <p><b>Note:</b> The actions, and commands, required to verify the PMAC backups exist, and the commands required to perform backup and restore on the backup server are the responsibility of the site customer.</p>
11. <input type="checkbox"/>	<b>PMAC:</b> Verify no alarms are present	<p>Verify no alarms are present.</p> <pre>\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre>
12. <input type="checkbox"/>	Restore the PMAC data from backup	<ol style="list-style-type: none"> <li>1. Restore the PMAC data from backup. <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm restore</pre> <p>PM&amp;C Restore been successfully initiated as task ID 1</p> </li> <li>2. Check the status of the background task: <pre>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</pre> </li> </ol> <p><b>Note:</b> The result eventually displays PMAC Restore successful.</p>

**Procedure 21. Restore PMAC from Backup Server**

13. <input type="checkbox"/>	<b>PMAC GUI:</b> Login	<ol style="list-style-type: none"> <li>1. Open web browser and navigate to the PMAC GUI.  <div data-bbox="505 291 1065 340" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> https://&lt;pmac_network_ip&gt; </div> </li> <li>2. Login as <b>PMACadmin</b> user:</li> </ol> <div data-bbox="505 407 1432 1142" style="text-align: center;">  <p>The screenshot shows the Oracle System Login page. At the top is the Oracle logo in red. Below it is the text 'Oracle System Login' and a timestamp 'Tue Jun 7 13:49:06 2016 EDT'. In the center is a 'Log In' box with the text 'Enter your username and password to log in'. Inside this box are fields for 'Username:' and 'Password:', a 'Change password' link, and a 'Log In' button. Below the box is a warning: 'Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.' At the bottom is a copyright notice: 'Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.'</p> </div>
14. <input type="checkbox"/>	<b>PMAC GUI:</b> Verify restore task completed	<ol style="list-style-type: none"> <li>1. Navigate to <b>Task Monitoring</b>.</li> <li>2. Verify the restore background task completed successfully.</li> </ol> <p><b>Note:</b> After the restore is complete, you should see <b>Add Enclosure</b> tasks start for all previously provisioning servers. These should be allowed to complete before continuing.</p> <p><b>Note:</b> After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior. ISO images are added in the next step.</p>

**Procedure 21. Restore PMAC from Backup Server**

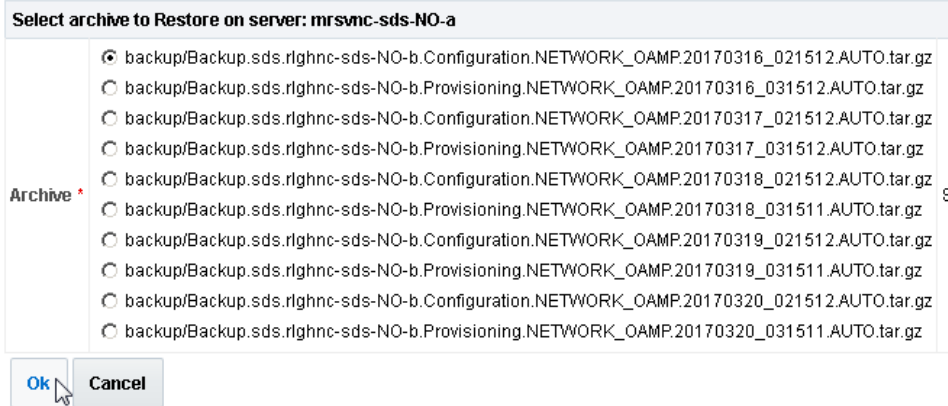

15. <input type="checkbox"/>	<b>PMAC GUI:</b> Verify system inventory	1. Navigate to <b>Hardware &gt; System Inventory</b> .  2. Verify previously provisioned enclosures are present
16. <input type="checkbox"/>	<b>PMAC:</b> Verify PMAC	Perform a system health check on the PMAC. <pre>\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre> This command should return no output on a healthy system. <pre>\$ sudo /usr/TKLC/smac/bin/sentry status</pre> All processes should be running, displaying output similar to the following: PM&C Sentry Status ----- sentryd started: Mon Jul 23 17:50:49 2012 Current activity mode: ACTIVE Process PID Status StartTS NumR ----- smacTalk 9039 running Tue Jul 24 12:50:29 2012 2 smacMon 9094 running Tue Jul 24 12:50:29 2012 2 hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2 snmpEventHandler 9176 running Tue Jul 24 12:50:29 2012 2 Fri Aug 3 13:16:35 2012 Command Complete.
17. <input type="checkbox"/>	<b>PMAC:</b> Add ISO images to the PMAC	Re-add any needed ISO images to the PMAC by executing procedure <b>Load Application and TPD ISO onto PMAC Server</b> from reference [8].

## Appendix I. Restore Provisioning Database

### Procedure 22. Restore Provisioning Database

<div>S T E P #</div>	<div>This procedure restores the SDS provisioning database.</div> <div>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</div> <div>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</div>																																																																																																			
<div>1. <input type="checkbox"/></div>	<div>Primary SDS NOAM GUI: Log into the primary SDS NOAM GUI</div> <div>Log into primary SDS NOAM GUI using its static IP (not the VIP).</div>																																																																																																			
<div>2. <input type="checkbox"/></div>	<div>Primary SDS NOAM GUI: Place the newly recovered standby NOAM into forced standby</div> <div><div>1. Navigate to <b>Status &amp; Manage &gt; HA</b>.</div><div>2. Click <b>Edit</b>.</div><div>3. Move the newly recovered standby server to forced <b>Standby</b>.</div></div> <div><div>Main Menu: Status &amp; Manage -&gt; HA [Edit]</div><div></div><div>Modifying HA attributes</div><table><thead><tr><th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr></thead><tbody><tr><td>rlghnc-sds-NO-a</td><td>Active</td><td>The maximum desired HA Role for rlghnc-sds-NO-a</td></tr><tr><td>rlghnc-sds-NO-b</td><td>Standby</td><td>The maximum desired HA Role for rlghnc-sds-NO-b</td></tr><tr><td>rlghnc-sds-QS</td><td>Observer</td><td>The maximum desired HA Role for rlghnc-sds-QS</td></tr></tbody></table></div>	Hostname	Max Allowed HA Role	Description	rlghnc-sds-NO-a	Active	The maximum desired HA Role for rlghnc-sds-NO-a	rlghnc-sds-NO-b	Standby	The maximum desired HA Role for rlghnc-sds-NO-b	rlghnc-sds-QS	Observer	The maximum desired HA Role for rlghnc-sds-QS																																																																																							
Hostname	Max Allowed HA Role	Description																																																																																																		
rlghnc-sds-NO-a	Active	The maximum desired HA Role for rlghnc-sds-NO-a																																																																																																		
rlghnc-sds-NO-b	Standby	The maximum desired HA Role for rlghnc-sds-NO-b																																																																																																		
rlghnc-sds-QS	Observer	The maximum desired HA Role for rlghnc-sds-QS																																																																																																		
<div>3. <input type="checkbox"/></div>	<div>Primary SDS NOAM GUI: Restore provisioning data</div> <div><div>1. Navigate to <b>Status &amp; Manage &gt; Database</b>.</div><div>2. Select the active NOAM and click <b>Restore</b>.</div></div> <div><div>Main Menu: Status &amp; Manage -&gt; Database</div><div>Mon Mar 20 16:38:03 2017 UTC</div><div><div>Filter* Info* Tasks</div><table><thead><tr><th>Network Element</th><th>Server</th><th>Role</th><th>OAM Max HA Role</th><th>Application Max HA Role</th><th>Status</th><th>DB Level</th><th>OAM Repl Status</th><th>SIG Repl Status</th><th>Repl Status</th><th>Repl Audit Status</th></tr></thead><tbody><tr><td>NO_RLGHNC</td><td>rlghnc-sds-NO-b</td><td>Network OAM&amp;P</td><td>Active</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>NO_MRSVNC</td><td>mrsync-sds-NO-b</td><td>Network OAM&amp;P</td><td>Active</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>SDS_SO_Nassau</td><td>nassau-dp-2</td><td>MP</td><td>Active</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>Normal</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>SDS_SO_Turks</td><td>turks-dp-2</td><td>MP</td><td>Active</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>Normal</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>SDS_SO_Turks</td><td>turks-sds-so-b</td><td>System OAM</td><td>Standby</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>SDS_SO_Nassau</td><td>nassau-sds-so-b</td><td>System OAM</td><td>Active</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>NO_RLOHNC</td><td>rlghnc-sds-NO-a</td><td>Network OAM&amp;P</td><td>Standby</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>SDS_SO_Fresno</td><td>fresno-dp-2</td><td>MP</td><td>Active</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>Normal</td><td>Allowed</td><td>NotApplicable</td></tr></tbody></table><div><div>Disable Provisioning</div><div>Report</div><div>Inhibit/Allow Replication</div><div>Backup...</div><div>Compare...</div><div>Restore</div><div>Man Audit</div><div>Resume Auto Audit</div></div></div></div>	Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status	NO_RLGHNC	rlghnc-sds-NO-b	Network OAM&P	Active	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable	NO_MRSVNC	mrsync-sds-NO-b	Network OAM&P	Active	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable	SDS_SO_Nassau	nassau-dp-2	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplicable	SDS_SO_Turks	turks-dp-2	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplicable	SDS_SO_Turks	turks-sds-so-b	System OAM	Standby	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable	SDS_SO_Nassau	nassau-sds-so-b	System OAM	Active	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable	NO_RLOHNC	rlghnc-sds-NO-a	Network OAM&P	Standby	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable	SDS_SO_Fresno	fresno-dp-2	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplicable
Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status																																																																																										
NO_RLGHNC	rlghnc-sds-NO-b	Network OAM&P	Active	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable																																																																																										
NO_MRSVNC	mrsync-sds-NO-b	Network OAM&P	Active	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable																																																																																										
SDS_SO_Nassau	nassau-dp-2	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplicable																																																																																										
SDS_SO_Turks	turks-dp-2	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplicable																																																																																										
SDS_SO_Turks	turks-sds-so-b	System OAM	Standby	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable																																																																																										
SDS_SO_Nassau	nassau-sds-so-b	System OAM	Active	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable																																																																																										
NO_RLOHNC	rlghnc-sds-NO-a	Network OAM&P	Standby	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable																																																																																										
SDS_SO_Fresno	fresno-dp-2	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplicable																																																																																										

**Procedure 22. Restore Provisioning Database**

		<p>3. Select the <b>Provisioning backup</b> file from the list (which was previously placed in the <code>/var/TKLC/db/filemgmt/backup</code> directory in step 5 of section 2.6.2) and click <b>OK</b>.</p> <p><b>Note:</b> You must use a <b>provisioning only</b> backup file. Combined backup files contain configuration and provisioning data and cause catastrophic issues, which could lead to a complete re-installation.</p> <p><b>Main Menu: Status &amp; Manage -&gt; Database [Restore]</b></p>  <p>4. Verify compatibility and click <b>OK</b> to restore.</p> <p><b>Main Menu: Status &amp; Manage -&gt; Database [Restoreconfirm]</b></p> 
<p>4. <input type="checkbox"/></p>	<p><b>Primary SDS NOAM GUI:</b> Wait for the restore to begin and track progress until the restore is complete</p>	<p>1. Wait 60 seconds for the restore to begin.</p> <p>2. Monitor the Info tab under the <b>Status &amp; Manage &gt; Database</b> screen and look for the following message:</p> <p>Restore on &lt;Active_NO_hostname&gt; status MAINT_IN_PROGRESS.</p> <p>3. Wait for the restore to complete by looking for the following message:</p> <p>Success: - Restore on rlghnc-sds-NO-b status MAINT_CMD_SUCCESS. Success</p> <p><b>Note:</b> Refresh the Info tab manually to see updated status by navigating to <b>Status &amp; Manage &gt; Database</b> again and selecting the Info tab.</p>

**Procedure 22. Restore Provisioning Database**

5. <input type="checkbox"/>	Primary SDS NOAM GUI: Uninhibit servers	<p>Uninhibit all servers in the following staggered arrangement:</p> <ol style="list-style-type: none"><li>Uninhibit active NOAM.  Refresh/monitor the <b>Status &amp; Manage &gt; Database</b> screen until a valid <b>DB Level</b> displays for the active NOAM.</li><li>Uninhibit <b>standby</b> NOAM/Query server.  Refresh/monitor the <b>Status &amp; Manage &gt; Database</b> screen until a valid <b>DB Level</b> displays for the standby NOAM/Query server.</li><li>Uninhibit <b>active</b> SOAMs.  Refresh/monitor the <b>Status &amp; Manage &gt; Database</b> screen until a valid <b>DB Level</b> displays for the active SOAMs.</li><li>Uninhibit <b>standby</b> SOAMs/DPs.  Refresh/monitor the <b>Status &amp; Manage &gt; Database</b> screen until a valid <b>DB Level</b> displays for the standby SOAMs/DPs.</li></ol>																																																																																																			
6. <input type="checkbox"/>	Recover Pdbrelay (if needed)	Verify whether PDB Relay is <b>Enabled</b> by following the instructions in Appendix J Recover PDB Relay.																																																																																																			
7. <input type="checkbox"/>	Primary SDS NOAM GUI: Enable provisioning	<p>Navigate to <b>Status &amp; Manage &gt; Database</b> and click <b>Enable Provisioning</b>.</p> <p>Main Menu: Status &amp; Manage -&gt; Database</p> <div><div>Filter* Info* Tasks</div><div>Mon Mar 20 17:09:34 2017 UTC</div></div> <table><thead><tr><th>Network Element</th><th>Server</th><th>Role</th><th>OAM Max HA Role</th><th>Application Max HA Role</th><th>Status</th><th>DB Level</th><th>OAM Repl Status</th><th>SIG Repl Status</th><th>Repl Status</th><th>Repl Audit Status</th></tr></thead><tbody><tr><td>SDS_SO_Turks</td><td>turks-sds-so-a</td><td>System OAM</td><td>Active</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>NO_RLGHNC</td><td>righnc-sds-NO-b</td><td>Network OAM&amp;P</td><td>Active</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>NO_MRSVNC</td><td>mrsvnc-sds-NO-b</td><td>Network OAM&amp;P</td><td>Active</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>SDS_SO_Nassau</td><td>nassau-dp-2</td><td>MP</td><td>Active</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>Normal</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>SDS_SO_Turks</td><td>turks-dp-2</td><td>MP</td><td>Active</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>Normal</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>SDS_SO_Turks</td><td>turks-sds-so-b</td><td>System OAM</td><td>Standby</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>SDS_SO_Nassau</td><td>nassau-sds-so-b</td><td>System OAM</td><td>Active</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr><tr><td>NO_RLGHNC</td><td>righnc-sds-NO-a</td><td>Network OAM&amp;P</td><td>Standby</td><td>N/A</td><td>Normal</td><td>7261273</td><td>Normal</td><td>NotApplicable</td><td>Allowed</td><td>NotApplicable</td></tr></tbody></table> <div><div>Enable Provisioning</div><div>Report</div><div>Inhibit/Allow Replication</div><div>Backup...</div><div>Compare...</div><div>Restore...</div><div>Man Audit</div><div>Resume Auto Audit</div></div>	Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status	SDS_SO_Turks	turks-sds-so-a	System OAM	Active	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable	NO_RLGHNC	righnc-sds-NO-b	Network OAM&P	Active	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable	NO_MRSVNC	mrsvnc-sds-NO-b	Network OAM&P	Active	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable	SDS_SO_Nassau	nassau-dp-2	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplicable	SDS_SO_Turks	turks-dp-2	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplicable	SDS_SO_Turks	turks-sds-so-b	System OAM	Standby	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable	SDS_SO_Nassau	nassau-sds-so-b	System OAM	Active	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable	NO_RLGHNC	righnc-sds-NO-a	Network OAM&P	Standby	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable
Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status																																																																																											
SDS_SO_Turks	turks-sds-so-a	System OAM	Active	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable																																																																																											
NO_RLGHNC	righnc-sds-NO-b	Network OAM&P	Active	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable																																																																																											
NO_MRSVNC	mrsvnc-sds-NO-b	Network OAM&P	Active	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable																																																																																											
SDS_SO_Nassau	nassau-dp-2	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplicable																																																																																											
SDS_SO_Turks	turks-dp-2	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplicable																																																																																											
SDS_SO_Turks	turks-sds-so-b	System OAM	Standby	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable																																																																																											
SDS_SO_Nassau	nassau-sds-so-b	System OAM	Active	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable																																																																																											
NO_RLGHNC	righnc-sds-NO-a	Network OAM&P	Standby	N/A	Normal	7261273	Normal	NotApplicable	Allowed	NotApplicable																																																																																											

Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.



**Procedure 22. Restore Provisioning Database**

8. <input type="checkbox"/>	<b>Primary SDS NOAM GUI:</b> Remove NO from forced standby	<ol style="list-style-type: none"><li>1. Navigate to <b>Status &amp; Manage &gt; HA</b> and click <b>Edit</b>.</li><li>2. Select the server, which was moved to forced standby in step 2, change <b>Max HA Role</b> to <b>Active</b>, and click <b>OK</b>.</li></ol> <p><b>Main Menu: Status &amp; Manage -&gt; HA [Edit]</b></p> <hr/> <p>Modifying HA attributes</p> <table><thead><tr><th>Hostname</th><th>Max Allowed HA Role</th><th>Description</th></tr></thead><tbody><tr><td>rlghnc-sds-NO-a</td><td>Active</td><td>The maximum desired HA Role for rlghnc-sds-NO-a</td></tr><tr><td>rlghnc-sds-NO-b</td><td>Active</td><td>The maximum desired HA Role for rlghnc-sds-NO-b</td></tr><tr><td>rlghnc-sds-QS</td><td>Observer</td><td>The maximum desired HA Role for rlghnc-sds-QS</td></tr></tbody></table>	Hostname	Max Allowed HA Role	Description	rlghnc-sds-NO-a	Active	The maximum desired HA Role for rlghnc-sds-NO-a	rlghnc-sds-NO-b	Active	The maximum desired HA Role for rlghnc-sds-NO-b	rlghnc-sds-QS	Observer	The maximum desired HA Role for rlghnc-sds-QS
Hostname	Max Allowed HA Role	Description												
rlghnc-sds-NO-a	Active	The maximum desired HA Role for rlghnc-sds-NO-a												
rlghnc-sds-NO-b	Active	The maximum desired HA Role for rlghnc-sds-NO-b												
rlghnc-sds-QS	Observer	The maximum desired HA Role for rlghnc-sds-QS												


## Appendix J. Recover PDB Relay

### Procedure 23. Recover PDB Relay

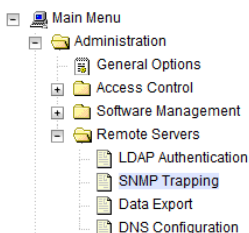
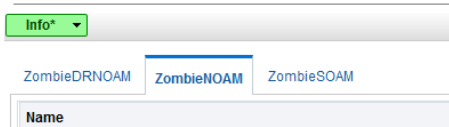
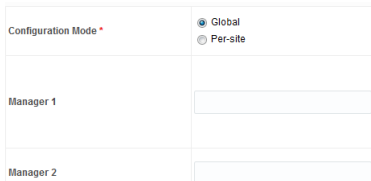
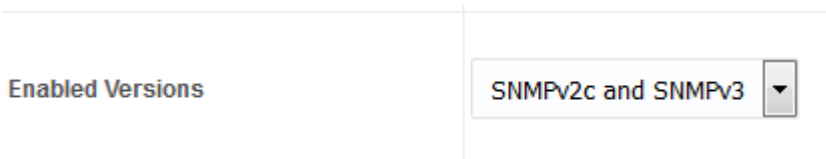
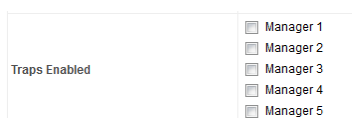

S T E P #		<p>This procedure re-establishes the PDB relay connection.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>
1. <input type="checkbox"/>	<b>NOAM VIP console:</b> Determine if pdbrelay is enabled	<p>Execute following command on console of Active NOAM server (accessed via the VIP) and compare the output:</p> <pre>\$ iqt -zhp -fvalue ProvOptions where "var='pdbRelayEnabled'" TRUE</pre> <p>Proceed to next step only if the result of above command is <b>true</b>.</p>
2. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Disable pdbrelay	<p>Unmark the <b>PDB Relay Enabled</b> checkbox on the <b>SDS &gt; Configuration &gt; Options</b> screen and click <b>Apply</b>.</p>
3. <input type="checkbox"/>	<b>NOAM VIP Console:</b> Emergency restart (start from beginning of Cmd log)	<p>Execute following command on console:</p> <pre>\$ iset -fvalue=0 ProvOptions where "var='pdbRelayMsgLogTimeStamp'"</pre>
4. <input type="checkbox"/>	<b>NOAM VIP GUI:</b> Enable pdbrelay	<p>Mark the <b>PDB Relay Enabled</b> checkbox on the <b>SDS &gt; Configuration &gt; Options</b> screen and click <b>Apply</b>.</p>

## Appendix K. SNMP Configuration

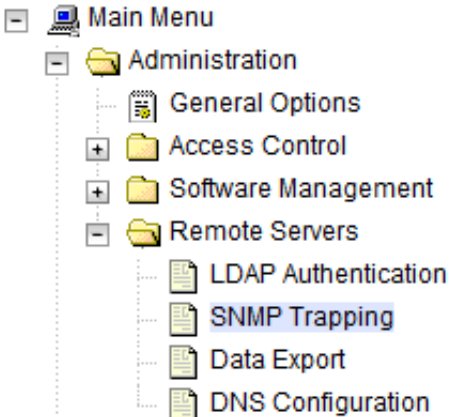

### Procedure 24. Configure SNMP

S T E P #	<p>This workaround configures SNMP with SNMPv2c and SNMPv3 as the enabled versions for SNMP traps configuration since PMAC does not support SNMPv3.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</p>
<p>1.</p> <p><input type="checkbox"/></p> <p>(Workaround)</p> <p><b>NOAM VIP</b></p> <p><b>GUI: Login</b></p>	<p><b>Note:</b> This workaround step should be performed only in the following cases:</p> <ol style="list-style-type: none"> <li>1. <b>If SNMP is not configured.</b></li> <li>2. <b>If SNMP is already configured and SNMPv3 is selected as enabled version.</b></li> </ol> <p><b>Note:</b> This is a workaround step to configure SNMP with 'SNMPv2c and SNMPv3' as the enabled versions for SNMP Traps configuration, since PMAC does not support SNMPv3.</p> <ol style="list-style-type: none"> <li>1. If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server.</li> <li>2. Open the web browser and enter a URL of: <div data-bbox="505 911 1308 959" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> http://&lt;Primary_NOAM_VIP_IP_Address&gt; </div> </li> <li>3. Log into the NOAM GUI as the <b>guiadmin</b> user:</li> </ol> <div data-bbox="467 1026 1414 1780" style="text-align: center; margin-top: 20px;">  <p><b>Oracle System Login</b></p> <hr/> <p style="text-align: right;">Tue Jun 7 13:49:06 2016 EDT</p> <div data-bbox="641 1241 1242 1608" style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 300px;"> <p><b>Log In</b></p> <p>Enter your username and password to log in</p> <p>Username: <input style="width: 100px;" type="text"/></p> <p>Password: <input style="width: 100px;" type="password"/></p> <p><input type="checkbox"/> Change password</p> <p><input type="button" value="Log In"/></p> </div> <p style="font-size: small;">Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.</p> <hr/> <p style="font-size: x-small;">Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</p> <p style="font-size: x-small;">Copyright © 2010, 2016, <a href="#">Oracle</a> and/or its affiliates. All rights reserved.</p> </div>

**Procedure 24. Configure SNMP**

<p>2. <input type="checkbox"/></p>	<p><b>NOAM VIP GUI:</b> Configure system-wide SNMP trap receiver(s)</p>	<ol style="list-style-type: none"> <li>Navigate to <b>Administration &gt; Remote Servers &gt; SNMP Trapping</b>.   </li> <li>Select the Server Group tab for SNMP trap configuration:  <b>Main Menu: Administration -&gt; Remote Servers</b>   </li> <li>Type the <b>IP address</b> or <b>hostname</b> of the Network Management Station (NMS) where you want to forward traps. This IP should be reachable from the NOAMP's XMI network. If already configured SNMP with <b>SNMPv3</b> as enabled version, another server needs to be configured here.</li> <li>Continue to fill in additional secondary, tertiary, etc., <b>Manager IPs</b> in the corresponding slots if desired.  <b>SNMP Trap Configuration Insert for ZombieNOAM</b>   </li> <li>Set the Enabled Versions as <b>SNMPv2c and SNMPv3</b>.   </li> <li>Check <b>Traps Enabled</b> checkboxes for the Manager servers being configured.   </li> <li>Type the SNMP Community Name.   </li> <li>Leave all other fields at their default values.</li> <li>Click <b>OK</b>.</li> </ol>
------------------------------------	---	--

**Procedure 24. Configure SNMP**

3. <input type="checkbox"/>	<b>NOAMP VIP:</b> Enable traps from individual servers (optional)	<p><b>Note:</b> By default SNMP traps from MPs are aggregated and displayed at the active NOAMP. If, instead, you want every server to send its own traps directly to the NMS, then execute this procedure.</p> <p>This procedure requires all servers, including MPs, to have an XMI interface on which the customer SNMP target server (NMS) is reachable.</p> <ol style="list-style-type: none"> <li>1. Navigate to <b>Administration &gt; Remote Servers &gt; SNMP Trapping</b>.</li> </ol>  <ol style="list-style-type: none"> <li>2. Make sure the <b>Enabled</b> checkbox is marked.</li> </ol>  <ol style="list-style-type: none"> <li>3. Click <b>Apply</b> and verify the data is committed.</li> </ol>
4. <input type="checkbox"/>	<b>PMAC GUI:</b> Update the TVOE host SNMP community string	<ol style="list-style-type: none"> <li>1. Establish an SSH session to the PMAC.</li> <li>2. Login as <b>admusr</b> user:</li> <li>3. Update the TVOE hos community string with this command:</li> </ol> <pre>\$ sudo pmaccli setCommStr --accessType=rw --commStr=&lt;site specific value&gt;</pre> <p><b>Note:</b> When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest on the PMAC control network are updated. All those servers that match the existing Site Specific Community String are not updated again until the string name is changed.</p>

## Appendix L. Backup Directory

### Procedure 25. Backup Directory

S T E P #	This procedure checks and creates the backup directory. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.
1. <input type="checkbox"/>	<p><b>NOAM/SOAM VIP Console:</b> Determine if backup directory exists</p> <ol style="list-style-type: none"> <li>Execute this command an active NOAM/SOAM server console (accessed using the VIP) and compare the output. <div data-bbox="505 590 1443 674" style="border: 1px solid black; padding: 5px;"> <pre>\$ cd /var/TKLC/db/filemgmt/ \$ ls -ltr</pre> </div> </li> <li>Look for the backup directory in the output.</li> <li>Make sure the directory is already created with correct permission. The directory looks like this: <div data-bbox="505 810 1443 856" style="border: 1px solid black; padding: 5px;"> <pre>drwxrwx--- 2 awadmin awadm 4096 Dec 19 02:15 backup</pre> </div> </li> <li>If the directory is already there with correct permissions, then skip steps 2 and 3.</li> <li>If directory does not have the correct permissions, then go to step 3.</li> </ol>
2. <input type="checkbox"/>	<p><b>NOAM/SOAM VIP Console:</b> Create backup directory</p> <ol style="list-style-type: none"> <li>Go to the backup directory location. <div data-bbox="505 1056 1443 1102" style="border: 1px solid black; padding: 5px;"> <pre>cd /var/TKLC/db/filemgmt/</pre> </div> </li> <li>Create backup directory. <div data-bbox="505 1161 1443 1207" style="border: 1px solid black; padding: 5px;"> <pre>\$ mkdir backup</pre> </div> </li> <li>Verify directory has been created. <div data-bbox="505 1266 1443 1312" style="border: 1px solid black; padding: 5px;"> <pre>\$ ls -ltr /var/TKLC/db/filemgmt/backup</pre> </div> <p><b>Note:</b> A <b>No such file or directory</b> error message should not display. The directory should show as empty with the total as 0 for content.</p> </li> </ol>

**Procedure 25. Backup Directory**

3. <input type="checkbox"/>	<b>NOAM/SOAM VIP Console:</b> Change permissions of backup directory	<ol style="list-style-type: none"> <li>1. Verify directory has been created.  <pre>\$ ls -ltr /var/TKLC/db/filemgmt/backup</pre> <p><b>Note:</b> A <b>No such file or directory</b> error message should not display. The directory should show as empty with the total as 0 for content.</p> </li> <li>2. Change permissions for the backup directory.  <pre>\$ chmod 770 /var/TKLC/db/filemgmt/backup</pre> </li> <li>3. Change ownership of backup directory.  <pre>\$ sudo chown -R awadmin:awadm /var/TKLC/db/filemgmt/backup</pre> </li> <li>4. Directory displays as follows:  <pre>drwxrwx--- 2 awadmin awadm          4096 Dec 22 02:15 backup</pre> </li> </ol>
4. <input type="checkbox"/>	<b>NOAM/SOAM VIP Console:</b> Copy the backup file to the backup directory	<ol style="list-style-type: none"> <li>1. Copy the backup file to the backup directory.  <pre>\$ cp BACKUPFILE /var/TKLC/db/filemgmt/backup</pre> </li> <li>2. Change permissions of files in the backup directory.  <pre>\$ chmod 666 Backup.*</pre> </li> <li>3. Change ownership of files in the backup directory.  <pre>\$ sudo chown -R awadmin:awadm Backup.*</pre> </li> </ol>

## Appendix M. netConfig backupConfiguration/restoreConfiguration/upgradeFirmware with TPD cipher change

Beginning with TPD 7.7.0.0-88.68.0, the cipher list is restricted to allow only a limited number of ciphers for ssh access to the servers. As a result, netConfig backup and restore operations are not functional with Cisco switches (3020, 4948s), as these switches use other ciphers. Executing these commands with the restricted ciphers would fail as shown below:

```
[admusr@p5-pmac ~]$ /usr/bin/sudo /usr/TKLC/plat/bin/netConfig --
device=3020_ip backupConfiguration service=ssh_ip filename=backup
```

```
Command failed: backupConfiguration
```

```
Error saving to SSH service
```

```
[admusr@p5-pmac ~]$
```

To avoid this issue, while maintaining a focus on improved security, the following procedure must be executed before and after netConfig backup and restore operations.

### Procedure 26. Turn off cipher list before backupConfiguration/restoreConfiguration/upgradeFirmware command

STEP #	Procedure	Description
<p>This procedure prepares the PM&amp;C to avoid the cipher mismatch issue with Cisco switches. This is performed before the netConfig backup, restore or upgrade operations.</p> <p><i>Check off (✓) each step as it is completed.</i> Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>		
1 <input type="checkbox"/>	Turn off cipher list	<p>From the PMAC shell enter the following:</p> <pre>/usr/bin/sudo /bin/vi /etc/ssh/sshd_config</pre> <p>Add # in the beginning of the following three lines to comment them out, the result is:</p> <pre>#Ciphers aes256-ctr,aes192-ctr,aes128-ctr #MaxAuthTries 4 #LoginGraceTime 1m</pre>
2 <input type="checkbox"/>	Restart sshd	<pre>/usr/bin/sudo service sshd restart</pre>



STEP #	Procedure	Description
3 <input type="checkbox"/>	Run the netConfig backupConfiguration/restoreConfiguration/upgradeFirmware command	<p>For a backup operation:</p> <pre>[admusr@pmac ~]\$ /usr/bin/sudo /usr/TKLC/plat/bin/netConfig backupConfiguration --device=&lt;switch_name&gt; service=&lt;ssh_service&gt; filename=&lt;switch_name&gt;-backup</pre> <p>For a restore operation:</p> <pre>[admusr@pmac ~]\$ /usr/bin/sudo /usr/TKLC/plat/bin/netConfig restoreConfiguration --device=&lt;switch_name&gt; service=&lt;ssh_service&gt; filename=&lt;switch_name&gt;-backup</pre> <p>For a upgrade operation:</p> <pre>[admusr@pmac ~]\$ /usr/bin/sudo /usr/TKLC/plat/bin/netConfig upgradeFirmware --device=&lt;switch_name&gt; service=&lt;ssh_service&gt; filename=&lt;Cisco IOS&gt;</pre>

**Procedure 27. Resume cipher list after backupConfiguration/restoreConfiguration/upgradeFirmware command**

STEP #	Task	Description
<p>This procedure restores the PM&amp;C restricted cipher list after perform the netConfig backup, restore or upgrade operations.</p> <p><i>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</i></p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>		
1 <input type="checkbox"/>	Resume the cipher list	<p>From the PMAC shell enter the following:</p> <pre>/usr/bin/sudo /bin/vi /etc/ssh/sshd_config</pre> <p>Uncomment the three lines:</p> <pre>Ciphers aes256-ctr,aes192-ctr,aes128-ctr MaxAuthTries 4 LoginGraceTime 1m</pre>
2 <input type="checkbox"/>	Restart sshd	<pre>/usr/bin/sudo service sshd restart</pre>

## Appendix N. My Oracle Support (MOS)

### My Oracle Support

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

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

1. Select 2 for **New Service Request**.
2. Select 3 for **Hardware, Networking, and Solaris Operating System Support**.
3. Select one of the following options:
  - For technical issues such as creating a new Service Request (SR), select **1**.
  - For non-technical issues such as registration or assistance with MOS, select **2**.

You are connected to a live agent who can assist you with MOS registration and opening a support ticket. MOS is available 24 hours a day, 7 days a week, 365 days a year.

### Emergency Response

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

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

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

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

### Locate Product Documentation on the Oracle Help Center

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

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

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