

Oracle® Communications

Diameter Signaling Router

DSR C-Class Disaster Recovery User's Guide

Release 8.2

E88960-01

April 2018

ORACLE®

Oracle Communications DSR C-Class Disaster Recovery User's Guide, Release 8.2

Copyright © 2017, 2018 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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



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

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

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

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

See more information My Oracle Support (MOS).

Table of Contents

1. Introduction.....	6
1.1 References	6
1.2 Acronyms.....	6
1.3 Terminology.....	7
1.4 Optional Features	8
2. General Description	8
2.1 Complete Server Outage (All Servers).....	9
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	10
2.5 Partial Service Outage with Corrupt Database	10
3. Procedure Overview	10
3.1 Required Materials	10
3.2 Disaster Recovery Strategy.....	11
4. Disaster Recovery Procedure	13
4.1 Recovery Scenario 1 (Complete Server Outage).....	13
4.2 Recovery Scenario 2 (Partial Server Outage with One NOAM Server Intact and ALL SOAMs Failed).....	47
4.3 Recovery Scenario 3 (Partial Server Outage with All NOAM Servers Failed and One SOAM Server Intact)	73
4.4 Recovery Scenario 4 (Partial Server Outage with One NOAM Server and One SOAM Server Intact)	96
4.5 Recovery Scenario 5 (Both NOAM Servers Failed with DR-NOAM Available).....	116
4.6 Recovery Scenario 6 (Database Recovery)	124
4.6.1 Recovery Scenario 6: Case 1	124
4.6.2 Recovery Scenario 6: Case 2	130
5. Resolve User Credential Issues after Database Restore	135
5.1 Restore a Deleted User	135
5.2 Keep a Restored User	135
5.3 Remove a Restored User.....	137
5.4 Restore a Modified User.....	138
5.5 Restore an Archive that Does Not Contain a Current User	138
6. IDIH Disaster Recovery	143
Appendix A. DSR Database Backup	148
Appendix B. Recover/Replace Failed 3rd Party Components (Switches, OAs)	152
Appendix C. Inhibit A and B Level Replication on C-level Servers	157

Appendix D.	Un-Inhibit A and B Level Replication on C-level Servers	158
Appendix E.	Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost)	159
Appendix F.	Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost)	161
Appendix G.	Restore TVOE Configuration from Backup Media	162
Appendix H.	Restore PMAC from Backup	169
Appendix I.	Configure TVOE Hosts	178
Appendix J.	Create NOAM/SOAM Virtual Machines	188
Appendix K.	SNMP Configuration	196
Appendix L.	Backup Directory	200
Appendix M.	My Oracle Support (MOS)	201

List of Tables

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

List of Figures

Figure 1. Determining Recovery Scenario	12
---	----

List of Procedures

Procedure 1. Recovery Scenario 1	14
Procedure 2. Recovery Scenario 2	48
Procedure 3. Recovery Scenario 3	74
Procedure 4. Recovery Scenario 4	97
Procedure 5. Recovery Scenario 5	116
Procedure 6. Recovery Scenario 6 (Case 1)	125
Procedure 7. Recovery Scenario 6 (Case 2)	130
Procedure 8. Keep Restored User	135
Procedure 9. Remove the Restored User	137
Procedure 10. Restore an Archive That Does Not Contain a Current User.....	139
Procedure 11. IDIH Disaster Recovery Preparation	143
Procedure 12. IDIH Disaster Recovery (Re-Install Mediation and Application Servers)	145
Procedure 13. DSR Database Backup.....	148

Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F)	152
Procedure 15. Recover a Failed Enclosure Switch (Cisco 3020)	154
Procedure 16. Recover a Failed Enclosure Switch (HP 6120XG , HP 6125XLG, HP 6125G).....	154
Procedure 17. Recover a Failed Enclosure OA	157
Procedure 18. Inhibit A and B Level Replication on C-level Servers	157
Procedure 19. Un-Inhibit A and B Level Replication on C-level Servers	158
Procedure 20. Inhibit A and B Level Replication on C-level Servers	159
Procedure 21. Un-Inhibit A and B Level Replication on C-Level Servers	161
Procedure 22. Restore TVOE Configuration from Backup Media.....	162
Procedure 23. Restore PMAC from Backup Media.....	169
Procedure 24. Restore PMAC from Backup Server.....	172
Procedure 25. Configure TVOE	178
Procedure 26. Create NOAM Guest VMs	188
Procedure 27. Create SOAM Guest VMs	192
Procedure 28. Configure SNMP	196
Procedure 29. Backup Directory	200

1. Introduction

This document describes procedures used to execute disaster recovery for DSR. This includes recovery of partial or complete loss of one or more DSR servers. The audience for this document includes GPS groups such as software engineering, product verification, documentation, customer service, software operations, and first office application. This document can be executed by Oracle customers as long as Oracle Customer Service personnel are involved and/or consulted. Executing this procedure also involves referring to and executing procedures in existing support documents.

Note: Components dependent on DSR might need to be recovered as well, for example, SDS, IDIH, and PMAC.

1.1 References

- [1] TPD Initial Product Manufacture
- [2] Platform 7.2 Configuration Procedure Reference
- [3] CPA Feature Activation Procedure
- [4] DSR Mediation Feature Activation Procedure
- [5] DSR FABR Feature Activation Procedure
- [6] DSR RBAR Feature Activation Procedure
- [7] DSR MAP-Diameter IWF Feature Activation Procedure
- [8] DSR C-Class Software Installation and Configuration Procedure Part 2/2
- [9] DSR GLA Feature Activation Procedure
- [10] DSR C-Class Hardware and Software Installation
- [11] PMAC 6.2 Disaster Recovery Guide
- [12] SDS C-Class Disaster Recovery Guide
- [13] DSR PCA Activation Guide
- [14] DSR DTLS Feature Activation Procedure
- [15] DSR Security Guide
- [16] DCA Framework and Application Activation and Deactivation Guide
- [17] DSR/SDS 8.x 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
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
FRU	Field Replaceable Unit
HP c-Class	HP blade server offering

Acronym	Definition
iLO	Integrated Lights Out manager
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 (for example, TPD)
RMS	Rack Mounted Server
PMAC	Platform Management & Configuration
SAN	Storage Area Network
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtual Operating Environment
VM	Virtual Machine
VSP	Virtual Serial Port
IPFE	IP Front End
PCA	Policy and Charging Application
IDIH	Integrated Diameter Intelligence Hub
SDS	Subscriber Database Server

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.

Term	Definition
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 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
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"> All NOAM servers failed. All SOAM servers failed. MP servers may or may not have failed.
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"> At least 1 NOAM server is intact and available. All SOAM servers failed. MP servers may or may not have failed.
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"> All NOAM servers failed. At least 1 SOAM server out of active, standby, spare is intact and available. MP servers may or may not have failed.

Procedure	State of NOAM and/or SOAM server(s)
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"> At least 1 NOAM server is intact and available. At least 1 SOAM server out of active, standby, spare is intact and available. 1 or more MP servers have failed.
Recovery Scenario 5 (Both NOAM Servers Failed with DR-NOAM Available)	<ul style="list-style-type: none"> Both NOAM servers failed. DR NOAM is available SOAM servers may or may not be failed. MP servers may or may not be failed.
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"> Server is intact Database gets corrupted on the server Latest database backup of the corrupt server is present Replication is inhibited (either manually or because of Comcol upgrade barrier)
Section Recovery Scenario 6: Case 1	<ul style="list-style-type: none"> Server is intact Database gets corrupted on the server Replication is occurring to the server with corrupted database
Section Recovery Scenario 6: Case 2	<ul style="list-style-type: none"> Server is intact Database gets corrupted on the server Latest Database backup of the corrupt server is NOT present Replication is inhibited (either manually or because of Comcol upgrade barrier)

Note: For failed aggregation switches, OA, or 6120/6125/3020 switches, refer to Recover/Replace Failed 3rd Party Components (Switches, OAs).

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 at least one NOAM server is intact. All SOAM servers have failed and are recovered using base recovery of hardware and software. Database is restored on the SOAM server and replication recovers 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 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. Oracle Tekelec Platform Distribution (TPD) Media (64 bits).
6. Platform Management and Configuration (PMAC) ISO or SW.
7. DSR CD-ROM (or ISO image file on USB Flash) of the target release.
8. TVOE Platform Media (64 bits).
9. The XML configuration files used to configure the switches, available on the PMAC server (or PMAC backup).
10. The switch backup files taken after the switch is configured, available on the PMAC server (or PMAC backup).

11. The network element XML file used for the blades initial configuration.
12. The HP firmware upgrade pack (or customer-provided firmware).
13. NetBackup Files if they exist. This may require the assistance of the customer's NetBackup administrator.
14. PMAC and TVOE backups (if available).
15. Latest RADIUS shared secret encryption key file backup (DpiKf.bin.encr).
16. List of activated and enabled features.
17. IDIH CD-ROM (or ISO image file on USB Flash) of the target release (if IDIH is being recovered).

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.

Note: NOAMs are deployed using the fast deployment tool from the PMAC. In scenarios where both NOAMs are failed, this fast deployment file is used. In scenarios where only one NOAM is failed, the fast deployment file is NOT used.

SUDO

As a non-root user (**admusr**), many commands (when run as **admusr**) now require the use of **sudo**.

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 Required Materials.
4. From the failure conditions, determine the Recovery Scenario and procedure to follow (using Figure 1. Determining Recovery Scenario and Table 4. Recovery Scenarios).
5. Execute appropriate recovery procedures (listed in Table 4. Recovery Scenarios).

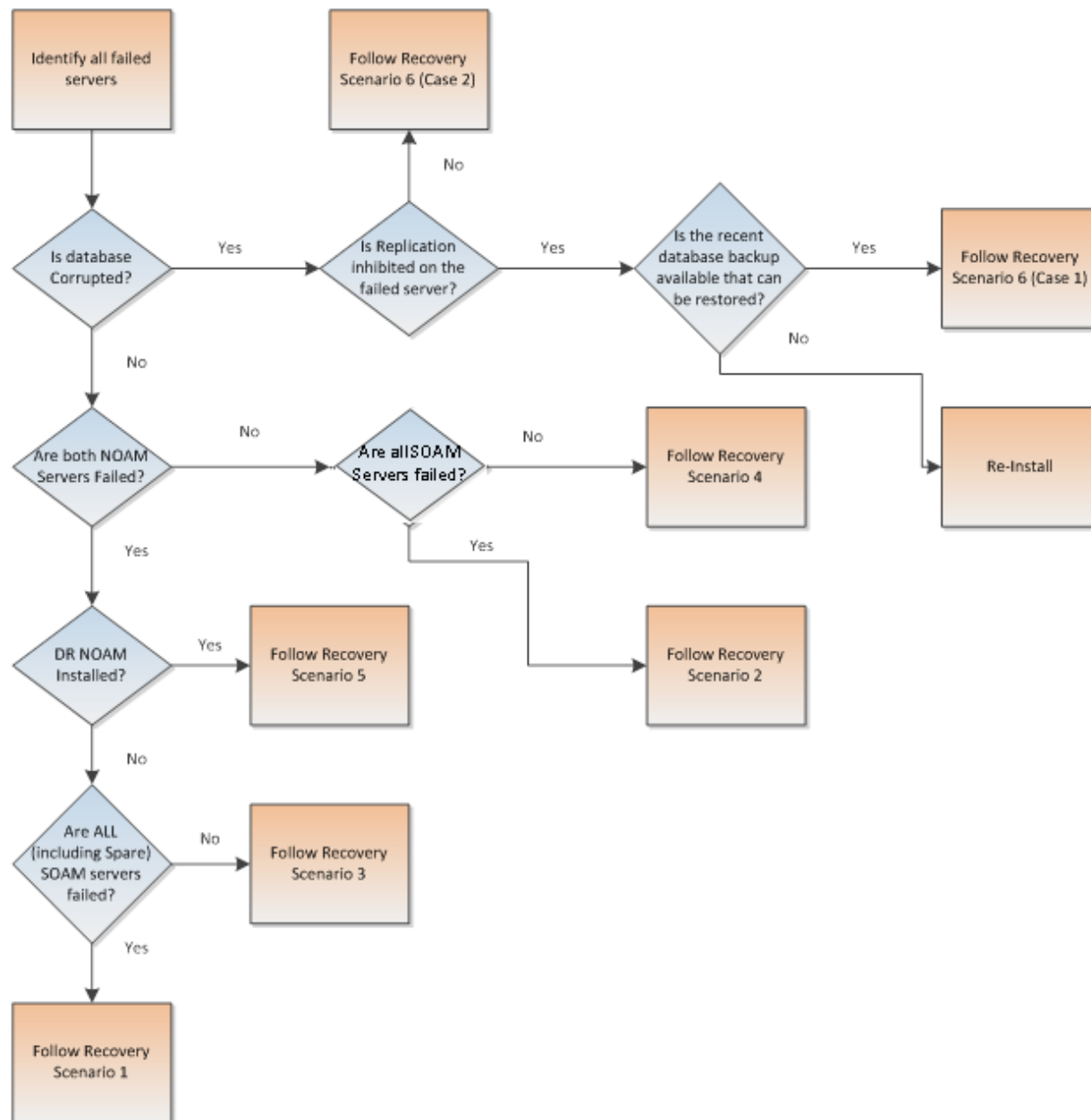


Figure 1. Determining Recovery Scenario

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.HPC02-NO2.FullIDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2

4.1 Recovery Scenario 1 (Complete Server Outage)

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

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 and blades
 - Recover the base hardware. (By replacing the hardware and executing hardware configuration procedures) — Reference [10] for the DSR base hardware installation procedure
- Recover the **NOAM** servers by recovering executing the fast deployment xml file
 - Recover the NOAM database
 - Reconfigure the DSR application
- Recover the **SOAM** servers by recovering base hardware/software and/or VM image

- Recover the SOAM database
- Reconfigure the DSR Application
- Recover all **MP servers** by recovering base hardware and software
 - Reconfigure the signaling interface and routes on the MPs. The DSR software automatically reconfigures the signaling interface from the recovered database
 - Reference [8] for the applicable DSR software installation/configuration guide if any existing routes need to be altered
- Restart process and re-enable provisioning replication

Note: Any other applications DR recovery actions (SDS and IDIH) may occur in parallel. These actions can/should be worked simultaneously; doing so would allow faster recovery of the complete solution, that is, stale DB on DP servers do not receive updates until SDS-SOAM servers are recovered. Section 6.6 for IDIH disaster recovery and [12] for SDS 7.2/7.3 disaster recovery.


Procedure 1. Recovery Scenario 1

S T E 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. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
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"/>	Recover PMAC and PMAC TVOE Host: Configure BIOS settings and update firmware	1. Configure and verify the BIOS settings by executing the Configure the RMS and Blade Server BIOS Settings procedure from reference [10]. 2. Verify and/or upgrade server firmware by executing the Upgrade Management Server Firmware procedure from reference [10]. Note: As indicated in [10], repeat for additional rack mount servers, if equipped.

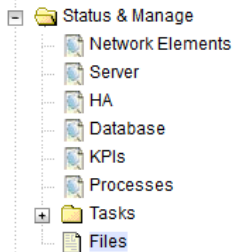
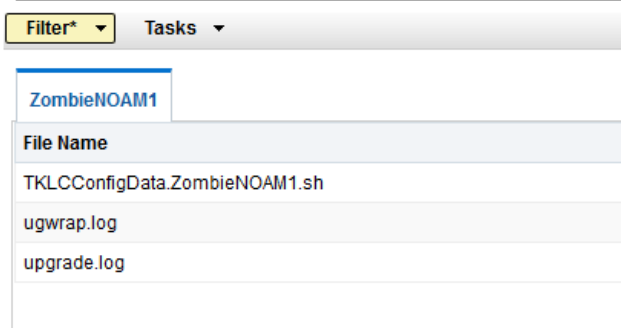
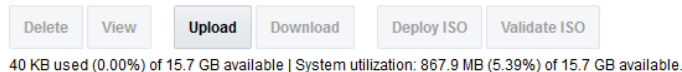
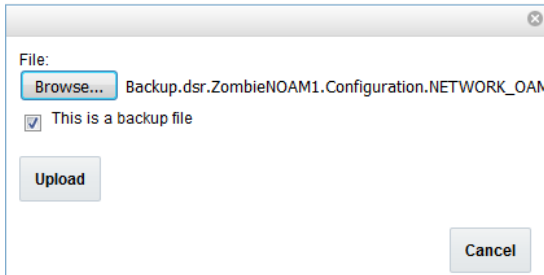
Procedure 1. Recovery Scenario 1

5. <input type="checkbox"/>	PMAC, TVOE Hosts, and Switch Recovery: Backups available	<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"> 1. Restore the PMAC TVOE host backup by executing Appendix G Restore TVOE Configuration from Backup Media. 2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup. 3. Recover failed OAs, aggregation, and enclosure switches by referring to Appendix B Recover/Replace Failed 3rd Party Components (Switches, OAs). 4. Verify/Update blade server firmware by executing the Server Blades Installation Preparation section from reference [10]. 5. Install TVOE on ALL failed TVOE servers as needed by executing the Install TVOE on Blade Servers procedure from reference [10]. 6. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed TVOE host blade servers. 7. Proceed to step 7.
6. <input type="checkbox"/>	PMAC, TVOE Hosts, and Switch Recovery: Backups NOT available	<p>This step assumes TVOE and PMAC backups are NOT available. If the TVOE and PMAC have already been restored, skip this step.</p> <ol style="list-style-type: none"> 1. Execute the Configure and IPM Management Server section from reference [10]. 2. Execute the Install PMAC procedure from reference [10]. 3. Execute the Configure Aggregation Switches procedure from reference [10] to recover Cisco 4948 aggregation switches, if needed. 4. Execute the Configure PMAC Application procedure from reference [10]. 5. Execute the HP C-7000 Enclosure Configuration procedure from reference [10] to recover and configure any failed OAs, if needed. 6. Execute the Enclosure and Blades Setup procedure from reference [10]. 7. Execute the Configure Enclosure Switches procedure from reference [10] to recover enclosure switches, if needed. 8. Verify/Update Blade server firmware by executing the Server Blades Installation Preparation procedure from reference [10]. 9. Install and configure TVOE on failed rack mount servers by executing the Installing TVOE on Rack Mount Server(s) procedure from reference [10]. 10. Install and configure TVOE on failed TVOE blade servers by executing the Install TVOE on Blade Servers procedure from reference [10].

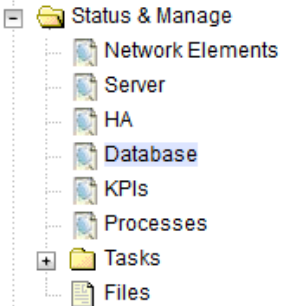


Procedure 1. Recovery Scenario 1

7. <input type="checkbox"/>	Execute Fast Deployment File for NOAMs	<p>The backup fdconfig file used during the initial DSR installation is available on the PMAC, if a database backup was restored on the PMAC.</p> <p>If a backup fast deployment xml is NOT available, execute Configure NOAM Servers from reference [8].</p> <p>If a backup fast deployment xml is already present on the PMAC, execute this procedure:</p> <ol style="list-style-type: none"> 1. Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade has been performed since initial installation). 2. Execute these commands: <pre>\$ cd /usr/TKLC/smac/etc \$ screen \$ sudo fdconfig config --file=<Created_FD_File>.xml</pre>
8. <input type="checkbox"/>	Obtain latest database backup and network configuration data	<ol style="list-style-type: none"> 1. Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. 2. Obtain most recent RADIUS shared secret encryption key file DpiKf.bin.encr from external backup sources. (Only when the RADIUS Key Revocation MOP has been executed on the system). <p>Note: Shared secret encryption key file needs to be handled by someone authorized to handle shared secrets information.</p> <p>Note: From Required Materials list; use site survey documents and Network Element report (if available) to determine network configuration data.</p>
9. <input type="checkbox"/>	Execute DSR installation procedure for the first NOAM	<ol style="list-style-type: none"> 1. Configure the first NOAM server by executing Configure the First NOAM NE and Server section from reference [8]. 2. Configure the NOAM server group by executing the Configure the NOAM Server Group section from reference [8]. <p>Note: Use the backup copy of network configuration data and site surveys (Step 2).</p>
10. <input type="checkbox"/>	NOAM GUI: Login	<p>Log into the NOAM GUI as the guiadmin user:</p> 

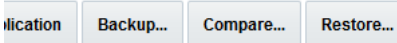
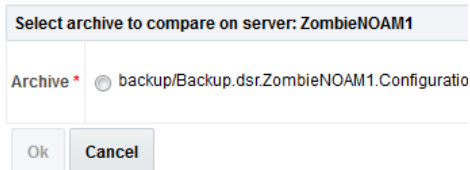
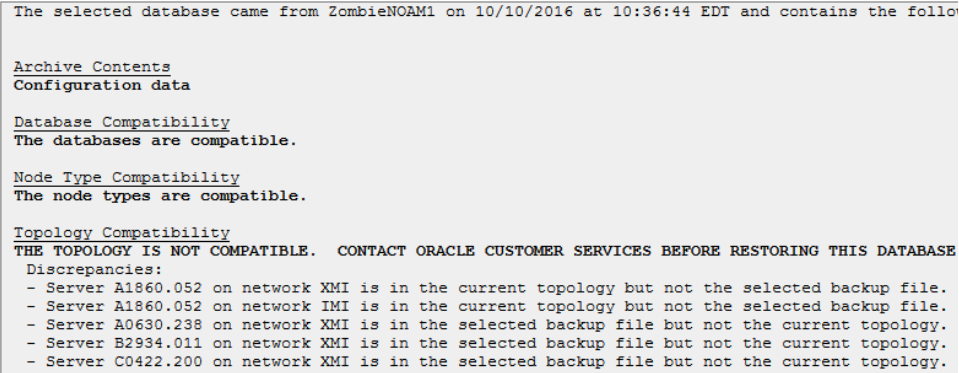
Procedure 1. Recovery Scenario 1

11. <input type="checkbox"/>	NOAM GUI: Upload the backup database file	<ol style="list-style-type: none"> Navigate to Status & Manage > Files.  Select the active NOAM server. Main Menu: Status & Manage -> Files  Click Upload and select the NO Provisioning and Configuration file backed up after initial installation and provisioning.  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. Click Open. Mark the This is a backup file checkbox. Click Upload.  <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>
------------------------------	---	--

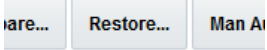
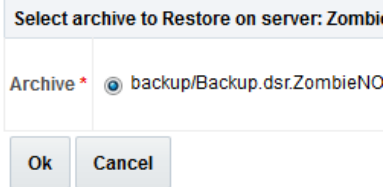
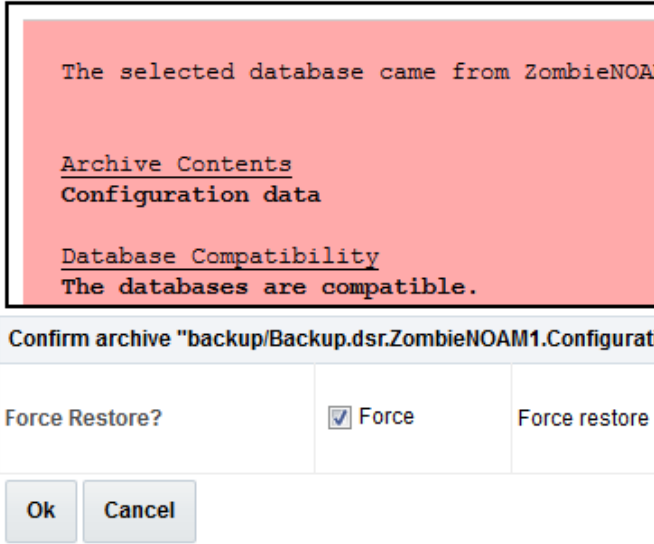
Procedure 1. Recovery Scenario 1

12.	NOAM GUI: Disable provisioning	<p>1. Navigate to Status & Manage > Database.</p>  <p>2. Click Disable Provisioning.</p>  <p>3. Click OK to disable Provisioning.</p> 
-----	--	---


Procedure 1. Recovery Scenario 1

13. <input type="checkbox"/>	NOAM GUI: Verify the archive contents and database compatibility	<ol style="list-style-type: none"> 1. Select the active NOAM server and click Compare.  2. Click the button for the restored database file uploaded as a part of step 11. of this procedure. Database Compare  3. Verify the output window matches the screen below. Note: A database mismatch regarding the Topology Compatibility and possibly User compatibility (due to authentication) display. These warnings are expected. If these are the only mismatches, proceed; otherwise, stop and contact My Oracle Support (MOS) to ask for assistance. Database Archive Compare  <p>Note: Archive Contents and Database Compatibilities must be the following:</p> <p>Archive Contents: Configuration data.</p> <p>Database Compatibility: The databases are compatible.</p> <p>Note: The following is expected output for Topology Compatibility Check since we are restoring from an existing backed up database to a database with just one NOAM:</p> <p>Topology Compatibility THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.</p> <p>Note: 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"> 4. If the verification is successful, click Back and continue to next step in this procedure.
------------------------------	--	--

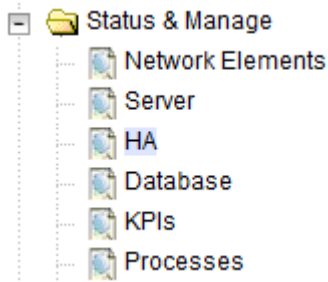

Procedure 1. Recovery Scenario 1

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

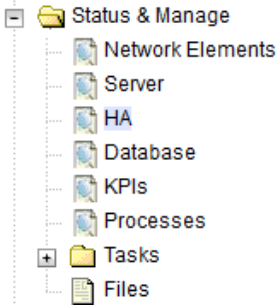
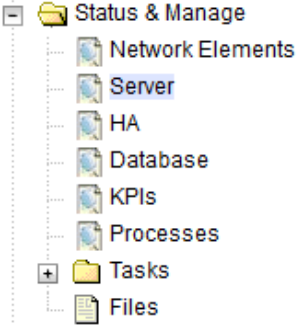

Procedure 1. Recovery Scenario 1

15. <input type="checkbox"/>	NOAM VIP GUI: Login	<ol style="list-style-type: none"> 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://<Primary_NOAM_VIP_IP_Address></div> Login as the guiadmin user: <div style="text-align: center; margin: 20px 0;">  </div> <div style="text-align: center;"> Oracle System Login </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 black; padding: 10px; width: 60%; margin: 0 auto;"> <p>Log In</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; margin-top: 10px;"> <input type="button" value="Log In"/> </p> </div> </div> <p style="font-size: small; 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="width: 60%; margin: 10px auto;"/> <p style="font-size: x-small; text-align: center; margin: 5px auto;">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; margin: 5px auto;">Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.</p>
16. <input type="checkbox"/>	NOAM VIP GUI: Monitor and confirm database restore	<ol style="list-style-type: none"> Wait for 5-10 minutes for the system to stabilize with the new topology: Monitor the Info tab for Success. This indicates the restore is complete and the system is stabilized. <p>Ignore these alarms for NOAM and MP servers until all the servers are configured:</p> <ul style="list-style-type: none"> Alarms with Type Column as REPL, COLL, HA (with mate NOAM), DB (about Provisioning Manually Disabled). <p>Note: Do not pay attention to alarms until all the servers in the system are completely restored.</p> <p>Note: The Configuration and Maintenance information is in the same state it was when backed up during initial backup.</p>

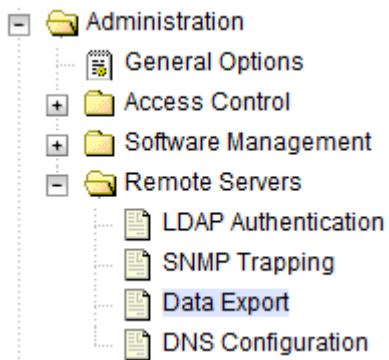

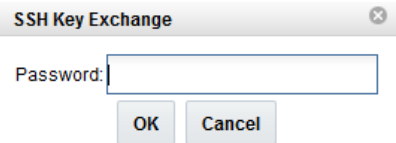

Procedure 1. Recovery Scenario 1

17. <input type="checkbox"/>	Active NOAM: Set failed servers to OOS	<p>1. Navigate to Status & Manage > HA.</p>  <p>2. Click Edit.</p> <p>3. Set the Max Allowed HA Role option to OOS for the failed servers.</p> <p>Modifying HA attributes</p> <table border="1" data-bbox="509 758 1045 1100"> <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>Active Standby Spare Observer OOS</td><td>The maximum des</td></tr> </tbody> </table> <p>4. Click OK.</p> 	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active ▼	The maximum des	ZombieNOAM2	OOS ▼	The maximum des	ZombieDRNOAM1	Active Standby Spare Observer OOS	The maximum des
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active ▼	The maximum des												
ZombieNOAM2	OOS ▼	The maximum des												
ZombieDRNOAM1	Active Standby Spare Observer OOS	The maximum des												
18. <input type="checkbox"/>	Active NOAM: Login	Log into the recovered active NOAM using SSH terminal as admusr user.												
19. <input type="checkbox"/>	NOAM VIP GUI: Recover standby NOAM	<p>1. Install the second NOAM server by executing the Configure the Second NOAM Server procedure, steps 3-5 and 7, from reference [8].</p> <p>Note: Execute step 6 if NetBackup is used.</p> <p>2. If NetBackup is used, execute the Install NetBackup Client procedure from reference [8].</p>												

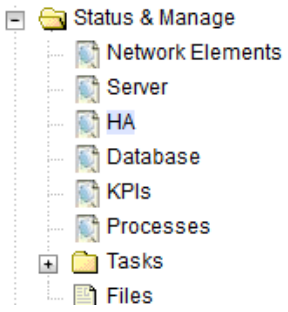
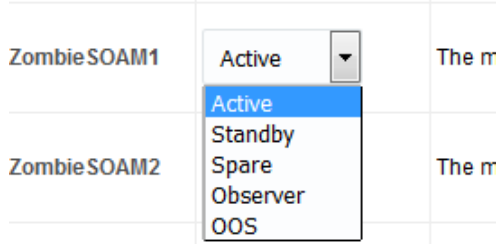
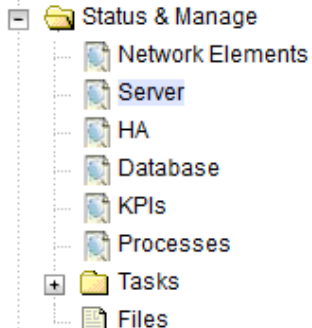
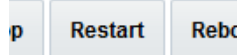
Procedure 1. Recovery Scenario 1

20. <input type="checkbox"/>	NOAM VIP GUI: Set HA on standby NOAM	<ol style="list-style-type: none"> Navigate to Status & Manage > HA.  Click Edit. Select the standby NOAM server and set it to Active. Modifying HA attributes <table border="1" data-bbox="516 764 989 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> Click OK. 	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												
21. <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application	<ol style="list-style-type: none"> Navigate to Status & Manage > Server.  Select the recovered standby NOAM server and click Restart.  												

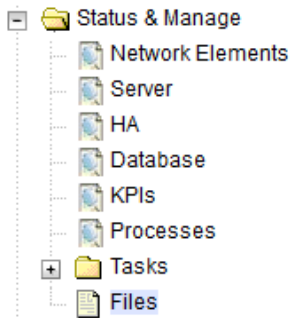
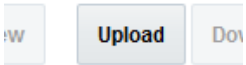
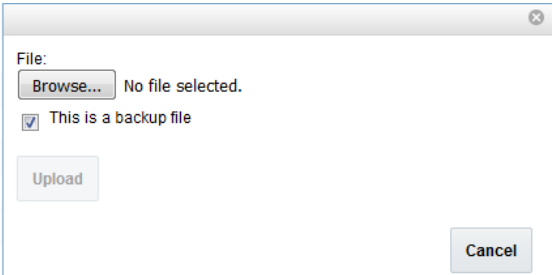
Procedure 1. Recovery Scenario 1

22. <input type="checkbox"/>	NOAM VIP GUI: Perform key exchange with export server	<ol style="list-style-type: none"> Navigate to Administration > Remote Servers > Data Export.  Click SSH Key Exchange at the bottom of the screen.  Type the Password and click OK. 
23. <input type="checkbox"/>	NOAM VIP GUI: Stop replication to the C-level servers of this site 	<p style="text-align: center;">!!Warning!!</p> <p>Before continuing this procedure, replication to C-level servers MUST 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>If the spare SOAM is also present in the site and lost, execute Appendix E Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost) to inhibit replication to working C-level servers before continuing.</p> <p>If the spare SOAM is NOT deployed in the site, execute Appendix C Inhibit A and B Level Replication on C-level Servers to inhibit replication to working C-level servers before continuing.</p>
24. <input type="checkbox"/>	Configure SOAM TVOE server blades	<p>If the TVOE restore has already been executed (step 5), skip this step.</p> <p>If a TVOE backup of the SOAM server blades is not available, execute Configure SOAM TVOE Server Blades from reference [8].</p>
25. <input type="checkbox"/>	Create and IPM SOAM VMs	<ol style="list-style-type: none"> Execute Create SOAM Guest VMs for the failed SOAM VMs and MP blades from reference [8]. Execute IPM Blades and VMs for the failed SOAM VMs and MP blades from reference [8]. Execute Install the Application for the failed SOAM VMs and MP blades from reference [8].


Procedure 1. Recovery Scenario 1

26. <input type="checkbox"/>	Recover active SOAM server	<p>1. Execute Configure the SOAM Servers, steps 1-3 and 5-8, from reference [8].</p> <p>Note: If you are using NetBackup, also execute step 10.</p> <p>2. If you are using NetBackup, execute Install NetBackup Client from reference [8].</p>
27. <input type="checkbox"/>	NOAM VIP GUI: Set HA on the SOAM server	<p>1. Navigate to Status & Manage > HA.</p>  <p>2. Click Edit.</p> <p>3. Select the SOAM server and set it to Active.</p>  <p>4. Click OK.</p>
28. <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application	<p>1. Navigate to Status & Manage > Server.</p>  <p>2. Select the recovered SOAM server and click Restart.</p> 

Procedure 1. Recovery Scenario 1

<p>29. <input type="checkbox"/></p>	<p>NOAM VIP GUI: Upload the backed up SOAM database file</p>	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > Files.  2. Select the active SOAM server tab. Click Upload and select the file SO Provisioning and Configuration file backed up after initial installation and provisioning.  3. Click Browse and locate the backup file. 4. Mark the This is a backup file checkbox. 5. Click Open. 6. Click Upload.  <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>
-------------------------------------	---	--

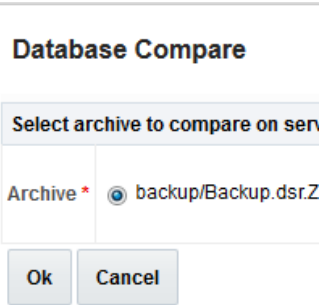
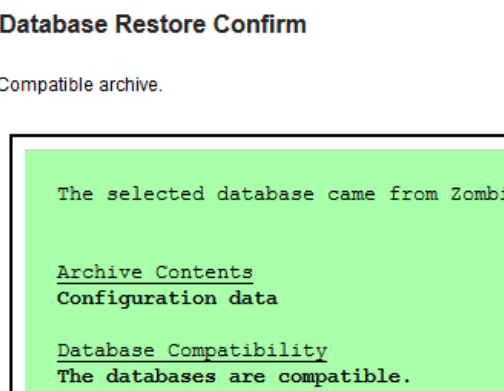
Procedure 1. Recovery Scenario 1

30. <input type="checkbox"/>	Recovered SOAM GUI: Login	<ol style="list-style-type: none">1. Establish a GUI session on the recovered SOAM server.2. Open the web browser and enter a URL of: <div data-bbox="548 338 1354 386" style="border: 1px solid black; padding: 2px; margin: 5px 0;">http://<Recovered_SOAM_IP_Address></div>3. Login as the guiadmin user: <div data-bbox="508 457 1451 1205"></div>
---------------------------------	----------------------------------	--


Procedure 1. Recovery Scenario 1

<p>31. <input type="checkbox"/></p>	<p>Recovered SOAM GUI: Verify the archive contents and database compatibility</p>	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > Database. 2. Select the Active SOAM server and click Compare. <div data-bbox="500 363 698 394" data-label="Image"> </div> 3. Click the button for the restored database file uploaded as a part of step 29. of this procedure. <div data-bbox="511 510 730 537" data-label="Section-Header"> <h4>Database Compare</h4> </div> <div data-bbox="511 573 834 751" data-label="Image"> </div> 4. Verify the output window matches the screen below. <div data-bbox="503 858 850 890" data-label="Section-Header"> <h4>Database Archive Compare</h4> </div> <div data-bbox="503 924 1156 1140" data-label="Image"> </div> <p>Note: Archive Contents and Database Compatibilities must be the following:</p> <p>Archive Contents: Configuration data.</p> <p>Database Compatibility: The databases are compatible.</p> <p>Note: The following is expected output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM:</p> <p>Topology Compatibility</p> <p>THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.</p> <p>Note: 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"> 5. If the verification is successful, click Back and continue to next step in this procedure.
-------------------------------------	--	--

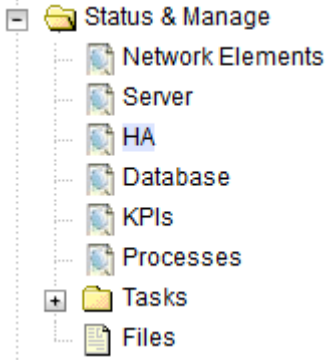
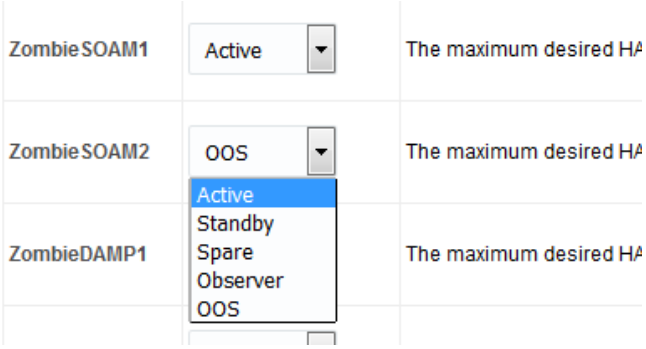
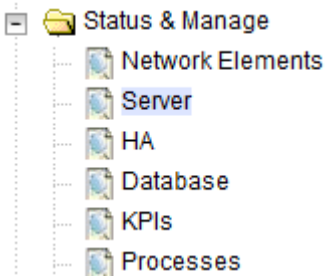

Procedure 1. Recovery Scenario 1

32. <input type="checkbox"/>	Recovered SOAM GUI: Restore the database	<ol style="list-style-type: none"> 1. Select the Active SOAM server and click Restore. 2. Select the backup provisioning and configuration file.  <ol style="list-style-type: none"> 3. Click OK.  <ol style="list-style-type: none"> 4. If the Node Type Compatibility error displays, it is expected. If no other errors display, mark the Force checkbox and click OK to proceed with the DB restore. <p>Note: After the restore has started, the user is logged out of XMI SOAM GUI since the restored topology is old data. The provisioning is disabled after this step.</p>
33. <input type="checkbox"/>	Recovered SOAM GUI: Monitor and confirm database restoral	<p>Wait for 5-10 minutes for the system to stabilize with the new topology: Monitor the Info tab for Success. This indicates the restore is complete and the system is stabilized.</p> <p>Note: Do not pay attention to alarms until all the servers in the system are completely restored.</p> <p>Note: The Configuration and Maintenance information is in the same state it was when backed up during initial backup.</p>

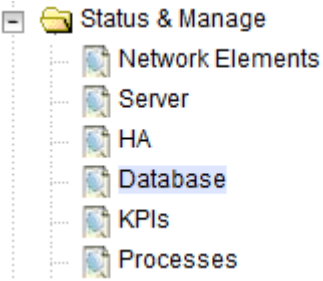
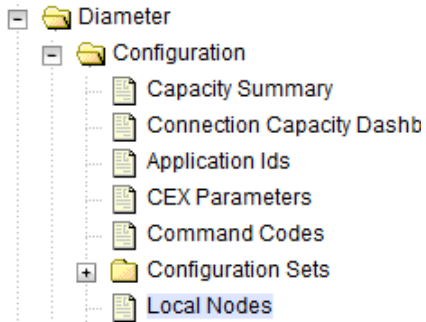
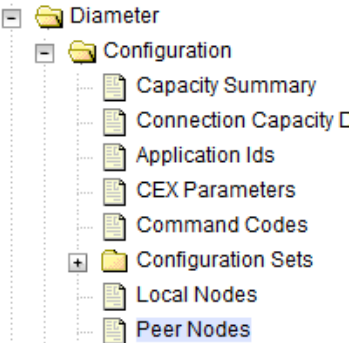
Procedure 1. Recovery Scenario 1

34. <input type="checkbox"/>	NOAM VIP GUI: Login	<ol style="list-style-type: none"> 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://<Primary_NOAM_VIP_IP_Address></div> Login as the guiadmin user: <div style="text-align: center; margin: 20px 0;">  </div> <div style="text-align: center;"> Oracle System Login </div> <hr style="width: 50%; margin: 10px auto;"/> <div style="text-align: right; margin-right: 50px;">Tue Jun 7 13:49:06 2016 EDT</div> <div style="text-align: center; margin: 20px 0;"> <div style="border: 1px solid black; padding: 10px; width: 60%; margin: 0 auto;"> <p>Log In</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; margin-top: 10px;"> <input type="button" value="Log In"/> </p> </div> </div> <p style="font-size: small; text-align: center; 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="width: 50%; margin: 10px auto;"/> <p style="font-size: x-small; text-align: center; margin-top: 10px;">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; margin-top: 10px;">Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.</p>
35. <input type="checkbox"/>	NOAM VIP GUI: Recover the remaining SOAM servers	<p>Recover the remaining SOAM servers (standby, spare) by repeating these steps for each SOAM server:</p> <ol style="list-style-type: none"> Execute Configure the SOAM Servers, steps 1-3 and 5-8, from reference [8]. <p>Note: If you are using NetBackup, also execute step 10.</p> <ol style="list-style-type: none"> If you are using NetBackup, execute Install NetBackup Client from reference [8].

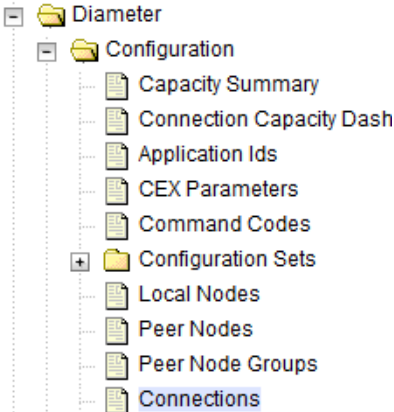
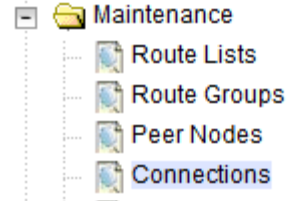
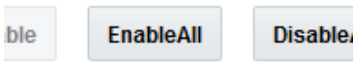
Procedure 1. Recovery Scenario 1

<p>36. <input type="checkbox"/></p>	<p>NOAM VIP GUI: Set HA on the remaining SOAMs</p>	<ol style="list-style-type: none"> Navigate to Status & Manage > HA.  Click Edit at the bottom of the screen. Select the recovered SOAM server and set it to Active.  Click OK.
<p>37. <input type="checkbox"/></p>	<p>NOAM VIP GUI: Restart DSR application</p>	<ol style="list-style-type: none"> Navigate to Status & Manage > Server.  Select the recovered standby SOAM server and click Restart. 

Procedure 1. Recovery Scenario 1

38. <input type="checkbox"/>	NOAM VIP GUI: Start replication on the recovered standby SOAM	<p>Un-Inhibit (start) replication to the recovered standby SOAM.</p> <ol style="list-style-type: none"> 1. Navigate to Status & Manage > Database.  <ol style="list-style-type: none"> 2. Click Allow Replication on the recovered standby SOAM server. 3. Verify the replication on all servers is allowed. This can be done by checking Repl status column of respective server
39. <input type="checkbox"/>	SOAM VIP GUI: Verify the local node info	<ol style="list-style-type: none"> 1. Navigate to Diameter > Configuration > Local Node.  <ol style="list-style-type: none"> 2. Verify all the local nodes are shown.
40. <input type="checkbox"/>	SOAM VIP GUI: Verify the peer node info	<ol style="list-style-type: none"> 1. Navigate to Diameter > Configuration > Peer Node.  <ol style="list-style-type: none"> 2. Verify all the peer nodes are shown.

Procedure 1. Recovery Scenario 1

41. <input type="checkbox"/>	SOAM VIP GUI: Verify the connections info	<ol style="list-style-type: none"> 1. Navigate to Diameter > Configuration > Connections.  2. Verify all the connections are shown.
42. <input type="checkbox"/>	SOAM VIP GUI: Enable connections, if needed	<ol style="list-style-type: none"> 1. Navigate to Diameter > Maintenance > Connections.  2. Select each connection and click Enable. Alternatively, you can enable all the connections by clicking EnableAll.  3. Verify the Operational State is Available. Note: If a Disaster Recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution
43. <input type="checkbox"/>	Active NOAM: Activate optional features	<p>Establish an SSH session to the active NOAM, login as admusr.</p> <p>Note for PCA Activation: If you have PCA installed in the system being recovered, re-activate PCA by executing PCA Activation on Entire Server on Recovered NOAM Server from [13].</p> <p>Note: If not all SOAM sites are recovered at this point, then you should repeat activation for each *new* SOAM site that comes online.</p> <p>Note: If any of the MPs are failed and recovered, then restart these MP servers after activation of the feature.</p> <p>Refer to 1.4 Optional Features to activate any features previously activated.</p>

Procedure 1. Recovery Scenario 1

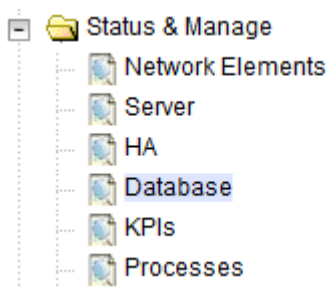
44. ☐ **NOAM VIP GUI:**
Start replication on working C-level servers

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

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




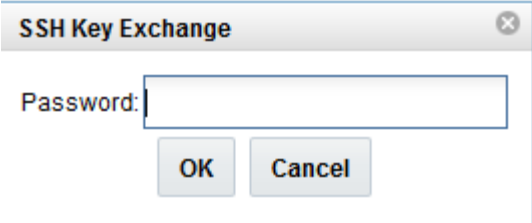
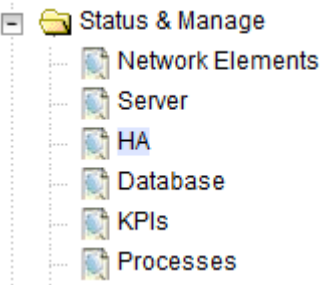
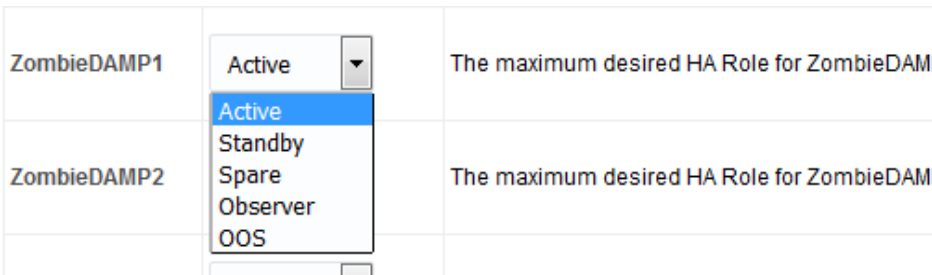
2. If the **Repl Status** is set to **Inhibited**, click **Allow Replication** using this order; otherwise, if none of the servers are inhibited, skip this step and continue with the next step:

- Active NOAM Server
- Standby NOAM Server
- Active SOAM Server
- Standby SOAM Server
- Spare SOAM Server (if applicable)
- 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)

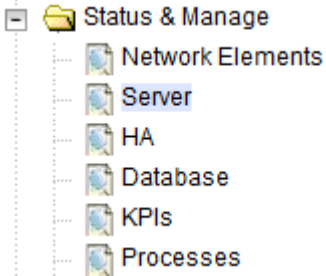

3. Verify the replication on all the working servers is allowed. This can be done by examining the Repl Status table.

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

45. <input type="checkbox"/>	SOAM VIP GUI: Perform key exchange with export server	<ol style="list-style-type: none"> Navigate to Administration > Remote Servers > Data Export.  Click SSH Key Exchange. Type the Password and click OK. 
46. <input type="checkbox"/>	NOAM VIP GUI: Recover the C-level server (DA-MP, SBRs, IPFE, SS7-MP)	<ol style="list-style-type: none"> Execute Configure MP Blade Servers, steps 1, 7, 11-14, and 17, from reference [8]. Note: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. Repeat this step for any remaining failed MP servers.
47. <input type="checkbox"/>	NOAM VIP GUI: Set HA on all C-level servers	<ol style="list-style-type: none"> Navigate to Status & Manage > HA.  Click Edit. For each recovered C-level with a Max Allowed HA Role set to Standby, set it to Active.  Click OK.

Procedure 1. Recovery Scenario 1

48.	NOAM VIP GUI: Restart DSR application on the recovered C-level servers	<div data-bbox="492 239 1442 695"><div>1. Navigate to Status & Manage > Server.</div><div></div><div>2. Select the recovered C-level servers and click Restart.</div><div></div></div>
-----	--	---

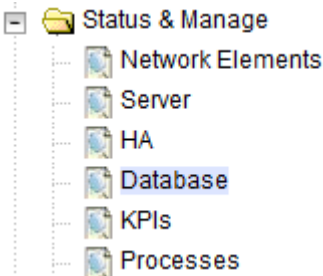
Procedure 1. Recovery Scenario 1

49. <div></div>	NOAM VIP GUI: Start replication on all C-level servers	<div>Un-inhibit (start) replication to the ALL C-level servers.</div> <div>1. Navigate to Status & Manage > Database.</div> <div><div><div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div><div>Status & 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. If the Repl Status is set to Inhibited, click Allow Replication using this order:</div> <div><div><div>Active NOAM Server</div><div>Standby NOAM Server</div><div>Active SOAM Server</div><div>Standby SOAM Server</div><div>Spare SOAM Server (if applicable)</div><div>Active DR NOAM Server</div><div>Standby DR NOAM Server</div><div>MP/IPFE servers (if MPs are configured as active/standby, start with the Active MP; otherwise, the order of the MPs does not matter)</div><div>SBRs (if SBR servers are configured, start with the active SBR, then standby, then spare)</div></div></div> <div>3. Verify the replication on all the working servers is allowed. This can be done by examining the Repl Status table.</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>	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																			
50. <div></div>	Active NOAM: Perform key exchange between the active-NOAM and recovered servers	<div>1. Establish an SSH session to the active NOAM, login as admusr.</div> <div>2. Perform a keyexchange from the active NOAM to each recovered server:</div> <div><div><div>\$ keyexchange admusr@<Recovered Server Hostname></div></div></div> <div>Note: If an export server is configured, perform this step.</div>																				

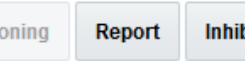
Procedure 1. Recovery Scenario 1

51. **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 1. Recovery Scenario 1

52. <input type="checkbox"/>	Active NOAM: Verify replication between servers	<ol style="list-style-type: none"> 1. Log into the active NOAM using SSH terminal as admusr. 2. Execute this command: <div data-bbox="503 336 1421 388" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>\$ sudo irepstat -m</pre> </div> <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 1. Recovery Scenario 1

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

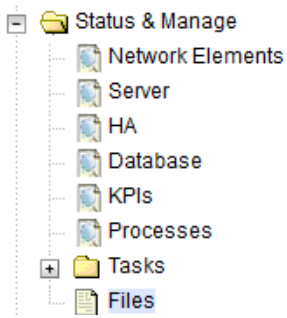
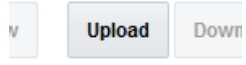
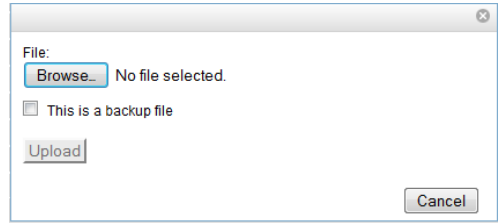
1. Navigate to **Status & Manage > Database**.

A screenshot of the NOAM VIP GUI navigation menu. The menu is displayed as a tree structure. The 'Status & Manage' folder is expanded, showing a list of sub-items: 'Network Elements', 'Server', 'HA', 'Database', 'KPIs', and 'Processes'. The 'Database' item is highlighted with a blue background.

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

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

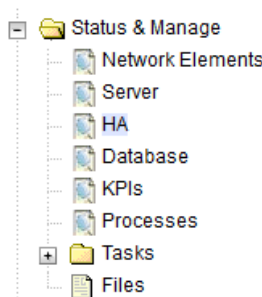
54. <input type="checkbox"/>	NOAM VIP GUI: Upload the backed up RADIUS key file (RADIUS only)	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> 1. Navigate to Status & Manage > Files.  <ol style="list-style-type: none"> 2. Select the active NOAM server tab. Click Upload and select the RADIUS shared secret encryption key file backed up after initial installation and provisioning or after key revocation execution.  <ol style="list-style-type: none"> 3. Click Browse. 4. Locate the DpiKf.bin.encr file. 5. Click Upload.  <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>Note: 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

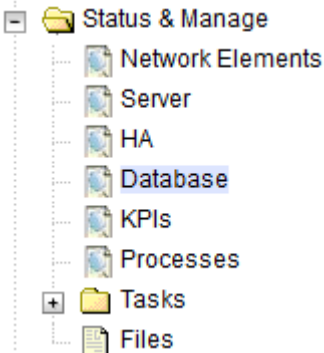
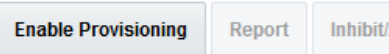
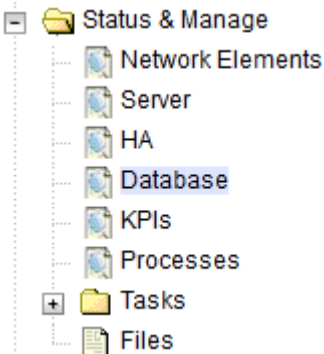
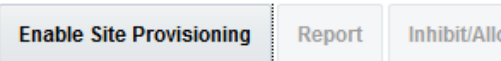
55. <input type="checkbox"/>	NOAM VIP: Copy and distribute RADIUS key file on active NOAM (RADIUS only) — Part 1	<p>If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.</p> <ol style="list-style-type: none"> 1. Log into the active NOAM VIP using SSH terminal as admusr user. 2. Copy the key file: <div data-bbox="505 436 1409 592" data-label="Text"> <pre>\$ cd /usr/TKLC/dpi/bin \$./sharedKrevo -decr \$ sudo rm /var/TKLC/db/filemgmt/<backed up key file name></pre> </div> 3. Make sure all servers in the topology are accessible. <div data-bbox="505 646 1409 1054" data-label="Text"> <pre>\$./sharedKrevo -checkAccess [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> </div> <p>Note: If all the servers are not accessible, then contact My Oracle Support (MOS).</p>
------------------------------	--	--

Procedure 1. Recovery Scenario 1

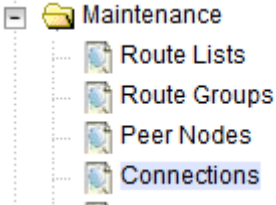
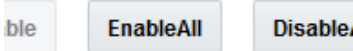
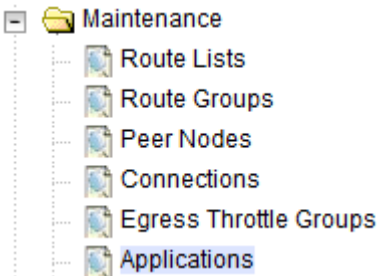
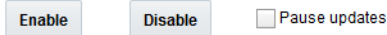
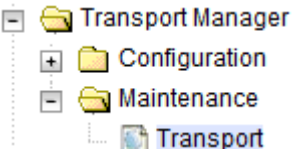
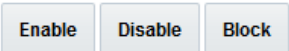
56. <input type="checkbox"/>	NOAM VIP: Copy and distribute the RADIUS key file on active NOAM (RADIUS only) — Part 2	<div>Distribute key file to all the servers in the topology:</div> <pre>\$./sharedKrevo -synchronize \$./sharedKrevo -updateData</pre> <div>Example output:</div> <pre>1450723210: [INFO] 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>Note: For any errors refer My Oracle Support (MOS).</div>
---------------------------------	--	--

57. <input type="checkbox"/>	NOAM VIP GUI: Verify the HA status	<div>1. Navigate to Status and Manage > HA.</div>  <div>2. Select the row for all of the servers.</div> <div>3. Verify the HA Role is either Active or Standby.</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																											

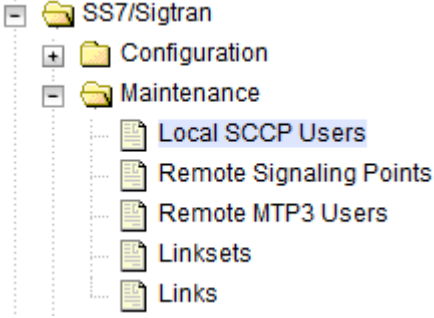
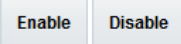
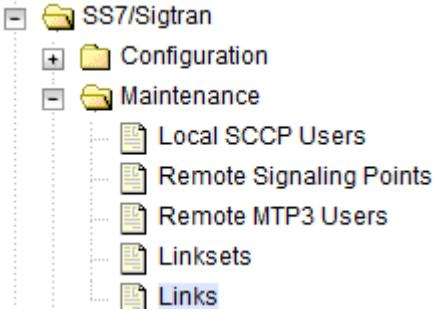
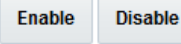
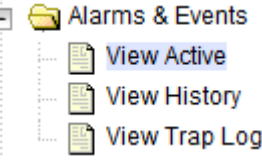
Procedure 1. Recovery Scenario 1

58. <input type="checkbox"/>	NOAM GUI: Enable provisioning	1. Navigate to Status & Manage > Database .  2. Click Enable Provisioning .  3. Click OK .
59. <input type="checkbox"/>	SOAM GUI: Enable site provisioning	1. Navigate to Status & Manage > Database .  2. Click Enable Site Provisioning .  3. Click OK .
60. <input type="checkbox"/>	MP Servers: Disable SCTP Auth Flag	For SCTP connections without DTLS enabled, refer to the Disable/Enable DTLS Feature Activation Guide [14]. Execute this procedure on all failed MP servers.

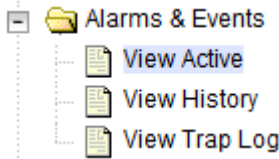
Procedure 1. Recovery Scenario 1

61. <input type="checkbox"/>	SOAM VIP GUI: Enable connections, if needed	<ol style="list-style-type: none"> Navigate to Diameter > Maintenance > Connections.  Select each connection and click Enable. Alternatively, enable all the connections by clicking EnableAll.  Verify the Operational State is Available. Note: If a disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution
62. <input type="checkbox"/>	SOAM VIP GUI: Enable optional features	<ol style="list-style-type: none"> Navigate to Diameter > Maintenance > Applications.  Select the optional feature application configured in step 43. Click Enable. 
63. <input type="checkbox"/>	SOAM VIP GUI: Re-enable transports, if needed	<ol style="list-style-type: none"> Navigate to Transport Manager > Maintenance > Transport.  Select each transport and click Enable.  Verify the Operational Status for each transport is Up.

Procedure 1. Recovery Scenario 1

64. <input type="checkbox"/>	SOAM VIP GUI: Re-enable MAPIWF application, if needed	<ol style="list-style-type: none"> Navigate to SS7/Sigtran > Maintenance > Local SCCP Users.  Click the Enable button corresponding to MAPIWF Application Name.  Verify the SSN Status is Enabled.
65. <input type="checkbox"/>	SOAM VIP GUI: Re-enable links, if needed	<ol style="list-style-type: none"> Navigate to SS7/Sigtran > Maintenance > Links.  Click Enable for each link.  Verify the Operational Status for each link is Up.
66. <input type="checkbox"/>	SOAM VIP GUI: Examine all alarms	<ol style="list-style-type: none"> Navigate to Alarms & Events > View Active.  Examine all active alarms and refer to the on-line help on how to address them. If needed, contact My Oracle Support (MOS).

Procedure 1. Recovery Scenario 1

67. <input type="checkbox"/>	NOAM VIP GUI: Examine all alarms	<p>1. Navigate to Alarms & Events > View Active.</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>
68. <input type="checkbox"/>	Restore GUI usernames and passwords	If applicable, execute the section 5 Resolve User Credential Issues after Database Restore procedure to recover the user and group information restored.
69. <input type="checkbox"/>	Backup and archive all the databases from the recovered system	Execute the DSR Database Backup procedure to back up the configuration databases.
70. <input type="checkbox"/>	Recover IDIH	If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.
71. <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"> 1. If SNMP is not configured in DSR. 2. If SNMP is already configured and SNMPv3 is selected as enabled version.

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

For a partial server outage with an NOAM server intact and available; SOAM servers are recovered using recovery procedures of base hardware and software and then executing a database restore to the active SOAM server using a database backup file obtained from the SOAM servers. All other servers are recovered using recovery procedures of base hardware and software. Database replication from the active NOAM server 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; detailed steps are in Procedure 2. The major activities are summarized as follows:

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

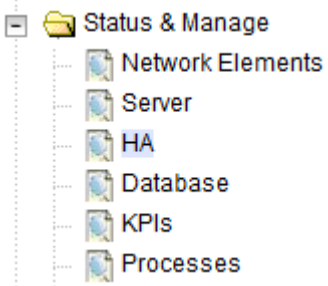
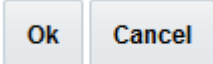
- Recover any failed **SOAM and MP** servers by recovering base hardware and software
 - Recover the base hardware
 - Recover the software

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

Procedure 2. Recovery Scenario 2

STEP #		<p>This procedure performs recovery if at least 1 NOAM server is available, but all SOAM servers in a site have failed. This includes any SOAM server that is in another location.</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"> If SNMP is not configured in DSR. 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"/>	NOAM VIP GUI: Login	<ol style="list-style-type: none"> 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="527 1087 1331 1138" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <code>http://<Primary_NOAM_VIP_IP_Address></code> </div> Login as the guiadmin user: <div data-bbox="760 1207 1182 1270" style="text-align: center; color: red; font-weight: bold; font-size: 1.2em;">ORACLE®</div> <div data-bbox="492 1323 743 1354" style="text-align: center;">Oracle System Login</div> <div data-bbox="1177 1350 1435 1375" style="text-align: right;">Tue Jun 7 13:49:06 2016 EDT</div> <div data-bbox="662 1417 1263 1785" style="border: 1px solid #ccc; padding: 10px; margin: 10px auto; width: 80%;"> <div data-bbox="922 1444 1006 1476" style="text-align: center;">Log In</div> <div data-bbox="717 1476 1211 1507" style="text-align: center;">Enter your username and password to log in</div> <div data-bbox="834 1533 1167 1566" style="text-align: center;">Username: <input style="width: 100%;" type="text"/></div> <div data-bbox="839 1589 1167 1623" style="text-align: center;">Password: <input style="width: 100%;" type="password"/></div> <div data-bbox="915 1646 1127 1671" style="text-align: center;"> <input type="checkbox"/> Change password </div> <div data-bbox="938 1709 993 1734" style="text-align: center; margin-top: 10px;"> <input type="button" value="Log In"/> </div> </div>


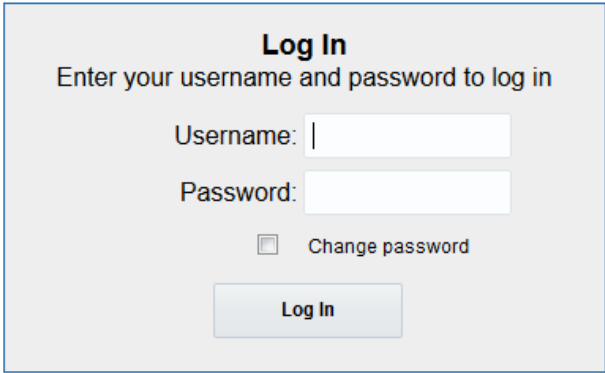
Procedure 2. Recovery Scenario 2

4. <input type="checkbox"/>	Active NOAM: Set failed servers to OOS	<ol style="list-style-type: none"> Navigate to Status & Manage > HA.  Click Edit. Modifying HA attributes <table border="1" data-bbox="487 714 1023 1060"> <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> Set the Max Allowed HA Role option to OOS for the failed servers. Click OK.  	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												
5. <input type="checkbox"/>	Replace failed equipment	HW vendor to replace the failed equipment.												
6. <input type="checkbox"/>	RMS NOAM Failure: Configure BIOS settings and update firmware	<p>If the failed server is NOT a rack mount server, skip to step 10.</p> <ol style="list-style-type: none"> Configure and verify the BIOS settings by executing procedure Configure the RMS and Blade Server BIOS Settings from reference [10]. Verify and/or upgrade server firmware by executing procedure Upgrade Management Server Firmware from reference [10]. <p>Note: Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.</p>												
7. <input type="checkbox"/>	RMS NOAM Failure: Backups available	<p>If the failed server is NOT a rack mount server, skip to step 10. This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media. If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing Restore PMAC from Backup 												

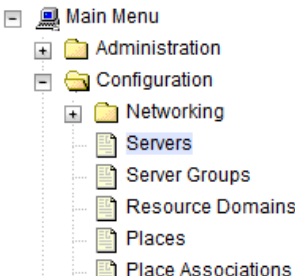
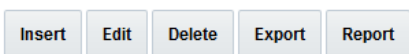
Procedure 2. Recovery Scenario 2

8. <input type="checkbox"/>	RMS NOAM Failure: Backups NOT available	<p>If the failed server is NOT a rack mount server, skip to step 10.</p> <p>This step assumes that TVOE and PMAC backups NOT are available, if the TVOE and PMAC have already been restored, skip this step.</p> <p>If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures:</p> <ol style="list-style-type: none"> 1. Configure and IPM Management Server from reference [10]. 2. Install PMAC from reference [10]. 3. Configure PMAC Application from reference [10]. <p>If the PMAC is NOT located on the same TVOE host as the failed NOAM, execute the following sections/procedures:</p> <ol style="list-style-type: none"> 1. Installing TVOE on Rack Mount Server(s) from reference [10].
9. <input type="checkbox"/>	Recover failed aggregation/ enclosure switches, and OAs	<p>Recover failed OAs, aggregation and enclosure switches, if needed.</p> <p>Backups Available:</p> <ol style="list-style-type: none"> 1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) section to recover failed OAs, aggregation, and enclosure switches <p>Backups NOT Available:</p> <ol style="list-style-type: none"> 1. Execute HP C-7000 Enclosure Configuration from reference [10] to recover and configure any failed OAs, if needed. 2. Execute Configure Enclosure Switches from reference [10] to recover enclosure switches, if needed.
10. <input type="checkbox"/>	HP-Class Blade Failure: Configure blade server iLO, update firmware/BIOS settings	<p>If the failed server is NOT an HP C-Class Blade, skip to step 14.</p> <ol style="list-style-type: none"> 1. Execute Configure Blade Server iLO Password for Administrator Account from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing Server Blades Installation Preparation from reference [10]
11. <input type="checkbox"/>	HP-Class Blade Failure: Backups available	<p>If the failed server is NOT an OAM type HP C-Class Blade, skip to step 14.</p> <p>This step assumes TVOE backups are available. If backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> 1. Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10]. 2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers.
12. <input type="checkbox"/>	HP-Class Blade Failure: Backups NOT available	<p>If the failed server is NOT an OAM type HP C-Class Blade, skip to step 14.</p> <p>This step assumes TVOE backups are NOT available:</p> <ol style="list-style-type: none"> 1. Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10]. 2. Configure the NOAM and/or SOAM failed TVOE server blades by executing Configure SOAM TVOE Server Blades from reference [8]. <p>Note: Although the title of the procedure is related to SOAMs only, execute this procedure for any failed NOAMs located on TVOE server blades.</p>

Procedure 2. Recovery Scenario 2

13. <input type="checkbox"/>	Create VMs	Execute Create NOAM/SOAM Virtual Machines to create the NOAM and SOAM VMs on failed TVOE servers.
14. <input type="checkbox"/>	IPM and install DSR application on failed guest/servers	<ol style="list-style-type: none"> 1. Execute IPM Blades and VMs for the failed SOAM VMs and MP blades from reference [8]. 2. Execute Install the Application Software for the failed SOAM VMs and MP blades from reference [8].
15. <input type="checkbox"/>	Install NetBackup client (Optional)	If NetBackup is used, execute Install NetBackup Client from reference [8].
16. <input type="checkbox"/>	NOAM VIP GUI: Login	<ol style="list-style-type: none"> 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://<Primary_NOAM_VIP_IP_Address></div> 2. Login as the guiadmin user: <div style="text-align: center; margin: 20px 0;">  </div> <div style="text-align: center;"> Oracle System Login Tue Jun 7 13:49:06 2016 EDT </div> <div style="text-align: center; margin: 20px 0;">  </div> <p style="text-align: center; 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 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, Oracle and/or its affiliates. All rights reserved.</p>

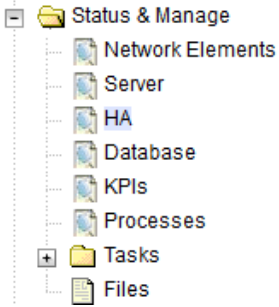
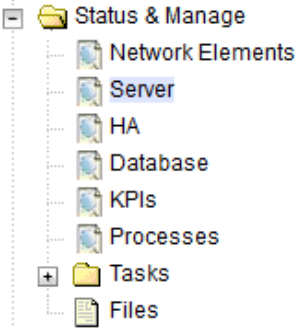

Procedure 2. Recovery Scenario 2

17. <input type="checkbox"/>	NOAM VIP GUI: Export the initial configuration	<p>If the failed server is NOT a NOAM server, skip to step 24.</p> <ol style="list-style-type: none"> 1. Navigate to Configuration > Servers.  <ol style="list-style-type: none"> 2. From the GUI screen, select the failed NOAM server and click Export to generate the initial configuration data for that server. 
18. <input type="checkbox"/>	NOAM VIP GUI: Copy configuration file to failed NOAM server	<ol style="list-style-type: none"> 1. Obtain a terminal session to the NOAM VIP, login as the admusr user. 2. Configure the failed NOAM server: <pre data-bbox="487 892 1412 1050">\$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<Failed_NOAM_Hostname>.sh admusr@<Failed_NOAM_control_IP_address>:/var/tmp/TKLCConfigData.sh</pre>
19. <input type="checkbox"/>	Failed NOAM Server: Verify the configuration was called and reboot the server	<ol style="list-style-type: none"> 1. Establish an SSH session to the failed NOAM server, login as the admusr user. The automatic configuration daemon looks for the file named TKLCConfigData.sh in the /var/tmp directory, implements the configuration in the file, and asks the user to reboot the server. 2. Verify awpushcfg was called by checking the following file. <pre data-bbox="487 1291 1380 1417">\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> <p>Verify this message displays: [SUCCESS] script completed successfully!</p> <ol style="list-style-type: none"> 3. Reboot the server: <pre data-bbox="487 1480 1380 1522">\$ sudo init 6</pre> <ol style="list-style-type: none"> 4. Wait for the server to reboot.


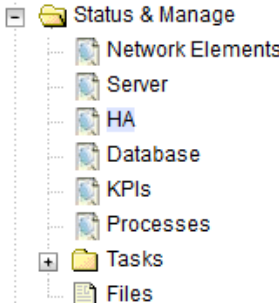
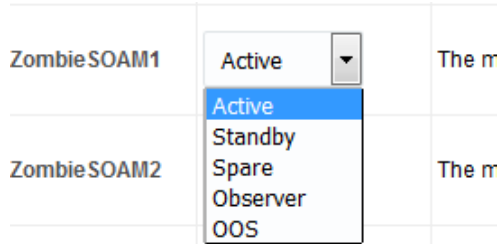
Procedure 2. Recovery Scenario 2

20. <input type="checkbox"/>	Failed NOAM Server: Configure networking for dedicated NetBackup interface (Optional)	<p>Note: Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.</p> <p>Obtain a terminal window to the failed NOAM server, logging in as the admusr.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP_Address> --netmask=<NO2_NetBackup_NetMask></pre> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NO1_NetBackup_Network_ID> --netmask=<NO2_NetBackup_NetMask> --gateway=<NO2_NetBackup_Gateway_IP_Address></pre>
21. <input type="checkbox"/>	Failed NOAM Server: Verify server health	<p>Execute this command on the 2nd NOAM server and make sure no errors are returned:</p> <pre>\$ sudo syscheck</pre> <pre>Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

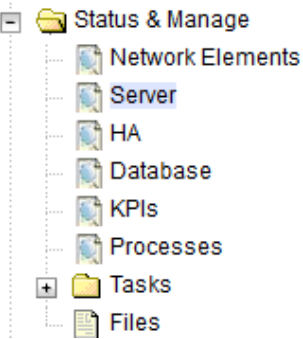

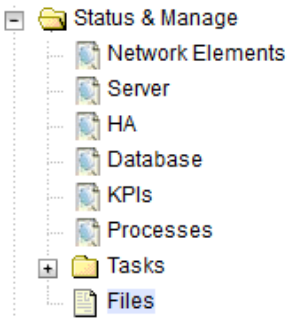


Procedure 2. Recovery Scenario 2

22. <input type="checkbox"/>	NOAM VIP GUI: Set HA on standby NOAM	<ol style="list-style-type: none"> Navigate to Status & Manage > HA.  Click Edit at the bottom of the screen. Select the standby NOAM server and set it to Active. Modifying HA attributes <table border="1" data-bbox="492 772 966 1045"> <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> Click OK. 	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												
23. <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application	<ol style="list-style-type: none"> Navigate to Status & Manage > Server.  Select the recovered standby NOAM server and click Restart.  												

Procedure 2. Recovery Scenario 2

24. <input type="checkbox"/>	NOAM VIP GUI: Stop replication to the C-level servers of this site 	<div style="text-align: center; color: red; font-weight: bold; font-size: 1.2em;">!!Warning!!</div> <p>Before continuing this procedure, replication to C-level servers at the SOAM site being recovered MUST be inhibited.</p> <p>Failure to inhibit replication to the working C-level servers results in the database being destroyed!</p> <p>If the spare SOAM is also present in the site and lost, execute 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>If the spare SOAM is NOT deployed in the site, execute Inhibit A and B Level Replication on C-level Servers to inhibit replication to working C-level servers before continuing.</p>
25. <input type="checkbox"/>	Recover active SOAM server	<ol style="list-style-type: none"> Execute Configure the SOAM Servers, steps 1-3 and 5-8, from reference [8]. Note: If you are using NetBackup, also execute step 10. If you are using NetBackup, execute Install NetBackup Client from reference [8].
26. <input type="checkbox"/>	NOAM VIP GUI: Set HA on SOAM server	<ol style="list-style-type: none"> Navigate to Status & Manage > HA.  Click Edit at the bottom of the screen. Select the SOAM server and set it to Active.  Click OK.

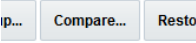
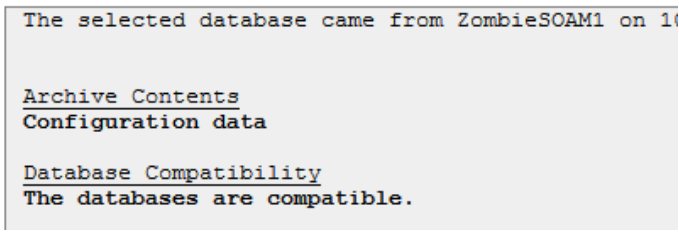
Procedure 2. Recovery Scenario 2

27. <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > Server.  2. Select the recovered SOAM server and click Restart. 
28. <input type="checkbox"/>	NOAM VIP GUI: Upload the backed up SOAM database file	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > Files.  2. Select the active SOAM server tab. Click Upload and select the SO Provisioning and Configuration file backed up after initial installation and provisioning.  3. Click Browse and locate the backup file. 4. Check This is a backup file checkbox. 5. Click Upload.  <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 2. Recovery Scenario 2

29.	<div data-bbox="191 279 219 310" data-label="Image"><input type="checkbox"/></div> Recovered SOAM GUI: Login	<ol style="list-style-type: none"> 1. Establish a GUI session on the recovered SOAM server. 2. Open the web browser and enter a URL of: <div data-bbox="527 338 1331 386" data-label="Text"><code>http://<Recovered_SOAM_IP_Address></code></div> 3. Login as the guiadmin user: <div data-bbox="751 457 1183 522" data-label="Image"></div> <div data-bbox="482 571 747 606" data-label="Section-Header">Oracle System Login</div> <div data-bbox="1164 598 1446 625" data-label="Text">Tue Jun 7 13:49:06 2016 EDT</div> <div data-bbox="656 663 1252 1033" data-label="Form"> <div> <div>Log In</div> <div>Enter your username and password to log in</div> <div>Username: <input type="text"/></div> <div>Password: <input type="password"/></div> <div><input type="checkbox"/> Change password</div> <div>Log In</div> </div> </div> <div data-bbox="505 1050 1424 1098" data-label="Text"> <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="592 1115 1326 1167" data-label="Text"> <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="656 1184 1266 1213" data-label="Text"> <p>Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.</p> </div>
-----	--	---

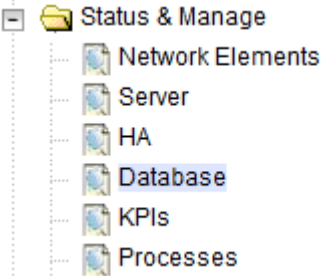
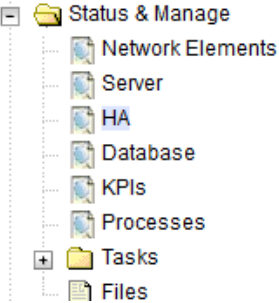
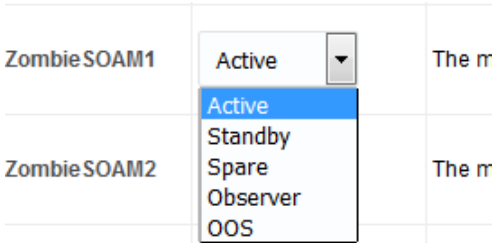
Procedure 2. Recovery Scenario 2

30. <input type="checkbox"/>	Recovered SOAM GUI: Verify the archive contents and database compatibility	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > Database. 2. Select the Active SOAM server and click Compare.  <ol style="list-style-type: none"> 3. Click the button for the restored database file uploaded as a part of step 28 of this procedure. <p>Database Compare</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"> 4. Verify the output window matches the screen below.  <p>Database Archive Compare</p> <pre>The selected database came from ZombieSOAM1 on 10/10/2019 10:10:10 AM</pre> <p><u>Archive Contents</u> Configuration data</p> <p><u>Database Compatibility</u> The databases are compatible.</p> <p>Note: Archive Contents and Database Compatibilities must be the following:</p> <p>Archive Contents: Configuration data.</p> <p>Database Compatibility: The databases are compatible.</p> <p>Note: The following is expected output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM:</p> <p>Topology Compatibility THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.</p> <p>Note: 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"> 5. If the verification is successful, click Back, then cancel and continue to next step in this procedure.
------------------------------	--	--

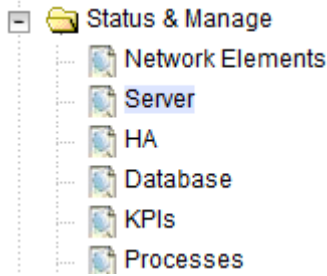

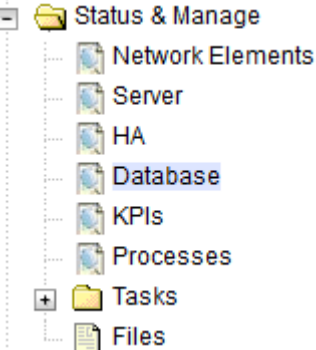
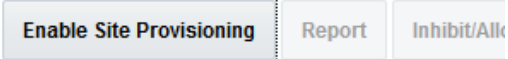
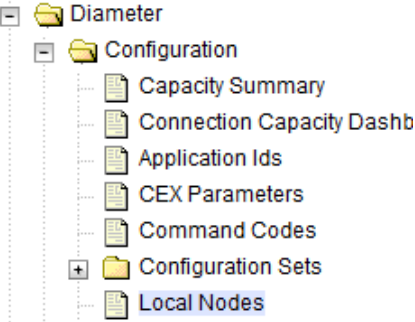
Procedure 2. Recovery Scenario 2

31. <input type="checkbox"/>	Recovered SOAM GUI: Restore the database	<ol style="list-style-type: none"> 1. Select the active SOAM server and click Restore. 2. Select the backup provisioning and configuration file. <div data-bbox="487 336 893 693"> <p>Database Restore</p> <p>Select archive to Restore on server: ZombieSOAM2</p> <div> <input type="radio"/> backup/Backup.dsr.ZombieSOAM2.Configura <input type="radio"/> backup/Backup.dsr.ZombieSOAM2.Configura <input type="radio"/> backup/Backup.dsr.ZombieSOAM2.Configura <input type="radio"/> backup/Backup.dsr.ZombieSOAM2.Configura <input type="radio"/> backup/Backup.dsr.ZombieSOAM2.Configura <input type="radio"/> backup/Backup.dsr.ZombieSOAM2.Configura <input type="radio"/> backup/Backup.dsr.ZombieSOAM2.Configura <input checked="" type="radio"/> backup/Backup.dsr.ZombieSOAM2.Configura </div> <p>Archive *</p> <p>Ok Cancel</p> </div> 3. Click OK. 4. If you get an error for Node Type Compatibility, that is expected. If no other errors display, mark the Force checkbox and click OK to proceed with the DB restore. <div data-bbox="487 861 990 1260"> <p>Database Restore Confirm</p> <p>Compatible archive.</p> <div> <p>The selected database came from Zombie</p> <p><u>Archive Contents</u> Configuration data</p> <p><u>Database Compatibility</u> The databases are compatible.</p> </div> </div> <p>Note: After the restore has started, the user is logged out of XMI SOAM GUI since the restored Topology is old data. The provisioning is disabled after this step.</p>
32. <input type="checkbox"/>	Recovered SOAM GUI: Monitor and Confirm database restoral	<p>Wait for 5-10 minutes for the system to stabilize with the new topology: Monitor the Info tab for Success. This indicates the restore is complete and the system is stabilized.</p> <p>Note: Do not pay attention to alarms until all the servers in the system are completely restored.</p> <p>Note: The Configuration and Maintenance information is in the same state it was when backed up during initial backup.</p>

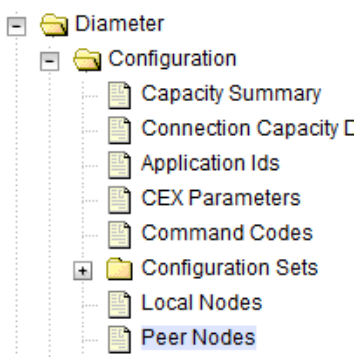
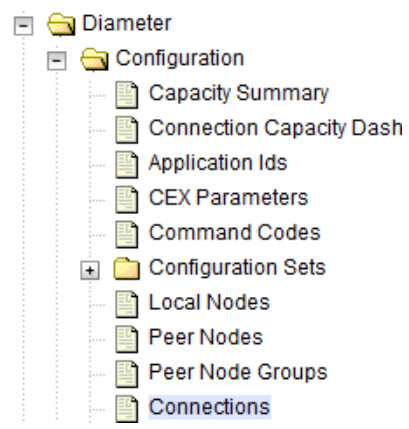
Procedure 2. Recovery Scenario 2

33. <input type="checkbox"/>	NOAM VIP GUI: Recover the remaining SOAM servers	<p>Recover the remaining SOAM servers (standby, spare) by repeating these steps for each SOAM server:</p> <ol style="list-style-type: none"> 1. Execute Configure the SOAM Servers, steps 1-3 and 5-8, from reference [8]. <p>Note: If you are using NetBackup, also execute step 10.</p> <ol style="list-style-type: none"> 2. If you are using NetBackup, execute Install NetBackup Client from reference [8]. 															
34. <input type="checkbox"/>	NOAM VIP GUI: Start replication on the recovered SOAMs	<p>Un-Inhibit (start) replication to the recovered SOAM servers</p> <ol style="list-style-type: none"> 1. Navigate to Status & Manage > Database.  <ol style="list-style-type: none"> 2. Click Allow Replication on the recovered SOAM servers. 3. Verify the replication on all SOAMs servers is allowed. This can be done by checking Repl status column of respective server 															
35. <input type="checkbox"/>	NOAM VIP GUI: Set HA on the recovered standby SOAM server	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > HA.  <ol style="list-style-type: none"> 2. Click Edit at the bottom of the screen 3. Select the recovered standby SOAM server and set it to Active.  <table border="1"> <tbody> <tr> <td>ZombieSOAM1</td> <td>Active</td> <td>The n</td> </tr> <tr> <td>ZombieSOAM2</td> <td>Standby</td> <td>The n</td> </tr> <tr> <td></td> <td>Spare</td> <td></td> </tr> <tr> <td></td> <td>Observer</td> <td></td> </tr> <tr> <td></td> <td>OOS</td> <td></td> </tr> </tbody> </table> <ol style="list-style-type: none"> 4. Click OK. 	ZombieSOAM1	Active	The n	ZombieSOAM2	Standby	The n		Spare			Observer			OOS	
ZombieSOAM1	Active	The n															
ZombieSOAM2	Standby	The n															
	Spare																
	Observer																
	OOS																

Procedure 2. Recovery Scenario 2

36. <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application	<p>1. Navigate to Status & Manage > Server.</p>  <p>2. Select the recovered standby SOAM server and click Restart.</p> 
37. <input type="checkbox"/>	SOAM GUI: Enable provisioning	<p>1. Navigate to Status & Manage > Database.</p>  <p>2. Click Enable Site Provisioning.</p>  <p>3. A confirmation window displays. Click OK to enable provisioning.</p>
38. <input type="checkbox"/>	SOAM VIP GUI: Verify local node information	<p>1. Navigate to Diameter > Configuration > Local Node.</p>  <p>2. Verify all the local nodes are shown.</p>

Procedure 2. Recovery Scenario 2

39. <input type="checkbox"/>	SOAM VIP GUI: Verify the peer node information	<p>1. Navigate to Diameter > Configuration > Peer Node.</p>  <p>2. Verify all the peer nodes are shown.</p>
40. <input type="checkbox"/>	SOAM VIP GUI: Verify the connections information	<p>1. Navigate to Diameter > Configuration > Connections.</p>  <p>2. Verify all the connections are shown.</p>

Procedure 2. Recovery Scenario 2

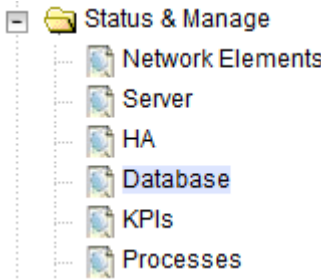
41. ☐ **NOAM VIP GUI:**
Start replication on working C-level servers

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

If the spare SOAM is also present in the site and lost, execute 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 Un-Inhibit A and B Level Replication on C-level Servers.

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



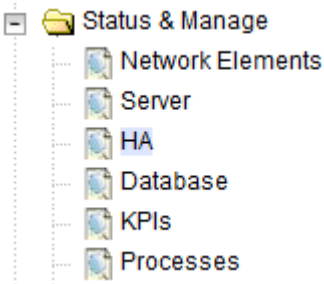
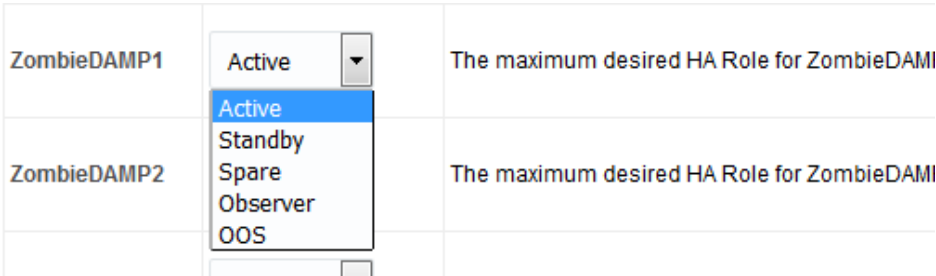
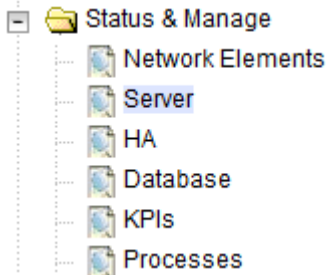

2. If the **Repl Status** is set to **Inhibited**, click **Allow Replication** using this order; otherwise, if none of the servers are inhibited, skip this step and continue with the next step:

- Active NOAM Server
- Standby NOAM Server
- Active SOAM Server
- Standby SOAM Server
- Spare SOAM Server (if applicable)
- 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)

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

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

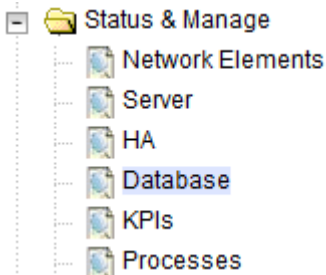

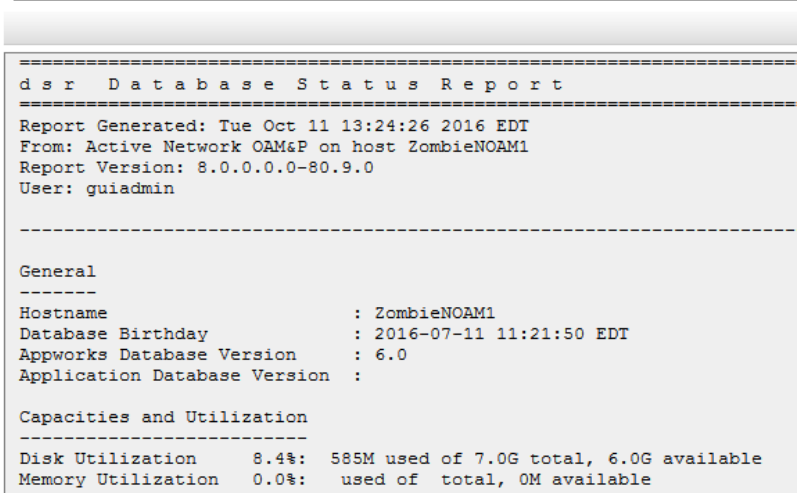
Procedure 2. Recovery Scenario 2

42. <input type="checkbox"/>	NOAM VIP GUI: Recover the C-level servers (DA-MP, SBRs, IPFE, SS7-MP)	<p>Execute the Configure MP Blade Servers procedure, steps 1, 7, 11-14, and 17, from reference [8].</p> <p>Note: Also execute step 15 and 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>Repeat this step for any remaining failed MP servers.</p>
43. <input type="checkbox"/>	NOAM VIP GUI: Set HA on all C-level servers	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > HA.  2. Click Edit at the bottom of the screen. 3. For each recovered C-level with a Max Allowed HA Role set to Standby, set it to Active.  4. Click OK.
44. <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application on the recovered C-level servers	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > Server.  2. Select the recovered C-level servers and click Restart. 

Procedure 2. Recovery Scenario 2

45. <div></div>	NOAM VIP GUI: Start replication on ALL C-level servers	<p>Un-Inhibit (start) replication to the ALL C-level servers.</p> <p>1. Navigate to Status & Manage > Database.</p> <div><div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div><div>Status & Manage</div><div>Network Elements</div><div>Server</div><div>HA</div><div>Database</div><div>KPIs</div><div>Processes</div></div> <p>2. If the Repl Status is set to Inhibited, click Allow Replication using this order:</p> <ul style="list-style-type: none">• Active NOAMP Server• Standby NOAMP Server• Active SOAM Server• Standby SOAM Server• Spare SOAM Server (if applicable)• 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). <p>3. Verify the replication on all servers is allowed. This can be done by checking the Repl Status.</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																			
46. <div></div>	Active NOAM: Perform keyexchange between the active-NOAM and recovered servers	<p>1. Establish an SSH session to the active NOAM, login as admusr.</p> <p>2. Execute this command to perform a keyexchange from the active NOAM to each recovered server:</p> <div><pre>\$ keyexchange admusr@<Recovered Server Hostname></pre></div>																				

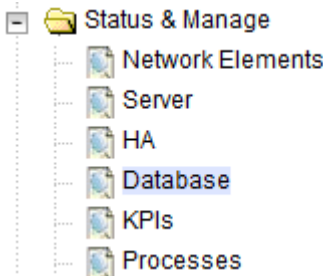
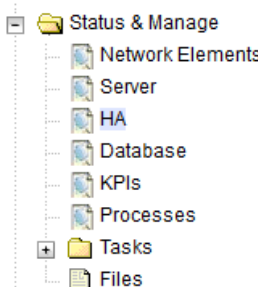
Procedure 2. Recovery Scenario 2

47. <input type="checkbox"/>	Active NOAM: Activate optional features	<p>Establish an SSH session to the active NOAM and login as admusr.</p> <p>Note for PCA Feature Activation:</p> <p>If you have PCA installed in the system being recovered, re-activate the PCA by executing the PCA Activation on Standby NOAM server procedure on the recovered standby NOAM server, and the PCA Activation on Active SOAM Server procedure on the recovered active SOAM server from [13].</p> <p>Refer to Optional Features to activate any features that were previously activated.</p> <p>Note: 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>Note: If any of the MPs are failed and recovered, then restart these MP servers after activation of the feature.</p>
48. <input type="checkbox"/>	NOAM VIP GUI: Fetch and store the database report for the newly restored data and save it	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > Database.  2. Select the active NOAM server and click Report.  <p>The following screen displays:</p> <p>Main Menu: Status & Manage -> Database [Report]</p>  3. Click Save and save the report to your local machine.

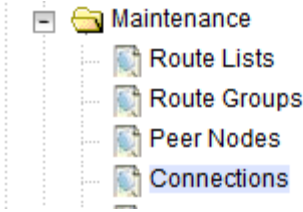
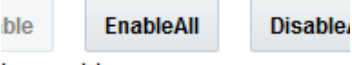
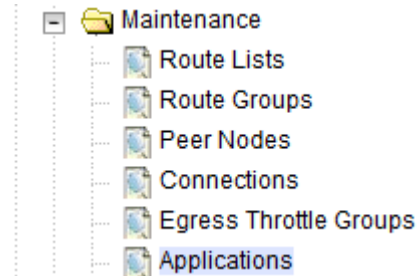
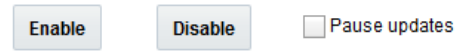
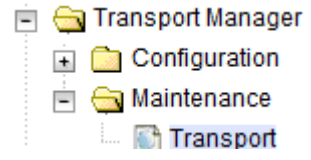

Procedure 2. Recovery Scenario 2

49. <input type="checkbox"/>	Active NOAM: Verify replication between servers	<ol style="list-style-type: none"> 1. Log into the active NOAM using SSH terminal as admusr. 2. Execute this command: <div data-bbox="477 338 1403 386" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>\$ sudo irepstat -m</pre> </div> <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>
---------------------------------	--	---

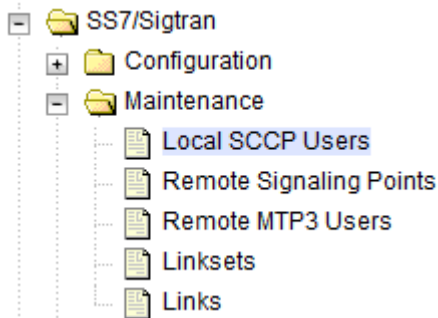
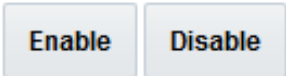
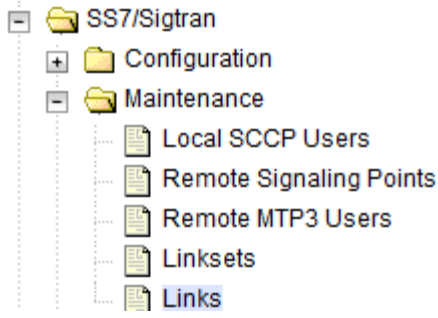
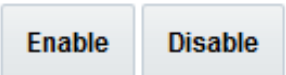
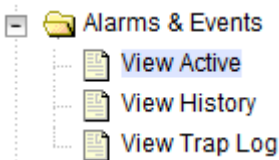
Procedure 2. Recovery Scenario 2

50. <input type="checkbox"/>	NOAM VIP GUI: Verify the database states	<div><div>1. Navigate to Status & Manager > Database.</div><div></div><div>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:</div><table><tr><th>Network Element</th><th>Server</th><th>Role</th><th>OAM Max HA Role</th></tr><tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM1</td><td>Network OAM&P</td><td>Active</td></tr><tr><td>ZombieNOAM</td><td>ZombieNOAM2</td><td>Network OAM&P</td><td>Standby</td></tr><tr><td>ZombieSOAM</td><td>ZombieSOAM2</td><td>System OAM</td><td>N/A</td></tr><tr><td>ZombieNOAM</td><td>ZombieNOAM1</td><td>Network OAM&P</td><td>Active</td></tr><tr><td>ZombieSOAM</td><td>ZombieSOAM1</td><td>System OAM</td><td>Active</td></tr><tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM2</td><td>Network OAM&P</td><td>Standby</td></tr><tr><td>ZombieSOAM</td><td>ZombieDAMP2</td><td>MP</td><td>Standby</td></tr><tr><td>ZombieSOAM</td><td>ZombieSS7MP2</td><td>MP</td><td>Active</td></tr><tr><td>ZombieSOAM</td><td>ZombieSS7MP1</td><td>MP</td><td>Active</td></tr><tr><td>ZombieSOAM</td><td>ZombieIPFE1</td><td>MP</td><td>Active</td></tr><tr><td>ZombieSOAM</td><td>ZombieIPFE2</td><td>MP</td><td>Active</td></tr></table></div>	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
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																																															
51. <input type="checkbox"/>	NOAM VIP GUI: Verify the HA status	<div><div>1. Navigate to Status and Manage > HA.</div><div></div><div>2. Select the row for all of the servers.</div><div>3. Verify the HA Role is either Active or Standby.</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></div>	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 2. Recovery Scenario 2

52. <input type="checkbox"/>	MP Servers: Disable SCTP auth flag	For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [14]. Execute this procedure on all failed MP servers.
53. <input type="checkbox"/>	SOAM VIP GUI: Enable connections, if needed	<ol style="list-style-type: none"> Navigate to Diameter > Maintenance > Connections.  Select each connection and click Enable. Alternatively, you can enable all the connections by clicking EnableAll.  Verify the Operational State is Available. Note: If disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution.
54. <input type="checkbox"/>	SOAM VIP GUI: Enable optional features	<ol style="list-style-type: none"> Navigate to Diameter > Maintenance > Applications.  Select the optional feature application configured in step 47. Click Enable. 
55. <input type="checkbox"/>	SOAM VIP GUI: Re-enable transports, if needed	<ol style="list-style-type: none"> Navigate to Transport Manager > Maintenance > Transport.  Select each transport and click Enable.  Verify the Operational Status for each transport is Up.

Procedure 2. Recovery Scenario 2

56. <input type="checkbox"/>	SOAM VIP GUI: Re-enable MAPIWF application, if needed	<ol style="list-style-type: none"> Navigate to SS7/Sigtran > Maintenance > Local SCCP Users.  Click the Enable button corresponding to MAPIWF Application Name.  Verify the SSN Status is Enabled.
57. <input type="checkbox"/>	SOAM VIP GUI: Re-enable links, if needed	<ol style="list-style-type: none"> Navigate to SS7/Sigtran > Maintenance > Links.  Click Enable for each link.  Verify the Operational Status for each link is Up.
58. <input type="checkbox"/>	SOAM VIP GUI: Examine All alarms	<ol style="list-style-type: none"> Navigate to Alarms & Events > View Active.  Examine all active alarms and refer to the on-line help on how to address them. If needed, contact My Oracle Support (MOS).

Procedure 2. Recovery Scenario 2

59. <input type="checkbox"/>	NOAM VIP GUI: Examine all alarms	<ol style="list-style-type: none"> 1. Log into the NOAM VIP if not already logged in. 2. Navigate to Alarms & Events > View Active.  3. Examine all active alarms and refer to the on-line help on how to address them.
60. <input type="checkbox"/>	NOAM VIP: 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"> 1. Establish an SSH session to the NOAM VIP. Login as admusr. 2. Check if all the servers in the Topology are accessible: <pre>\$ cd /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>
61. <input type="checkbox"/>	NOAM VIP: 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"> 1. Check if existing key file on active NOAM (the NOAM, which is intact and was not recovered) server is valid: <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.
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 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>Note: If any errors are present, stop and contact My Oracle Support (MOS).</p>
62. <input type="checkbox"/>	Backup and archive all the databases from the recovered system	Execute Appendix A DSR Database Backup to back up the Configuration databases.
63. <input type="checkbox"/>	Recover IDIH	If IDIH were 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 any failed **SOAM and MP 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 servers.

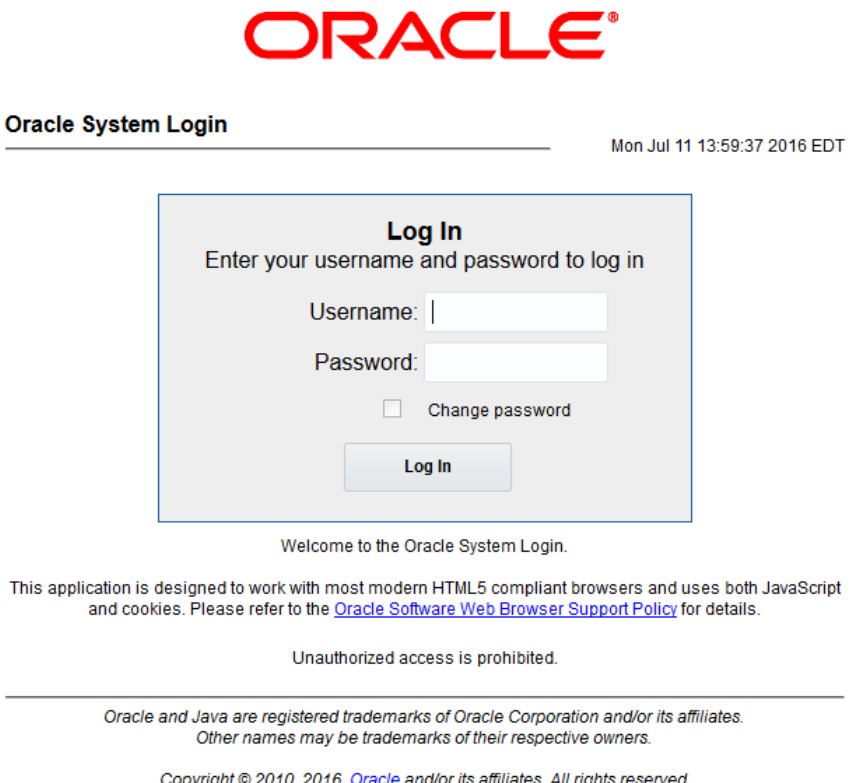
Procedure 3. Recovery Scenario 3

S T E P #		<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"/>	RMS NOAM Failure: Configure BIOS settings and update firmware	<p>If the failed server is NOT a rack mount server, skip to step 8.</p> <ol style="list-style-type: none"> 1. Configure and verify the BIOS settings by executing procedure Configure the RMS and Blade Server BIOS Settings from reference [10]. 2. Verify and/or upgrade server firmware by executing procedure Upgrade Management Server Firmware from reference [10]. <p>Note: Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.</p>
5. <input type="checkbox"/>	RMS NOAM Failure: Backups Available	<p>If the failed server is NOT a rack mount server, skip to step 8.</p> <p>This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step.</p> <p>Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media.</p> <p>If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing Restore PMAC from Backup.</p>
6. <input type="checkbox"/>	RMS NOAM Failure: Backups NOT available	<p>If the failed server is NOT a rack mount server, skip to step 8.</p> <p>This step assumes that TVOE and PMAC backups NOT are available, if the TVOE and PMAC have already been restored, skip this step.</p> <p>If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures:</p> <ol style="list-style-type: none"> 1. Configure and IPM Management Server from reference [10]. 2. Install PMAC from reference [10]. 3. Configure PMAC from reference [10]. <p>If the PMAC is NOT located on the same TVOE host as the failed NOAM, Execute the following sections/procedures:</p> <ol style="list-style-type: none"> 1. Installing TVOE on Rack Mount Server(s) from reference [10].

Procedure 3. Recovery Scenario 3

7. <input type="checkbox"/>	Recover failed aggregation/ enclosure switches, and OAs	<p>Recover failed OAs, aggregation and enclosure switches, if needed.</p> <p>Backups Available:</p> <ol style="list-style-type: none"> 1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches. <p>Backups NOT Available, execute:</p> <ol style="list-style-type: none"> 1. HP C-7000 Enclosure Configuration from reference [10] to recover and configure any failed OAs, if needed. 2. Configure Enclosure Switches from reference [10] to recover enclosure switches, if needed.
8. <input type="checkbox"/>	HP-Class Blade Failure: Configure blade server iLO, update firmware/BIOS settings	<p>If the failed server is NOT an HP C-Class Blade, skip to step 11.</p> <ol style="list-style-type: none"> 1. Execute Configure Blade Server iLO Password for Administrator Account from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing Server Blades Installation Preparation from reference [10].
9. <input type="checkbox"/>	HP-Class Blade Failure: Backups available	<p>If the failed server is NOT an OAM type HP C-Class Blade, skip to step 11.</p> <p>This step assumes TVOE backups are available. If backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> 1. Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10]. 2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers.
10. <input type="checkbox"/>	HP-Class Blade Failure: Backups NOT available	<p>If the failed server is NOT an OAM type HP C-Class Blade, skip to step 11.</p> <p>This step assumes TVOE backups are NOT are available.</p> <p>Install and configure TVOE on failed TVOE blade servers by executing section Install TVOE on Blade Servers from reference [10].</p>
11. <input type="checkbox"/>	Execute fast deployment file for NOAMs	<p>The backup fdconfig file used during the initial DSR installation is available on the PMAC, if a database backup was restored on the PMAC.</p> <p>If a backup fast deployment xml is NOT available, execute Configure NOAM Servers from reference [8].</p> <p>If a backup fast deployment xml is already present on the PMAC, execute the following procedure:</p> <ol style="list-style-type: none"> 1. Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade has been performed since initial installation). 2. Execute these commands: <pre> \$ cd /usr/TKLC/smac/etc \$ screen \$ sudo fdconfig config --file=<Created_FD_File>.xml </pre>

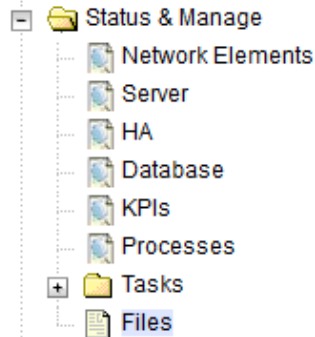
Procedure 3. Recovery Scenario 3

12. <input type="checkbox"/>	Obtain latest database backup and network configuration data	<p>Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources.</p> <p>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.</p>
13. <input type="checkbox"/>	Execute DSR installation procedure for the first NOAM	<ol style="list-style-type: none"> 1. Configure the first NOAM server by executing procedure Configure the First NOAM NE and Server from reference [8]. 2. Configure the NOAM server group by executing procedure Configure the NOAM Server Group from reference [8]. <p>Note: Use the backup copy of network configuration data and site surveys (step 2).</p>
14. <input type="checkbox"/>	NOAM GUI: Login	<p>Log into the NOAM GUI as the guiadmin user:</p> 

Procedure 3. Recovery Scenario 3

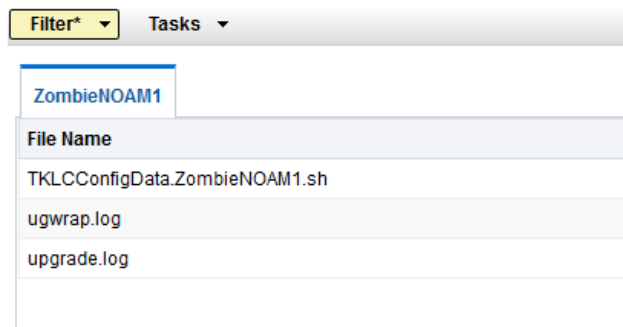
15. **NOAM GUI:**
☐ Upload the backed up database file

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

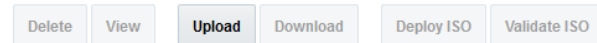


2. Select the active NOAM server.

Main Menu: Status & Manage -> Files

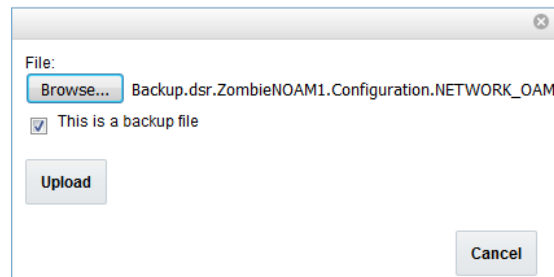


3. Click **Upload** and select the file **NO Provisioning and Configuration** file backed up after initial installation and provisioning.



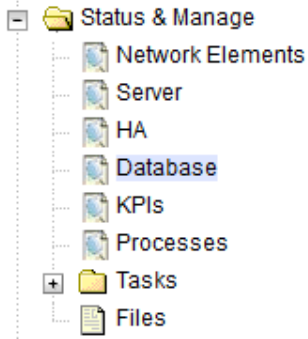
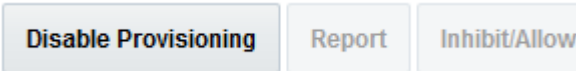

40 KB used (0.00%) of 15.7 GB available | System utilization: 867.9 MB (5.39%) of 15.7 GB available.

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

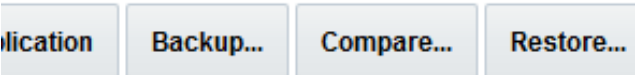
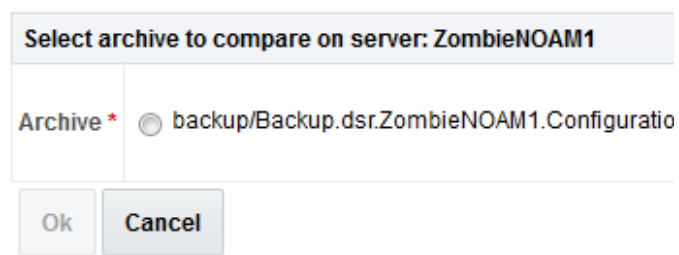
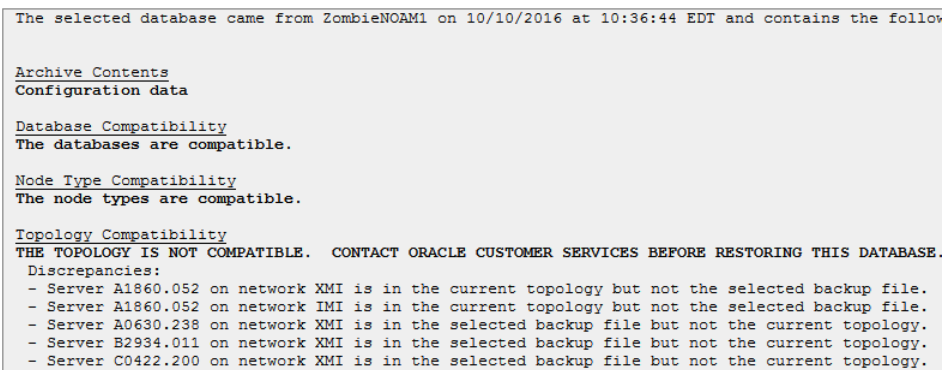


The file takes a few seconds to upload depending on the size of the backup data. The file is visible on the list of entries after the upload is complete.

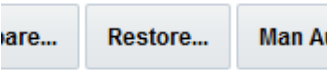
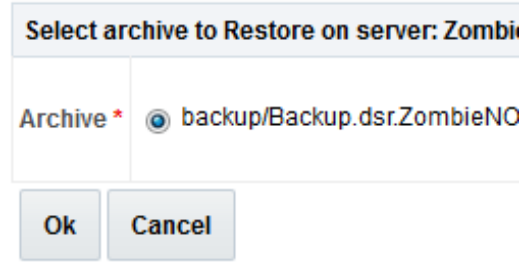
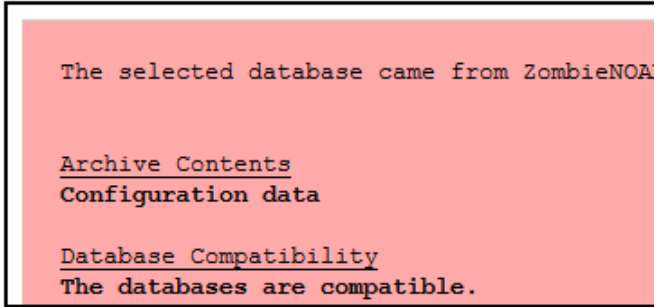
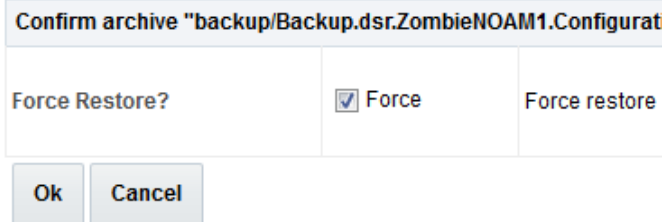
Procedure 3. Recovery Scenario 3

16.	NOAM GUI: Disable provisioning	<div>1. Navigate to Status & Manage > Database.</div> <div></div> <div>2. Click Disable Provisioning.</div> <div></div> <div>3. A confirmation window displays. Click OK to disable provisioning.</div> <div></div>
-----	--	--


Procedure 3. Recovery Scenario 3

17. <input type="checkbox"/>	NOAM GUI: Verify the archive contents and database compatibility	<ol style="list-style-type: none"> 1. Select the Active NOAM server and click Compare.  <ol style="list-style-type: none"> 2. Click the button for the restored database file uploaded as a part of Step 15 of this procedure. <p>Database Compare</p>  <ol style="list-style-type: none"> 3. Verify the output window matches the screen below. <p>Note: A database mismatch regarding the Topology Compatibility and possibly User compatibility (due to authentication) displays. 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>Database Archive Compare</p>  <p>Note: Archive Contents and Database Compatibilities must be the following:</p> <p>Archive Contents: Configuration data.</p> <p>Database Compatibility: The databases are compatible.</p> <p>Note: The following is expected output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one NOAM:</p> <p>Topology Compatibility THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.</p> <p>Note: 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"> 4. If the verification is successful, click Back.
------------------------------	--	---

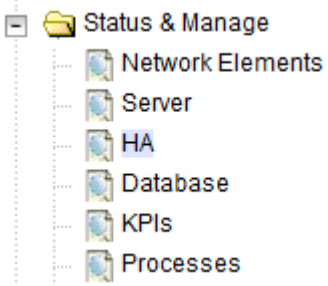
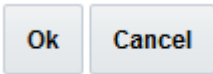
Procedure 3. Recovery Scenario 3

18.	Active NOAM: <input type="checkbox"/> Restore the database	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > Database. 2. Select the Active NOAM server and click Restore. <div data-bbox="479 357 803 430">  </div> 3. Select the backup provisioning and configuration file. <div data-bbox="479 525 998 787">  </div> 4. Click OK. 5. If you get errors related to the warnings highlighted in the previous step, that is expected. If no other errors display, mark the Force checkbox and click OK to proceed with the DB restore. <p>Database Restore Confirm</p> <p>Incompatible archive selected</p> <div data-bbox="503 1113 1153 1417">  </div> <div data-bbox="495 1428 1153 1648">  </div> <p>Note: After the restore has started, the user is logged out of XMI NO GUI since the restored Topology is old data.</p>
-----	--	---

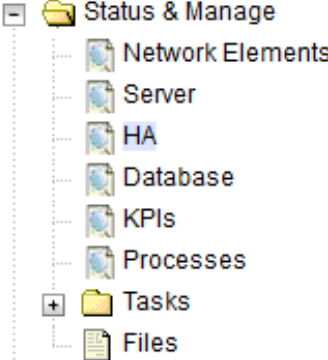
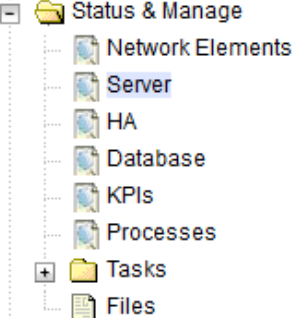

Procedure 3. Recovery Scenario 3

19. <input type="checkbox"/>	NOAM VIP GUI: Login	<ol style="list-style-type: none"> 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://<Primary_NOAM_VIP_IP_Address></div> Login as the guiadmin user: 
20. <input type="checkbox"/>	NOAM VIP GUI: Monitor and confirm database restoral	<p>Wait for 5-10 minutes for the System to stabilize with the new topology: Monitor the Info tab for Success. This indicates the restore is complete and the system is stabilized.</p> <p>Ignore the following alarms for NOAM and MP servers until all the servers are configured:</p> <ul style="list-style-type: none"> Alarms with Type Column as REPL, COLL, HA (with mate NOAM), DB (about Provisioning Manually Disabled). <p>Note: Do not pay attention to alarms until all the servers in the system are completely restored.</p> <p>Note: The Configuration and Maintenance information is in the same state it was when backed up during initial backup.</p>

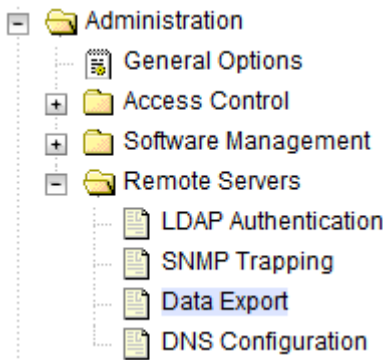
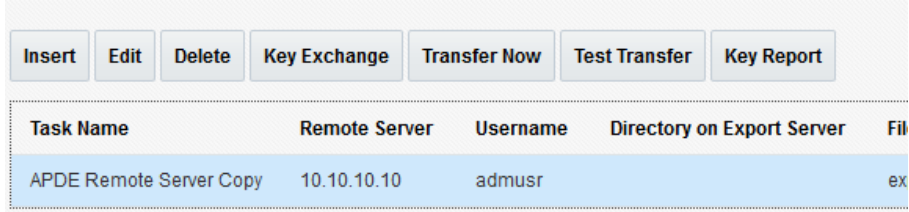
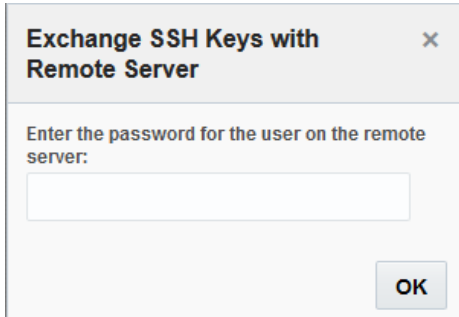
Procedure 3. Recovery Scenario 3

21. <input type="checkbox"/>	Active NOAM: Set failed servers to OOS	<ol style="list-style-type: none"> Navigate to Status & Manage > HA.  Click Edit. Modifying HA attributes <table border="1" data-bbox="487 724 1153 1155"> <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>Active Standby Spare Observer OOS</td><td>The maximum des</td></tr> </tbody> </table> Set the Max Allowed HA Role option to OOS for the failed servers. Click OK.  	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active ▼	The maximum des	ZombieNOAM2	OOS ▼	The maximum des	ZombieDRNOAM1	Active Standby Spare Observer OOS	The maximum des
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active ▼	The maximum des												
ZombieNOAM2	OOS ▼	The maximum des												
ZombieDRNOAM1	Active Standby Spare Observer OOS	The maximum des												
22. <input type="checkbox"/>	Active NOAM: Login	Log into the recovered active NOAM using SSH terminal as admusr user.												
23. <input type="checkbox"/>	NOAM VIP GUI: Recover standby NOAM	Install the second NOAM server by executing procedure Configure the Second NOAM Server , steps 3-5, 7 from reference [8]. Note: Execute step 6 if NetBackup is used.												

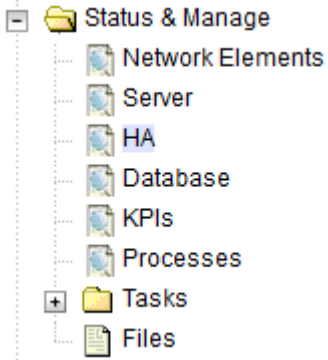
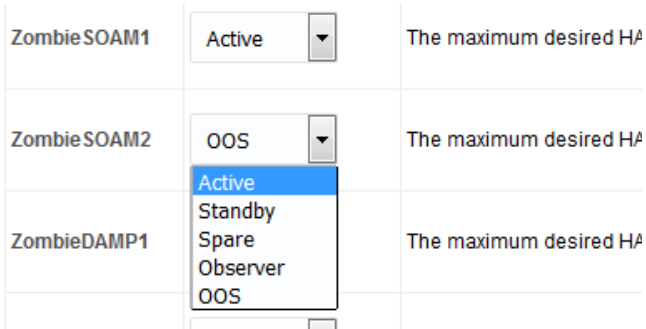
Procedure 3. Recovery Scenario 3

24. <input type="checkbox"/>	NOAM VIP GUI: Set HA on standby NOAM	<ol style="list-style-type: none"> Navigate to Status & Manage > HA.  Click Edit. Select the standby NOAM server and set it to Active. Modifying HA attributes <table border="1" data-bbox="495 850 1047 1165"> <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 Share</td><td>The maximum</td></tr> </tbody> </table> Click OK. 	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active ▼	The maximum	ZombieNOAM2	Active ▼	The maximum	ZombieDRNOAM1	Active Standby Share	The maximum
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active ▼	The maximum												
ZombieNOAM2	Active ▼	The maximum												
ZombieDRNOAM1	Active Standby Share	The maximum												
25. <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application	<ol style="list-style-type: none"> Navigate to Status & Manage > Server.  Select the recovered standby NOAM server and click Restart.  												

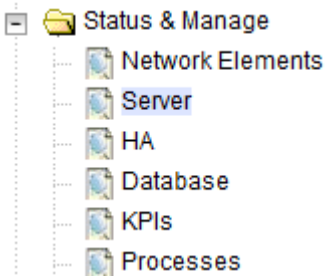

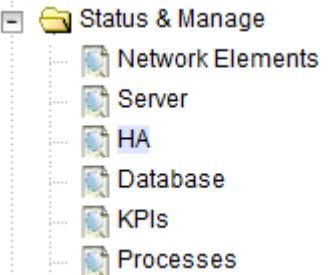
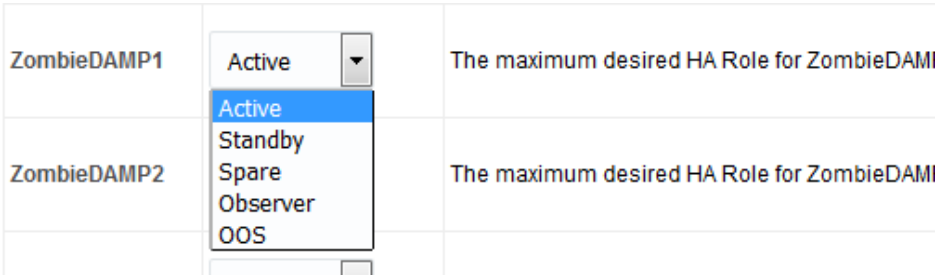
Procedure 3. Recovery Scenario 3

26. <input type="checkbox"/>	Active NOAM: Correct the recognized authority table	<div>1. Establish an SSH session to the active NOAM and login as admusr.</div> <div>2. Execute this command:</div> <div><pre>\$ sudo top.setPrimary - Using my cluster: A1789 - New Primary Timestamp: 11/09/15 20:21:43.418 - Updating A1789.022: <DSR_NOAM_B_hostname> - Updating A1789.144: <DSR_NOAM_A_hostname></pre></div>										
27. <input type="checkbox"/>	Install NetBackup client (Optional)	If NetBackup is used, execute Install NetBackup Client from reference [8].										
28. <input type="checkbox"/>	NOAM VIP GUI: Perform Keyexchange with export server	<div>1. Navigate to Administration > Remote Servers > Data Export.</div> <div></div> <div>2. Click the Task Name and click Key Exchange.</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 Password and click OK.</div> <div></div> <div>4. Repeat for each task.</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								

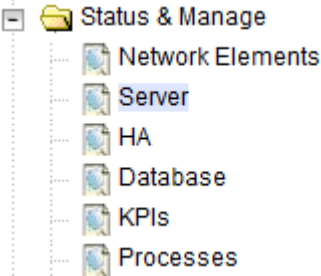

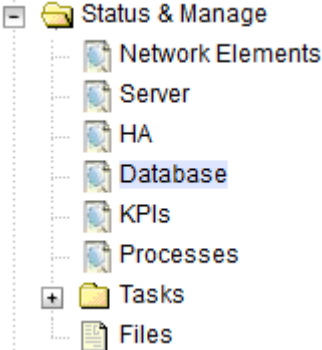
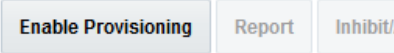
Procedure 3. Recovery Scenario 3

29. <input type="checkbox"/>	NOAM VIP GUI: Recover failed SOAM servers	<p>Recover failed SOAM servers (standby, spare) by repeating these steps for each SOAM server:</p> <ol style="list-style-type: none"> 1. Execute the Configure the SOAM Servers procedure, steps 1-3 and 5-8, from reference [8]. <p>Note: If you are using NetBackup, also execute step 10.</p> <ol style="list-style-type: none"> 2. If you are using NetBackup, execute the Install NetBackup Client procedure from reference [8].
30. <input type="checkbox"/>	NOAM VIP GUI: Set HA on standby SOAM	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > HA.  2. Click Edit.  3. Select the standby SOAM server and set it to Active. 4. Click OK.

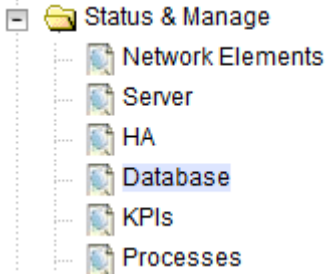

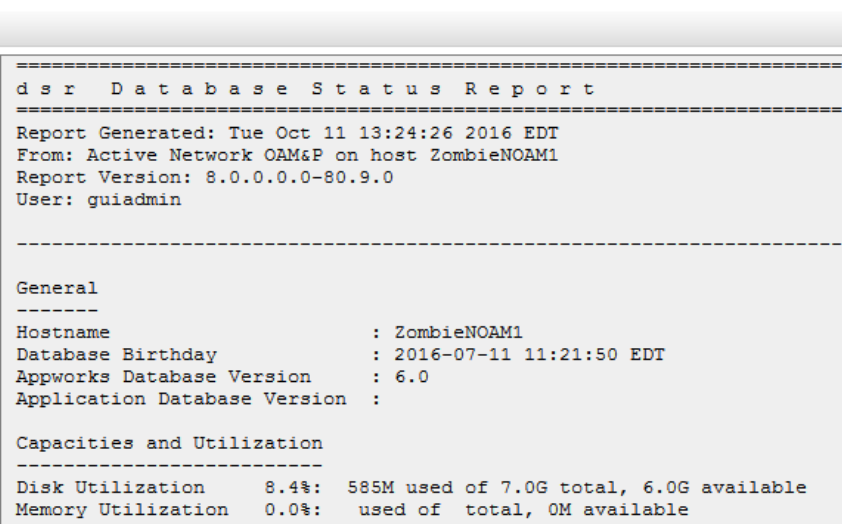
Procedure 3. Recovery Scenario 3

31. <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > Server.  2. Select the recovered standby SOAM server and click Restart. 
32. <input type="checkbox"/>	NOAM VIP GUI: Recover the C-level server (DA-MP, SBRs, IPFE, SS7-MP)	<p>Execute Configure MP Blade Servers, Steps 1, 7, 11-14, and 17, from reference [8].</p> <p>Note: Also, execute step 15 and 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>Repeat this step for any remaining failed MP servers.</p>
33. <input type="checkbox"/>	NOAM VIP GUI: Set HA on all C-level servers	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > HA.  2. Click Edit. 3. For each server whose Max Allowed HA Role is set to OOS, set it to Active.  4. Click OK.

Procedure 3. Recovery Scenario 3

34. <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application on the recovered C-level servers	<p>1. Navigate to Status & Manage > Server.</p>  <p>2. Select the recovered C-level servers and click Restart.</p> 
35. <input type="checkbox"/>	NOAM VIP GUI: Enable provisioning	<p>1. Navigate to Status & Manage > Database.</p>  <p>2. Click Enable Provisioning.</p>  <p>3. A confirmation window displays. Click OK to enable Provisioning.</p>
36. <input type="checkbox"/>	Active NOAM: Perform keyexchange between the active-NOAM and recovered servers	<p>1. Establish an SSH session to the active NOAM, login as admusr.</p> <p>2. Perform a keyexchange from the active NOAM to each recovered server:</p> <pre>\$ keyexchange admusr@<Recovered Server Hostname></pre> <p>Note: If an export server is configured, perform this step.</p>

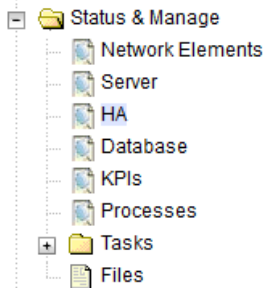
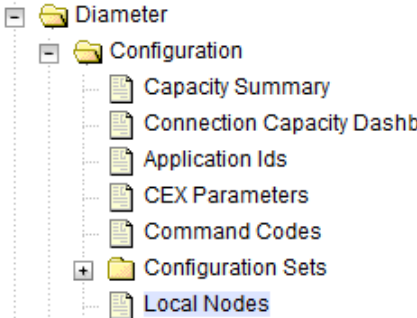
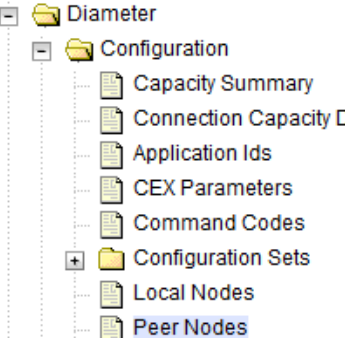
Procedure 3. Recovery Scenario 3

37. <input type="checkbox"/>	Active NOAM: Activate optional features	<p>Establish an SSH session to the active NOAM, login as admusr.</p> <p>Note For PCA Feature Activation:</p> <p>If you have PCA installed in the system being recovered, re-activate PCA by executing PCA Activation on Active NOAM server on the recovered active NOAM server and PCA Activation on Standby SOAM server on the recovered standby SOAM from [13].</p> <p>Refer to Optional Features to activate any features that were previously activated.</p> <p>Note: 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>Note: If any of the MPs are failed and recovered, then restart these MP servers after activation of the feature.</p>
38. <input type="checkbox"/>	NOAM VIP GUI: Fetch and store the database report for the newly restored data and save it	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > Database.  2. Select the active NOAM server and click Report.  <p>The following screen is displayed:</p> <p>Main Menu: Status & Manage -> Database [Report]</p>  <pre> dsr Database Status Report ===== Report Generated: Tue Oct 11 13:24:26 2016 EDT From: Active Network OAM&P on host ZombieNOAM1 Report Version: 8.0.0.0-80.9.0 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 </pre> <ol style="list-style-type: none"> 3. Click Save and save the report to your local machine.

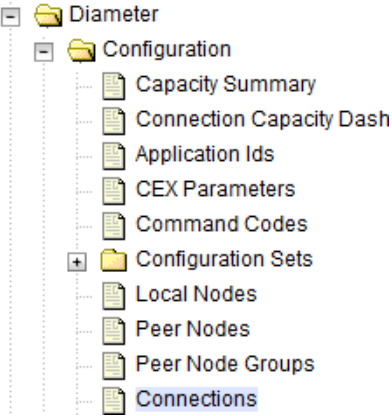
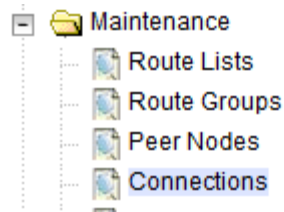
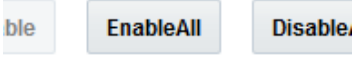
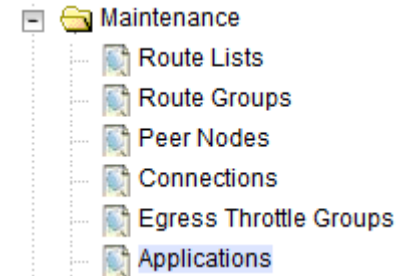
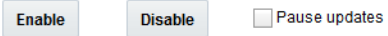
Procedure 3. Recovery Scenario 3

39. <div></div>	Active NOAM: Verify replication between servers	<div>1. Log into the active NOAM using SSH terminal as admusr.</div> <div>2. Execute this command:</div> <div><div>\$ sudo irepstat -m</div></div> <div>Example output:</div> <div>-- Policy 0 ActStb [DbReplication] ----- RDU06-MP1 -- Stby BC From RDU06-SO1 Active 0 0.50 ^0.17%cpu 42B/s A=none CC From RDU06-MP2 Active 0 0.10 ^0.17 0.88%cpu 32B/s A=none RDU06-MP2 -- Active BC From RDU06-SO1 Active 0 0.50 ^0.10%cpu 33B/s A=none CC To RDU06-MP1 Active 0 0.10 0.08%cpu 20B/s A=none RDU06-NO1 -- Active AB To RDU06-SO1 Active 0 0.50 1%R 0.03%cpu 21B/s RDU06-SO1 -- Active AB From RDU06-NO1 Active 0 0.50 ^0.04%cpu 24B/s BC To RDU06-MP1 Active 0 0.50 1%R 0.04%cpu 21B/s BC To RDU06-MP2 Active 0 0.50 1%R 0.07%cpu 21B/s</div>																																																
40. <div></div>	NOAM VIP GUI: Verify the database states	<div>1. Navigate to Status & Manager > Database.</div> <div><div><div><div></div><div>Status & 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>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:</div> <div><table><tr><th>Network Element</th><th>Server</th><th>Role</th><th>OAM Max HA Role</th></tr><tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM1</td><td>Network OAM&P</td><td>Active</td></tr><tr><td>ZombieNOAM</td><td>ZombieNOAM2</td><td>Network OAM&P</td><td>Standby</td></tr><tr><td>ZombieSOAM</td><td>ZombieSOAM2</td><td>System OAM</td><td>N/A</td></tr><tr><td>ZombieNOAM</td><td>ZombieNOAM1</td><td>Network OAM&P</td><td>Active</td></tr><tr><td>ZombieSOAM</td><td>ZombieSOAM1</td><td>System OAM</td><td>Active</td></tr><tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM2</td><td>Network OAM&P</td><td>Standby</td></tr><tr><td>ZombieSOAM</td><td>ZombieDAMP2</td><td>MP</td><td>Standby</td></tr><tr><td>ZombieSOAM</td><td>ZombieSS7MP2</td><td>MP</td><td>Active</td></tr><tr><td>ZombieSOAM</td><td>ZombieSS7MP1</td><td>MP</td><td>Active</td></tr><tr><td>ZombieSOAM</td><td>ZombieIPFE1</td><td>MP</td><td>Active</td></tr><tr><td>ZombieSOAM</td><td>ZombieIPFE2</td><td>MP</td><td>Active</td></tr></table></div>	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
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																																															

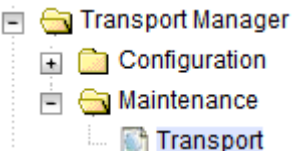

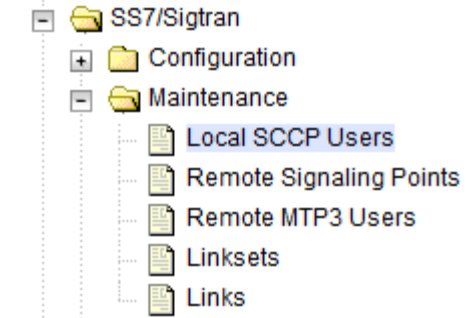

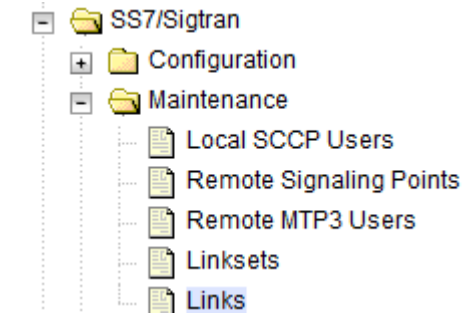
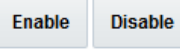
Procedure 3. Recovery Scenario 3

41. <input type="checkbox"/>	NOAM VIP GUI: Verify the HA status	<div>1. Navigate to Status & Manage > HA.</div> <div></div> <div>2. Select the row for all of the servers.</div> <div>3. Verify the HA Role is either Active or Standby.</div> <div><table><thead><tr><th>Hostname</th><th>OAM HA Role</th><th>Application HA Role</th><th>Max Allowed HA Role</th></tr></thead><tbody><tr><td>ZombieNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieDRNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieDRNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieSOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr><tr><td>ZombieSOAM2</td><td>Standby</td><td>N/A</td><td>Standby</td></tr></tbody></table></div>	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																											
42. <input type="checkbox"/>	SOAM VIP GUI: Verify the local node info	<div>1. Navigate to Diameter > Configuration > Local Node.</div> <div></div> <div>2. Verify all the local nodes are shown.</div>																												
43. <input type="checkbox"/>	SOAM VIP GUI: Verify the peer node info	<div>1. Navigate to Diameter > Configuration > Peer Node.</div> <div></div> <div>2. Verify all the peer nodes are shown.</div>																												

Procedure 3. Recovery Scenario 3

44. <input type="checkbox"/>	SOAM VIP GUI: Verify the connections info	<ol style="list-style-type: none"> 1. Navigate to Diameter > Configuration > Connections.  2. Verify all the connections are shown.
45. <input type="checkbox"/>	SOAM VIP GUI: Enable Connections, if needed	<ol style="list-style-type: none"> 1. Navigate to Diameter > Maintenance > Connections.  2. Select each connection and click Enable. Alternatively, you can enable all the connections by clicking EnableAll.  3. Verify the Operational State is Available. <p>Note: If a disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution</p>
46. <input type="checkbox"/>	SOAM VIP GUI: Enable optional features	<ol style="list-style-type: none"> 1. Navigate to Diameter > Maintenance > Applications.  2. Select the optional feature application configured in step 36. . 3. Click Enable. 

Procedure 3. Recovery Scenario 3

47. <input type="checkbox"/>	SOAM VIP GUI: Re-enable transports, if needed	<ol style="list-style-type: none"> 1. Navigate to Transport Manager > Maintenance > Transport.  2. Select each transport and click Enable.  3. Verify the Operational Status for each transport is Up.
48. <input type="checkbox"/>	SOAM VIP GUI: Re-enable MAPIWF application, if needed	<ol style="list-style-type: none"> 1. Navigate to SS7/Sigtran > Maintenance > Local SCCP Users.  2. Click the Enable button corresponding to MAPIWF Application Name.  3. Verify the SSN Status is Enabled.
49. <input type="checkbox"/>	SOAM VIP GUI: Re-enable links, if needed	<ol style="list-style-type: none"> 1. Navigate to SS7/Sigtran > Maintenance > Links.  2. Click Enable for each link.  3. Verify the Operational Status for each link is Up.

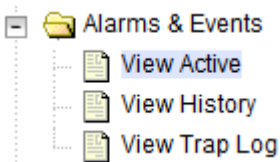
Procedure 3. Recovery Scenario 3

50.	NOAM VIP: <input type="checkbox"/> 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"> 1. Establish an SSH session to the NOAM VIP and login as admusr. 2. Check if all the servers in the topology are accessible: <pre>\$ /usr/TKLC/dpi/bin/sharedKrevo -checkAccess</pre> <p>Example output:</p> <pre>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>Note: If any of the servers are not accessible, stop and contact My Oracle Support (MOS).</p>
-----	--	--

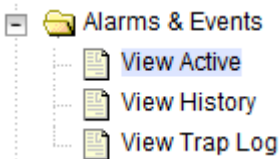
Procedure 3. Recovery Scenario 3

51. <input type="checkbox"/>	SOAM VIP: 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"> 1. Establish an SSH session to any active SOAM that remained intact and operational (Log into an active SOAM server that was not recovered or did not need recovery). 2. Login as admusr. 3. Check if the existing key file on active SOAM server is valid: <pre>\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -validate</pre> <p>Example output:</p> <pre>[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]\$</pre> <p>Note: If output of above command shows that existing key file is not valid, contact My Oracle Support (MOS)</p> <ol style="list-style-type: none"> 4. Establish an SSH session to the active SOAM, login as admusr. 5. Copy the key file to active NOAM: <pre>\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -copyKey -destServer <Active NOAM server name></pre>
------------------------------	--	---

Procedure 3. Recovery Scenario 3

52. <input type="checkbox"/>	NOAM VIP: Copy key file to all the servers in topology (RADIUS only)	<ol style="list-style-type: none"> 1. Establish an SSH session to any of the active NOAM. Login as admusr. 2. Copy the key file to all the servers in the topology: <div data-bbox="527 338 1419 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="527 472 1425 850" style="background-color: black; color: white; 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="527 856 1419 905" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>\$./sharedKrevo -updateData</pre> </div> <p>Example output:</p> <div data-bbox="527 951 1425 1249" style="background-color: black; color: white; padding: 5px; margin: 10px 0;"> <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>
53. <input type="checkbox"/>	SOAM VIP GUI: Examine all alarms	<ol style="list-style-type: none"> 1. Navigate to Alarms & Events > View Active. <div data-bbox="505 1312 782 1472" style="margin: 10px 0;">  </div> 2. Examine all active alarms and refer to the on-line help on how to address them. <p>If needed, contact My Oracle Support (MOS).</p>

Procedure 3. Recovery Scenario 3

54. <input type="checkbox"/>	NOAM VIP GUI: Examine all alarms	<ol style="list-style-type: none"> 1. Log into the NOAM VIP if not already logged in. 2. Navigate to Alarms & Events > View Active.  3. Examine all active alarms and refer to the on-line help on how to address them. <p>If needed, contact My Oracle Support (MOS).</p>
55. <input type="checkbox"/>	Restore GUI usernames and passwords	If applicable, execute Resolve User Credential Issues after Database Restore to recover the user and group information restored.
56. <input type="checkbox"/>	Backup and archive all the databases from the recovered system	Execute DSR Database Backup to back up the Configuration databases.
57. <input type="checkbox"/>	Recover IDIH	If IDIH were affected, refer to IDIH Disaster Recovery to perform disaster recovery on IDIH.
58. <input type="checkbox"/>	SNMP workaround	<p>Refer SNMP Configuration to configure SNMP as a workaround in the following cases:</p> <ol style="list-style-type: none"> 1. If SNMP is not configured in DSR. 2. If SNMP is already configured and SNMPv3 is selected as enabled version.


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:

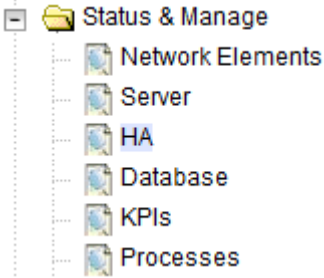

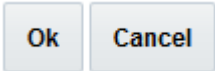
- Recover standby NOAM server by recovering base hardware and software
 - Recover the base hardware
 - Recover the software
- The database is intact at the active NOAM server and does not require restoration at the standby NOAM server
 - Recover any failed SO and MP servers by recovering base hardware 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 SO and MP servers

- Re-apply signaling networks configuration if the failed blade is an MP

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 SNMP Configuration to configure SNMP as a workaround in the following cases:</p> <ol style="list-style-type: none"> 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 section.
3. <input type="checkbox"/>	NOAM VIP GUI: Login	<ol style="list-style-type: none"> 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="516 856 1320 903" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> http://<Primary_NOAM_VIP_IP_Address> </div> 2. Login as the guiadmin user: <div data-bbox="479 972 1425 1732" style="text-align: center;">  <p>Oracle System Login Tue Jun 7 13:49:06 2016 EDT</p> <hr/> <div data-bbox="652 1182 1252 1549" style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 80%;"> <p>Log In 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><small>Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</small></p> <p><small>Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.</small></p> </div>


Procedure 4. Recovery Scenario 4

<p>4.</p> <p><input type="checkbox"/></p>	<p>Active NOAM: Set failed servers to OOS</p>	<ol style="list-style-type: none"> Navigate to Status & Manage > HA.  <ol style="list-style-type: none"> Click Edit. <p>Modifying HA attributes</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 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 to OOS for the failed servers.</p> <p>4. Select OK.</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.</p> <p><input type="checkbox"/></p>	<p>RMS NOAM Failure: Configure BIOS settings and update firmware</p>	<p>If the failed server is NOT a rack mount server, skip to step 9.</p> <ol style="list-style-type: none"> Configure and verify the BIOS settings by executing procedure Configure the RMS and Blade Server BIOS Settings from reference [10]. Verify and/or upgrade server firmware by executing procedure Upgrade Management Server Firmware from reference[10]. <p>Note: Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.</p>												
<p>6.</p> <p><input type="checkbox"/></p>	<p>RMS NOAM Failure: Backups available</p>	<p>If the failed server is NOT a rack mount server, skip to step 9.</p> <p>This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media. If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing Restore PMAC from Backup. 												

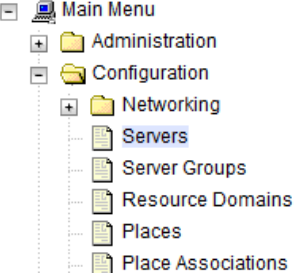
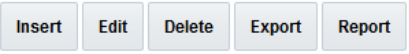
Procedure 4. Recovery Scenario 4

7. <input type="checkbox"/>	RMS NOAM Failure: Backups NOT available	<p>This step assumes that TVOE and PMAC backups are NOT available, if the TVOE and PMAC have already been restored, skip this step.</p> <p>If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures:</p> <ol style="list-style-type: none"> 1. Configure and IPM Management Server from reference [10]. 2. Install PMAC from reference [10]. 3. Configure PMAC from reference [10]. <p>If the PMAC is NOT located on the same TVOE host as the failed NOAM, execute the following sections/procedures.</p> <ol style="list-style-type: none"> 1. Installing TVOE on Rack Mount Server(s) from reference [10].
8. <input type="checkbox"/>	Recover failed aggregation/ enclosure switches, and OAs	<p>Recover failed OAs, aggregation and enclosure switches, if needed.</p> <p>Backups Available:</p> <ol style="list-style-type: none"> 1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches <p>Backups NOT available, execute:</p> <ol style="list-style-type: none"> 1. HP C-7000 Enclosure Configuration from reference [10] to recover and configure any failed OAs, if needed. 2. Configure Enclosure Switches from reference [10] to recover enclosure switches, if needed.
9. <input type="checkbox"/>	HP-Class Blade Failure: Configure blade server iLO, update firmware/BIOS settings	<p>If the failed server is NOT an HP C-Class Blade, skip to step 12.</p> <ol style="list-style-type: none"> 1. Configure Blade Server iLO Password for Administrator Account from reference [10]. 2. Verify/Update blade server firmware and BIOS settings by executing Server Blades Installation Preparation from reference [10]
10. <input type="checkbox"/>	HP-Class Blade Failure: Backups available	<p>If the failed server is NOT an OAM type HP C-Class Blade, skip to step 13.</p> <p>This step assumes that TVOE backups are available, if backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> 1. Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10]. 2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers.
11. <input type="checkbox"/>	HP-Class Blade Failure: Backups NOT available	<p>If the failed server is NOT an OAM HP C-Class Blade, skip to step 13.</p> <p>This step assumes that TVOE backups are NOT available</p> <ol style="list-style-type: none"> 1. Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10]. 2. Configure the NOAM and/or SOAM failed TVOE server blades by executing Configure SOAM TVOE Server Blades from reference [8]. <p>Note: Although the title of the procedure is related to SOAMs only, execute this procedure for any failed NOAMs located on TVOE server blades.</p>

Procedure 4. Recovery Scenario 4

12. <input type="checkbox"/>	Create VMs	Execute Create NOAM/SOAM Virtual Machines to create the NOAM and SOAM VMs on failed TVOE servers.
13. <input type="checkbox"/>	IPM and install DSR application on failed guest/servers	<ol style="list-style-type: none"> 1. Execute IPM Blades and VMs for the failed SOAM VMs and MP blades from reference [8]. 2. Execute Install the Application Software for the failed NOAM and SOAM VMs and MP blades from reference [8].
14. <input type="checkbox"/>	Install NetBackup client (Optional)	If NetBackup is used, execute Install NetBackup Client from reference [8].
15. <input type="checkbox"/>	NOAM VIP GUI: Login	<ol style="list-style-type: none"> 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;"> <code>http://<Primary_NOAM_VIP_IP_Address></code> </div> 2. Login as the guiadmin user: <div style="text-align: center; margin: 10px 0;">  </div> <div style="text-align: center; margin: 10px 0;"> Oracle System Login </div> <div style="text-align: right; margin: 10px 0;">Tue Jun 7 13:49:06 2016 EDT</div> <div style="border: 1px solid black; padding: 10px; margin: 10px 0; text-align: center;"> <p>Log In</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>
16. <input type="checkbox"/>	Exchange SSH keys between PMAC and failed NOAM server	<ol style="list-style-type: none"> 1. Use the PMAC GUI to determine the Control Network IP address of the failed NOAM server VM. From the PMAC GUI, navigate to Software > Software Inventory. 2. Note the IP address for the failed NOAM server VM. 3. Log into the PMAC terminal as the admusr. 4. From a terminal window connection on the PMAC as the admusr user, exchange SSH keys for admusr between the PMAC and the failed NOAM server VM control network IP address. When prompted for the password, enter the password for the admusr user of the NOAM server. <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <code>\$ keyexchange admusr@<NO2_Control_IP Address></code> </div> <p>Note: If Key exchange fails, edit /home/admusr/.ssh/known_hosts and remove blank lines, and retry the keyexchange commands.</p>

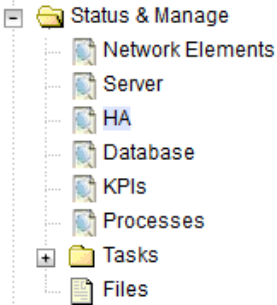
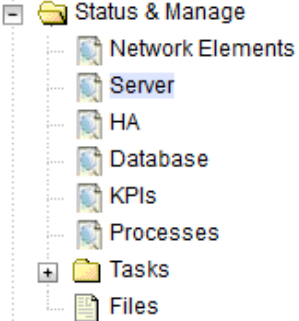

Procedure 4. Recovery Scenario 4

17. <input type="checkbox"/>	NOAM VIP GUI: Export the Initial configuration	<ol style="list-style-type: none"> 1. Navigate to Configuration > Servers.  2. From the GUI screen, select the failed NOAM server and click Export to generate the initial configuration data for that server. 
18. <input type="checkbox"/>	NOAM VIP: Copy configuration file to failed NOAM server	<ol style="list-style-type: none"> 1. Obtain a terminal session to the NOAM VIP, login as the admusr. 2. Use the awpushcfg utility to copy the configuration file created in the previous step from the <code>/var/TKLC/db/filemgmt</code> directory on the active NOAM to the failed NOAM server, using the Control network IP address for the failed NOAM VM. The configuration file has a filename like TKLCConfigData.<hostname>.sh. <pre>\$ sudo awpushcfg</pre> 3. The awpushcfg utility is interactive, so the user is prompted for the following: <ul style="list-style-type: none"> • IP address of the local PMAC server: Use the local control network address from the PMAC. • Username: Use admusr • Control network IP address for the target server: In this case, enter the control IP for the failed NOAM VM). • Hostname of the target server: Enter the server name from Step 17.
19. <input type="checkbox"/>	Failed NOAM Server: Verify awpushcfg was called and reboot the server	<ol style="list-style-type: none"> 1. Establish an SSH session to the failed NOAM server, login as the admusr user. 2. The automatic configuration daemon looks for the file named TKLCConfigData.sh in the <code>/var/tmp</code> directory, implements the configuration in the file, and asks the user to reboot the server. 3. Verify awpushcfg was called by checking the following file <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> Verify this message displays: <pre>[SUCCESS] script completed successfully!</pre> 4. Now reboot the server: <pre>\$ sudo init 6</pre> 5. Wait for the server to reboot

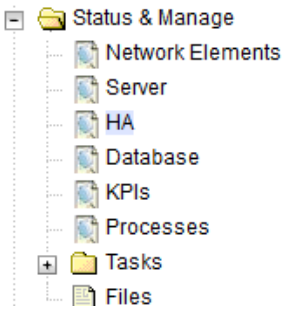
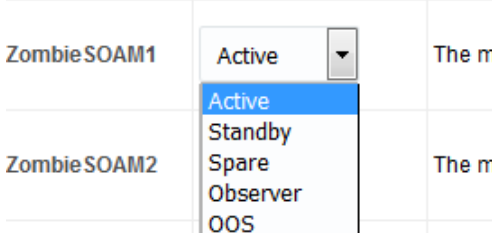
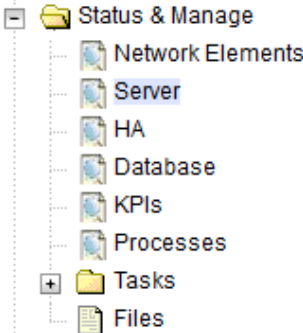

Procedure 4. Recovery Scenario 4

20. <input type="checkbox"/>	Failed NOAM Server: Configure networking for dedicated NetBackup interface (Optional)	<p>Note: Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.</p> <p>Obtain a terminal window to the failed NOAM server, logging in as the admusr.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP_Address> --netmask=<NO2_NetBackup_NetMask></pre> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NO1_NetBackup_Network_ID> --netmask=<NO2_NetBackup_NetMask> --gateway=<NO2_NetBackup_Gateway_IP_Address></pre>
21. <input type="checkbox"/>	Failed NOAM Server: Verify server health	<p>Execute this command on the 2nd NOAM server and make sure no errors are returned:</p> <pre>\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

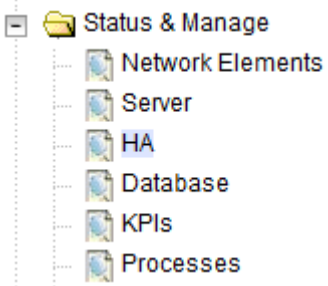
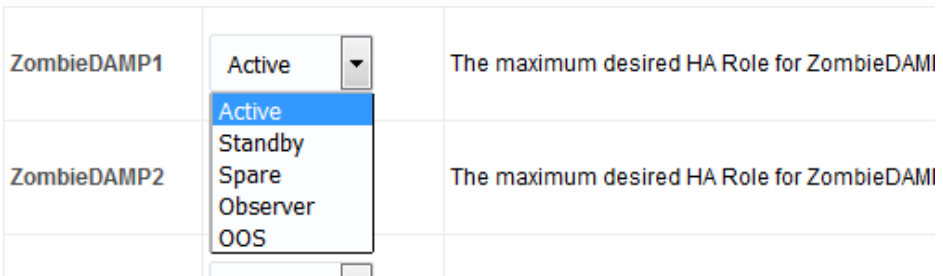
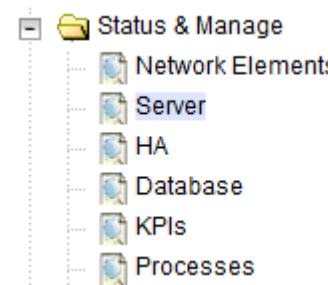

Procedure 4. Recovery Scenario 4

22. <input type="checkbox"/>	NOAM VIP GUI: Set HA on standby NOAM	<ol style="list-style-type: none"> Navigate to Status & Manage > HA.  Click Edit. Select the standby NOAM server and set it to Active. Modifying HA attributes <table border="1" data-bbox="480 772 954 1045"> <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>Standby</td><td>The maximum</td></tr> </tbody> </table> Click OK. 	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active	The maximum	ZombieNOAM2	Active	The maximum	ZombieDRNOAM1	Standby	The maximum
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active	The maximum												
ZombieNOAM2	Active	The maximum												
ZombieDRNOAM1	Standby	The maximum												
23. <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application	<ol style="list-style-type: none"> Navigate to Status & Manage > Server.  Select the recovered standby NOAM server and click Restart.  												
24. <input type="checkbox"/>	NOAM VIP GUI: Recover failed SOAM servers	<p>Recover failed SOAM servers (standby, spare) by repeating these steps for each SOAM server:</p> <ol style="list-style-type: none"> Execute Configure the SOAM Servers, steps 1-3 and 5-8, from reference [8]. Note: If you are using NetBackup, also execute step 10. If you are using NetBackup, execute Install NetBackup Client from reference [8]. 												

Procedure 4. Recovery Scenario 4

25. <input type="checkbox"/>	NOAM VIP GUI: Set HA on standby SOAM	<ol style="list-style-type: none"> Navigate to Status & Manage > HA.  Click Edit. Select the SOAM server and set it to Active.  Click OK.
26. <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application	<ol style="list-style-type: none"> Navigate to Status & Manage > Server.  Select the recovered SOAM server and click Restart. 
27. <input type="checkbox"/>	NOAM VIP GUI: Recover the C-level server (DA-MP, SBRs, IPFE, SS7-MP)	<ol style="list-style-type: none"> Execute Configure MP Blade Servers, steps 1, 7, 11-14, and 17, from reference [8]. <p>Note: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.</p> Repeat this step for any remaining failed MP servers.

Procedure 4. Recovery Scenario 4

28. <input type="checkbox"/>	NOAM VIP GUI: Set HA on all C-level servers	<p>1. Navigate to Status & Manage > HA.</p>  <p>2. Click Edit.</p> <p>3. For each server whose Max Allowed HA Role is set to OOS, set it to Active.</p>  <p>4. Click OK.</p>
29. <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application	<p>1. Navigate to Status & Manage > Server.</p>  <p>2. Select the recovered C-level servers and click Restart.</p> 
30. <input type="checkbox"/>	Active NOAM: Login	Log into the recovered active NOAM using SSH terminal as admusr user.
31. <input type="checkbox"/>	Active NOAM: Perform key exchange between the active-NOAM and recovered servers	<p>1. Establish an SSH session to the active NOAM, login as admusr.</p> <p>2. Perform a keyexchange from the active NOAM to each recovered server:</p> <pre>\$ keyexchange admusr@<Recovered Server Hostname></pre>

Procedure 4. Recovery Scenario 4

32. <input type="checkbox"/>	Active NOAM: Activate optional features	<p>Establish an SSH session to the active NOAM, login as admusr.</p> <p>Note For PCA Feature Activation:</p> <p>If you have PCA installed in the system being recovered, re-activate PCA by executing PCA Activation on Standby NOAM Server on the recovered standby NOAM server and PCA Activation on Standby SOAM server on the recovered standby SOAM server from [13].</p> <p>Refer to Optional Features to activate any features that were previously activated.</p> <p>Note: 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>Note: If any of the MPs are failed and recovered, then restart these MP servers after activation of the feature.</p>
33. <input type="checkbox"/>	MP Servers: Disable SCTP auth flag (DSR Only)	<p>DSR Only, SDS Skip This Step.</p> <p>For SCTP connections without DTLS enabled, refer to Enable/Disable DTLS Appendix from reference [14].</p> <p>Execute this procedure on all failed MP servers.</p>

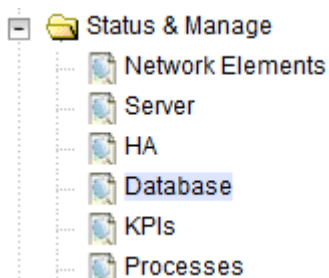
Procedure 4. Recovery Scenario 4

34.

**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 is displayed:

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 :

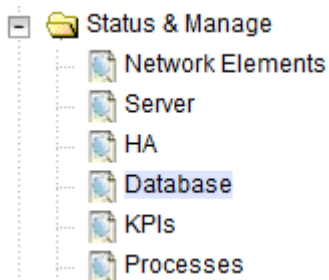
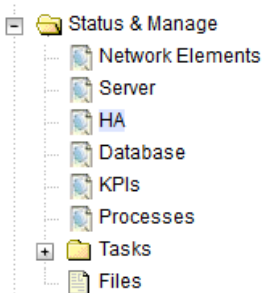
Capacities and Utilization
-----
Disk Utilization      8.4%:  585M used of 7.0G total, 6.0G available
Memory Utilization   0.0%:   used of  total, 0M available
=====
```

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

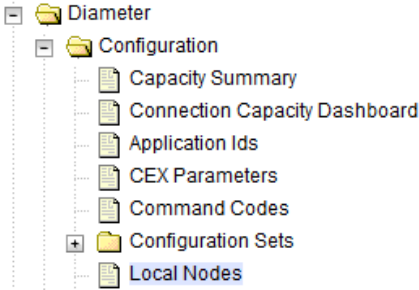
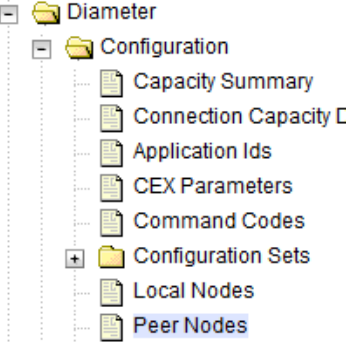
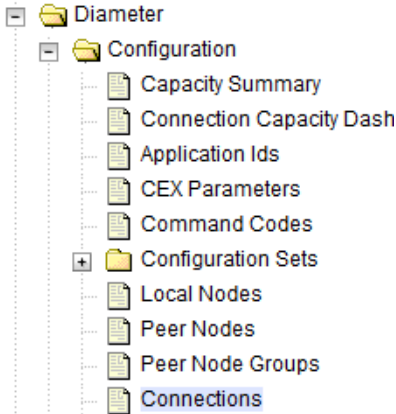
Procedure 4. Recovery Scenario 4

35. <input type="checkbox"/>	Active NOAM: Verify replication between servers	<div>1. Log into the active NOAM using SSH terminal as admusr.</div> <div>2. Execute this command:</div> <div><pre>\$ sudo irepstat -m</pre></div> <div>Example output:</div> <div><pre>-- Policy 0 ActStb [DbReplication] ----- RDU06-MP1 -- Stby BC From RDU06-SO1 Active 0 0.50 ^0.17%cpu 42B/s A=none CC From RDU06-MP2 Active 0 0.10 ^0.17 0.88%cpu 32B/s A=none RDU06-MP2 -- Active BC From RDU06-SO1 Active 0 0.50 ^0.10%cpu 33B/s A=none CC To RDU06-MP1 Active 0 0.10 0.08%cpu 20B/s A=none RDU06-NO1 -- Active AB To RDU06-SO1 Active 0 0.50 1%R 0.03%cpu 21B/s RDU06-SO1 -- Active AB From RDU06-NO1 Active 0 0.50 ^0.04%cpu 24B/s BC To RDU06-MP1 Active 0 0.50 1%R 0.04%cpu 21B/s BC To RDU06-MP2 Active 0 0.50 1%R 0.07%cpu 21B/s</pre></div>
---------------------------------	---	--

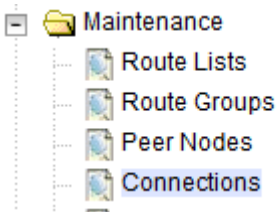
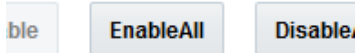
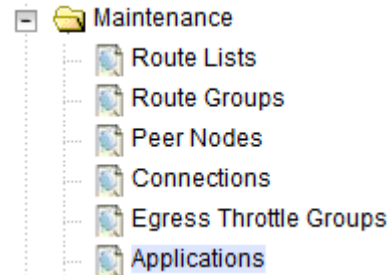
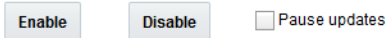
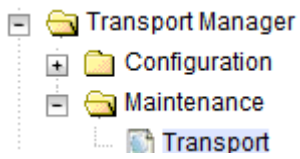
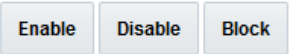
Procedure 4. Recovery Scenario 4

36. <input type="checkbox"/>	NOAM VIP GUI: Verify the database states	<ol style="list-style-type: none"> Navigate to Status & Manager > Database.  Verify the OAM Max HA Role is either Active or Standby for NOAM and SOAM and Application Max HA Role for MPs is Active, and that the status is Normal. <table border="1"> <thead> <tr> <th>Network Element</th><th>Server</th><th>Role</th><th>OAM Max HA Role</th></tr> </thead> <tbody> <tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM1</td><td>Network OAM&P</td><td>Active</td></tr> <tr><td>ZombieNOAM</td><td>ZombieNOAM2</td><td>Network OAM&P</td><td>Standby</td></tr> <tr><td>ZombieSOAM</td><td>ZombieSOAM2</td><td>System OAM</td><td>N/A</td></tr> <tr><td>ZombieNOAM</td><td>ZombieNOAM1</td><td>Network OAM&P</td><td>Active</td></tr> <tr><td>ZombieSOAM</td><td>ZombieSOAM1</td><td>System OAM</td><td>Active</td></tr> <tr><td>ZombieDRNOAM</td><td>ZombieDRNOAM2</td><td>Network OAM&P</td><td>Standby</td></tr> <tr><td>ZombieSOAM</td><td>ZombieDAMP2</td><td>MP</td><td>Standby</td></tr> <tr><td>ZombieSOAM</td><td>ZombieSS7MP2</td><td>MP</td><td>Active</td></tr> <tr><td>ZombieSOAM</td><td>ZombieSS7MP1</td><td>MP</td><td>Active</td></tr> <tr><td>ZombieSOAM</td><td>ZombieIPFE1</td><td>MP</td><td>Active</td></tr> <tr><td>ZombieSOAM</td><td>ZombieIPFE2</td><td>MP</td><td>Active</td></tr> </tbody> </table> 	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
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																																															
37. <input type="checkbox"/>	NOAM VIP GUI: Verify the HA status	<ol style="list-style-type: none"> Navigate to Status & Manager > HA.  Select the row for all of the servers. Verify the HA Role is either Active or Standby. <table border="1"> <thead> <tr> <th>Hostname</th><th>OAM HA Role</th><th>Application HA Role</th><th>Max Allowed HA Role</th></tr> </thead> <tbody> <tr><td>ZombieNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr> <tr><td>ZombieNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr> <tr><td>ZombieDRNOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr> <tr><td>ZombieDRNOAM2</td><td>Standby</td><td>N/A</td><td>Active</td></tr> <tr><td>ZombieSOAM1</td><td>Active</td><td>N/A</td><td>Active</td></tr> <tr><td>ZombieSOAM2</td><td>Standby</td><td>N/A</td><td>Standby</td></tr> </tbody> </table> 	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																																															

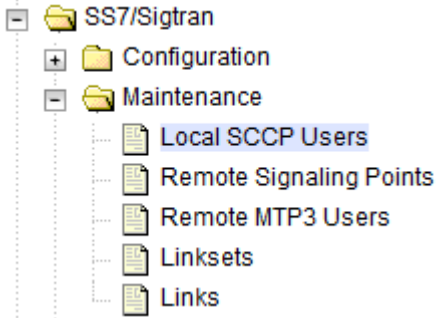

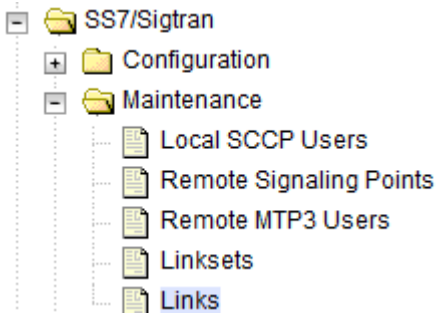
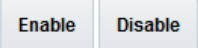
Procedure 4. Recovery Scenario 4

38. <input type="checkbox"/>	SOAM VIP GUI: Verify the local node info	1. Navigate to Diameter > Configuration > Local Nodes .  2. Verify all the connections are shown.
39. <input type="checkbox"/>	SOAM VIP GUI: Verify the peer node info	1. Navigate to Diameter > Configuration > Peer Node .  2. Verify all the peer nodes are shown.
40. <input type="checkbox"/>	SOAM VIP GUI: Verify the connections info	1. Navigate to Diameter > Configuration > Connections .  2. Verify all the connections are shown.

Procedure 4. Recovery Scenario 4

41. <input type="checkbox"/>	SOAM VIP GUI: Enable connections, if needed	<ol style="list-style-type: none"> 1. Navigate to Diameter > Maintenance > Connections.  2. Select each connection and click Enable. Alternatively, you can enable all the connections by clicking EnableAll.  3. Verify the Operational State is Available. Note: If a Disaster Recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution.
42. <input type="checkbox"/>	SOAM VIP GUI: Enable optional features	<ol style="list-style-type: none"> 1. Navigate to Diameter > Maintenance > Applications.  2. Select the optional feature application configured in step 32. 3. Click Enable. 
43. <input type="checkbox"/>	SOAM VIP GUI: Re-enable transports, if needed (Applicable ONLY for DSR 6.0+)	<ol style="list-style-type: none"> 1. Navigate to Transport Manager > Maintenance > Transport.  2. Select each transport and click Enable.  3. Verify the Operational Status for each transport is Up.

Procedure 4. Recovery Scenario 4

44. <input type="checkbox"/>	SOAM VIP GUI: Re-enable MAPIWF application, if needed	<ol style="list-style-type: none"> 1. Navigate to SS7/Sigtran > Maintenance > Local SCCP Users.  2. Click the Enable button corresponding to MAPIWF Application Name.  3. Verify the SSN Status is Enabled.
45. <input type="checkbox"/>	SOAM VIP GUI: Re-enable links, if needed	<ol style="list-style-type: none"> 1. Navigate to SS7/Sigtran > Maintenance > Links.  <p>Click Enable for each link.</p>  <ol style="list-style-type: none"> 2. Verify the Operational Status for each link is Up.

Procedure 4. Recovery Scenario 4

46. <input type="checkbox"/>	NOAM VIP: 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"> 1. Establish an SSH session to the NOAM VIP and login as admusr. 2. Check if all the servers in the Topology are accessible: <div data-bbox="477 443 1398 527" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -checkAccess</pre> </div> <p>Example output:</p> <div data-bbox="467 573 1284 999" style="background-color: #2e3436; color: #eeeeec; padding: 10px; margin: 10px 0;"> <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. FIPS integrity verification test failed. 1450723086: [INFO] 'MP-1' is accessible. [admusr@NOAM-2 bin]\$</pre> </div> <p>Note: If any of the servers are not accessible, stop and contact My Oracle Support (MOS).</p>
------------------------------	---	--

Procedure 4. Recovery Scenario 4

47. **NOAM VIP:**
☐ Copy key file to all the servers in topology (RADIUS Only)

If the RADIUS key has never been revoked, skip this step. If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator.

1. Check if existing key file on active NOAM server is valid:

```
$ ./sharedKrevo -validate
[admusr@NOAM-2 bin]$ ./sharedKrevo -validate
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450887507: [INFO] Key file for 'NOAM-1' is valid
1450887507: [INFO] Key file for 'NOAM-2' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450887507: [INFO] Key file for 'SOAM-1' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450887508: [INFO] Key file for 'SOAM-2' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450887509: [INFO] Key file for 'IPFE' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450887510: [INFO] Key file for 'MP-2' is valid
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450887510: [INFO] Key file for 'MP-1' is valid
[admusr@NOAM-2 bin]$
```

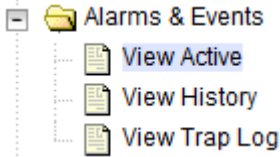
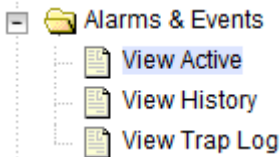
If output of above command shows that existing key file is not valid, then contact My Oracle Support (MOS).

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

```
$ ./sharedKrevo -synchronize
[admusr@NOAM-2 bin]$ ./sharedKrevo -synchronize
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450887549: NOAM-2 and NOAM-1 key files differ. Sync NOAM-2 key file to NOAM-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.
1450887551: [INFO] Synced key to NOAM-1
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450887552: NOAM-2 and SOAM-1 key files differ. Sync NOAM-2 key file to SOAM-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.
1450887554: [INFO] Synced key to SOAM-1
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450887554: [INFO] Key file on Active NOAM and SOAM-2 are same.
1450887554: [INFO] NO NEED to sync key file to SOAM-2.
```

```
$ ./sharedKrevo -updateData
[admusr@NOAM-2 bin]$ ./sharedKrevo -updateData
1450887607: [INFO] Updating data on server 'NOAM-2'
1450887608: [INFO] Data updated to 'NOAM-2'
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450887609: [INFO] Updating data on server 'SOAM-2'
FIPS integrity verification test failed.
FIPS integrity verification test failed.
1450887611: [INFO] 1 rows updated on 'SOAM-2'...
1450887611: [INFO] Data updated to 'SOAM-2'
```

Procedure 4. Recovery Scenario 4

48. <input type="checkbox"/>	SOAM VIP GUI: Examine all alarms	<ol style="list-style-type: none"> 1. Navigate to Alarms & Events > View Active.  2. Examine all active alarms and refer to the on-line help on how to address them. <p>If needed, contact My Oracle Support (MOS).</p>
49. <input type="checkbox"/>	NOAM VIP GUI: Examine all alarms	<ol style="list-style-type: none"> 1. Log into the NOAM VIP if not already logged in. 2. Navigate to Alarms & Events > View Active.  3. Examine all active alarms and refer to the on-line help on how to address them. <p>If needed, contact My Oracle Support (MOS).</p>
50. <input type="checkbox"/>	Restart oampAgent, if needed	<p>Note: If alarm 10012: The responder for a monitored table failed to respond to a table change is raised, the oampAgent needs to be restarted.</p> <ol style="list-style-type: none"> 1. Establish an SSH session to each server that has the alarm., login as admusr. 2. Execute these commands: <pre>\$ sudo pm.set off oampAgent \$ sudo pm.set on oampAgent</pre>
51. <input type="checkbox"/>	Backup and archive all the databases from the recovered system	Execute DSR Database Backup to back up the Configuration databases.
52. <input type="checkbox"/>	Recover IDIH	If IDIH were affected, refer to 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

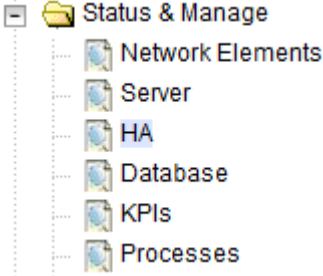
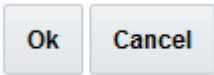
Procedure 5. Recovery Scenario 5

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 SNMP Configuration to configure SNMP as a workaround in the following 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 section.
3. <input type="checkbox"/>	Switch DR NOAM to primary	Refer to DSR/SDS 8.x NOAM Failover User's Guide [17].
4. <input type="checkbox"/>	Recover failed SOAMs	If ALL SOAM servers have failed, execute Procedure 2.

Procedure 5. Recovery Scenario 5

5. <input type="checkbox"/>	DR-NOAM VIP GUI: Login	<ol style="list-style-type: none">1. Establish a GUI session on the DR-NOAM server by using the VIP IP address of the DR-NOAM server. Open the web browser and enter a URL of: <div data-bbox="516 321 1318 369" style="border: 1px solid black; padding: 2px; margin: 5px 0;">http://<Primary_DR-NOAM_VIP_IP_Address></div>2. Login as the guiadmin user: <div data-bbox="477 438 1425 1199" 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 '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', the instruction 'Enter your username and password to log in', and two input fields for 'Username:' and 'Password:'. Below the password field is a checkbox labeled 'Change password' and a 'Log In' button. At the bottom of the page, 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 a horizontal line and copyright information: 'Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.' and 'Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.'</p></div>
--------------------------------	-----------------------------------	--

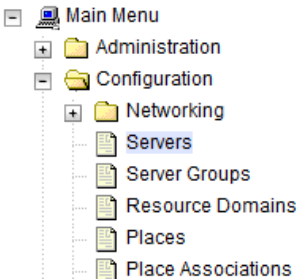

Procedure 5. Recovery Scenario 5

6. <input type="checkbox"/>	DR-NOAM VIP GUI: Set failed NOAM servers to standby	<ol style="list-style-type: none"> Navigate to Status & Manage > HA.  Click Edit. Modifying HA attributes <table border="1" data-bbox="474 724 1006 1060"> <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> Set the Max Allowed HA Role option to OOS for the failed servers. Click OK.  	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												
7. <input type="checkbox"/>	RMS NOAM Failure: Configure BIOS settings and update firmware	<p>If the failed server is NOT a rack mount server, skip to step 11.</p> <ol style="list-style-type: none"> Configure and verify the BIOS settings by executing procedure Configure the RMS and Blade Server BIOS Settings from reference [10]. Verify and/or upgrade server firmware by executing procedure Upgrade Management Server Firmware from reference[10]. <p>Note: Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.</p>												
8. <input type="checkbox"/>	RMS NOAM Failure: Backups available	<p>If the failed server is NOT a rack mount server, skip to step 11. This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media. If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing Restore PMAC from Backup. 												

Procedure 5. Recovery Scenario 5

9. <input type="checkbox"/>	Recover failed aggregation/ enclosure switches, and OAs	<p>Recover failed OAs, aggregation and enclosure switches, if needed.</p> <p>Backups available:</p> <ol style="list-style-type: none"> 1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches. <p>Backups NOT available, execute:</p> <ol style="list-style-type: none"> 1. HP C-7000 Enclosure Configuration from reference [10] to recover and configure any failed OAs, if needed. 2. Configure Enclosure Switches from reference [10] to recover enclosure switches, if needed.
10. <input type="checkbox"/>	RMS NOAM Failure: Backups NOT available	<p>If the failed server is NOT a rack mount server, skip to step 11.</p> <p>This step assumes that TVOE and PMAC backups are NOT available, if the TVOE and PMAC have already been restored, skip this step.</p> <p>If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures:</p> <ol style="list-style-type: none"> 1. Configure and IPM Management Server from reference [10]. 2. Install PMAC from reference [10]. 3. Configure PMAC from reference [10]. <p>If the PMAC is NOT located on the same TVOE host as the failed NOAM, execute the following sections/procedures:</p> <ol style="list-style-type: none"> 1. Installing TVOE on Rack Mount Server(s) from reference [10].
11. <input type="checkbox"/>	HP-Class Blade Failure: Configure blade server iLO, update firmware/BIOS settings	<p>If the failed server is NOT an HP C-Class Blade, skip to step 14.</p> <ol style="list-style-type: none"> 1. Execute Configure Blade Server iLO Password for Administrator Account from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing Server Blades Installation Preparation from reference [10]
12. <input type="checkbox"/>	HP-Class Blade Failure: Backups available	<p>If the failed server is NOT an OAM type HP C-Class Blade, skip to step 14.</p> <p>This step assumes that TVOE backups are available. If backups are NOT available, skip this step.</p> <ol style="list-style-type: none"> 1. Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10]. 2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers.
13. <input type="checkbox"/>	HP-Class Blade Failure: Backups NOT available	<p>If the failed server is NOT an OAM type HP C-Class Blade, skip to step 14.</p> <p>This step assumes TVOE backups are NOT are available.</p> <p>Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10].</p>

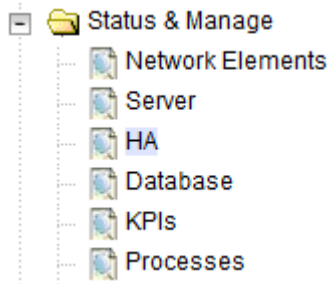
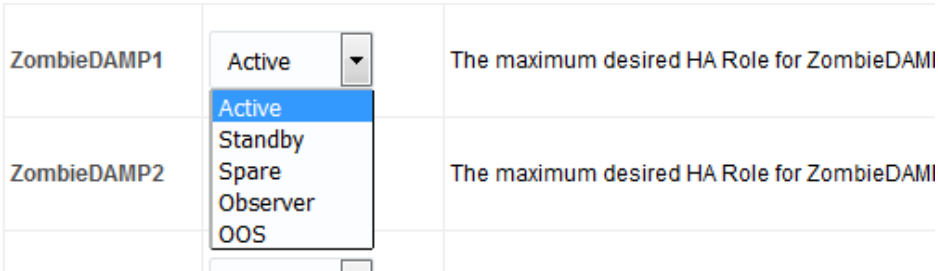
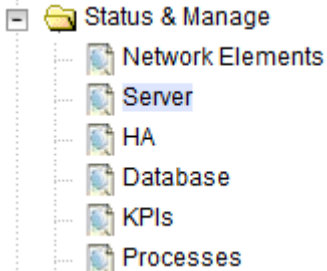
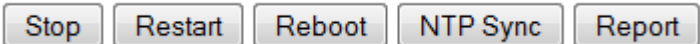
Procedure 5. Recovery Scenario 5

14. <input type="checkbox"/>	Execute fast deployment file for NOAMs	<p>The backup fdconfig file used during the initial DSR installation is available on the PMAC, if a database backup was restored on the PMAC.</p> <p>If a backup fast deployment xml is NOT available, execute Configure NOAM Servers from reference [8].</p> <p>If a backup fast deployment xml is already present on the PMAC, execute the following procedure:</p> <ol style="list-style-type: none"> 1. Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade has been performed since initial installation). 2. Execute these commands: <pre>\$ cd /usr/TKLC/smac/etc \$ screen \$ sudo fdconfig config --file=<Created_FD_File>.xml</pre>
15. <input type="checkbox"/>	DR-NOAM VIP GUI: Export the initial configuration	<ol style="list-style-type: none"> 1. Navigate to Configuration > Servers.  <ol style="list-style-type: none"> 2. From the GUI screen, select the failed NOAM server and click Export to generate the initial configuration data for that server. 
16. <input type="checkbox"/>	DR-NOAM VIP GUI: Copy configuration file to failed NOAM server	<ol style="list-style-type: none"> 1. Obtain a terminal session to the DR-NOAM VIP, login as the admusr user. 2. Configure the failed NOAM server: <pre>\$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<Failed_NOAM_Hostnam e>.sh admusr@<Failed_NOAM_xmi_IP_address>:/var/tmp/TKLCConfigDa ta.sh</pre>

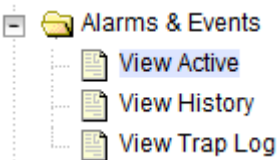
Procedure 5. Recovery Scenario 5

17. <input type="checkbox"/>	Recovered NOAM Server: Verify configuration was called and reboot the server	<ol style="list-style-type: none"> 1. Establish an SSH session to the Recovered NOAM server (Recovered_NOAM_xmi_IP_address) 2. Login as the admusr user. 3. The automatic configuration daemon looks for the file named TKLCConfigData.sh in the /var/tmp directory, implements the configuration in the file, and asks the user to reboot the server. 4. Verify awpushcfg was called by checking the following file. <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> Verify this message displays: <pre>[SUCCESS] script completed successfully!</pre> 5. Now reboot the server: <pre>\$ sudo init 6</pre> 6. Wait for the server to reboot
18. <input type="checkbox"/>	Recovered NOAM Server: Configure networking for dedicated netbackup interface (Optional)	<p>Note: Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP_Address> --netmask=<NO2_NetBackup_NetMask></pre> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=netbackup --address=<NO1_NetBackup_Network_ID> --netmask=<NO2_NetBackup_NetMask> --gateway=<NO2_NetBackup_Gateway_IP_Address></pre>
19. <input type="checkbox"/>	Recovered NOAM Server: Verify server health	<p>Execute this command on the failed NOAM server and make sure no errors are returned:</p> <pre>\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>
20. <input type="checkbox"/>	Repeat for additional 2 nd failed NOAM	Repeat steps 15-19 for the 2 nd failed NOAM server.

Procedure 5. Recovery Scenario 5

21. <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"> 1. From a terminal window connection on the active NOAM as the admusr user, exchange SSH keys for admusr between the active NOAM and the recovered NOAM servers using the keyexchange utility, using the host names of the recovered NOAMs. 2. When prompted for the password, enter the password for the admusr user of the recovered NOAM servers. <pre>\$ keyexchange admusr@<Recovered_NOAM_Hostname></pre>
22. <input type="checkbox"/>	NOAM VIP GUI: Set HA on the recovered NOAMs	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > HA.  2. Click Edit. 3. For each NOAM server whose Max Allowed HA Role is set to Standby, set it to Active.  4. Click OK.
23. <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application	<ol style="list-style-type: none"> 1. Navigate to Status & Manage > Server.  2. Select each recovered NOAM server and click Restart. 

Procedure 5. Recovery Scenario 5

24. <input type="checkbox"/>	Recovered NOAM Servers: 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>For PCA:</p> <p>Establish SSH sessions to the all the recovered NOAM servers and login as admusr. Refer [13] and execute PCA Activation on Standby NOAM Server on all recovered NOAM servers to re-activate PCA.</p> <p>For MAP-IWF:</p> <p>Establish SSH session to the recovered active NOAM, login as admusr. Refer to [7] to activate Map-Diameter Interworking (MAP-IWF).</p> <p>Note: 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>Note: If any of the MPs are failed and recovered, then restart these MP servers after activation of the feature.</p>
25. <input type="checkbox"/>	DR-NOAM VIP: Copy key file to recovered NOAM 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"> 1. Establish an SSH session to any of the active DR NOAM that is intact and operational. Login as admusr. 2. Check if existing key file on active DR NOAM server is valid: <pre>\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -validate</pre> <p>Note: If errors are present, stop and contact My Oracle Support (MOS).</p> <ol style="list-style-type: none"> 3. If key file is valid, copy key file from the active DR NOAM server to recovered NOAMs: <pre>\$/sharedKrevo -copyKey -destServer <First NOAM> \$/sharedKrevo -copyKey -destServer <Second NOAM></pre>
26. <input type="checkbox"/>	Switch DR NOAM back to secondary	Once the system have been recovered, refer to DSR/SDS 8.x NOAM Failover User's Guide [17].
27. <input type="checkbox"/>	Recovered Servers: Verify alarms	<ol style="list-style-type: none"> 1. Navigate to Alarms & Events > View Active.  <ol style="list-style-type: none"> 2. Verify the recovered servers are not contributing to any active alarms (Replication, Topology misconfiguration, database impairments, NTP, etc.)

Procedure 5. Recovery Scenario 5

28. <input type="checkbox"/>	NOAM VIP GUI: Recover standby/spare SOAM and C-level servers	If necessary, refer to Procedure 3 to recover any standby or Spare SOAMs as well as any C-level servers.
29. <input type="checkbox"/>	NOAM VIP: 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"> 1. Establish an SSH session to the NOAM VIP. Login as admusr. 2. Check if all the servers in the Topology are accessible: <pre>\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -checkAccess</pre> <p>Note: If any of the servers are not accessible, stop and My Oracle Support (MOS).</p>
30. <input type="checkbox"/>	NOAM VIP: Copy key file to all the servers in topology (RADIUS Only)	<ol style="list-style-type: none"> 1. Establish an SSH session to the active NOAM, login as admusr. 2. Copy the key file to all the servers in the Topology: <pre>\$./sharedKrevo -synchronize \$./sharedKrevo -updateData</pre> <p>Note: If errors are present, stop and contact My Oracle Support (MOS).</p>
31. <input type="checkbox"/>	Recover IDIH	If IDIH was affected, refer to IDIH Disaster Recovery section 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

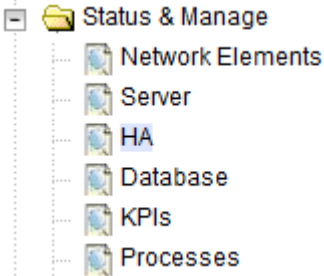

- Server having a corrupted database
- Replication channel from parent is inhibited because of upgrade activity; or
- Server is in a different release then that of its active parent because of upgrade activity
- Verify the server runtime backup files, performed at the start of the upgrade, are present 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

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

Procedure 6. Recovery Scenario 6 (Case 1)

S T E P #	<p>This procedure performs recovery if database is corrupted in the system</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>NOAM VIP GUI: Login</p> <ol style="list-style-type: none"> 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="516 510 1320 560" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> http://<Primary_NOAM_VIP_IP_Address> </div> 2. Login as the guiadmin user: <div data-bbox="477 625 1425 1381" style="text-align: center;">  <p>Oracle System Login</p> <hr/> <p>Tue Jun 7 13:49:06 2016 EDT</p> <div data-bbox="651 840 1252 1207" style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 80%;"> <p>Log In</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, Oracle and/or its affiliates. All rights reserved.</i></p> </div>

Procedure 6. Recovery Scenario 6 (Case 1)

2. <input type="checkbox"/>	NOAM VIP GUI: Set failed servers to OOS	<ol style="list-style-type: none"> Navigate to Status & Manage > HA.  Select Edit. Modifying HA attributes <table border="1" data-bbox="475 714 1008 1056"> <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>Active Standby Spare Observer OOS</td><td>The maximum des</td></tr> </tbody> </table> Set the Max Allowed HA Role option to OOS for the failed servers. Click OK.  	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active	The maximum des	ZombieNOAM2	OOS	The maximum des	ZombieDRNOAM1	Active Standby Spare Observer OOS	The maximum des
Hostname	Max Allowed HA Role	Description												
ZombieNOAM1	Active	The maximum des												
ZombieNOAM2	OOS	The maximum des												
ZombieDRNOAM1	Active Standby Spare Observer OOS	The maximum des												
3. <input type="checkbox"/>	Server in Question: Login	Establish an SSH session to the server in question. Login as admusr .												
4. <input type="checkbox"/>	Server in Question: Change runlevel to 3	Bring the system to runlevel 3. <pre>\$ sudo init 3</pre>												
5. <input type="checkbox"/>	Server in Question: Recover system	Execute this command and follow the instructions appearing in the console prompt. <pre>\$ sudo /usr/TKLC/appworks/sbin/backout_restore</pre>												
6. <input type="checkbox"/>	Server in Question: Change runlevel to 4	Bring the system back to runlevel 4. <pre>\$ sudo init 6</pre>												

Procedure 6. Recovery Scenario 6 (Case 1)

<p>7.</p> <p><input type="checkbox"/></p>	<p>Server in Question: 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 admusr]#</pre>												
<p>8.</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Set failed servers to active</p>	<ol style="list-style-type: none"> Navigate to Status & Manage > HA.  <ol style="list-style-type: none"> Click Edit. Select the failed server and set it to Active. <p>Modifying HA attributes</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</td> <td>The maximum</td> </tr> </tbody> </table> <p>4. Click OK.</p>	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 6. Recovery Scenario 6 (Case 1)

<p>9. <input type="checkbox"/></p>	<p>NOAM VIP: 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"> 1. Establish an SSH session to the NOAM VIP and login as admusr. 2. Check if all the servers in the Topology are accessible: <pre> \$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -checkAccess [admusr@NOAM-2 bin]\$./sharedKrevo -checkAccess FIPS integrity verification test failed. 1450723797: [INFO] 'NOAM-1' is accessible. FIPS integrity verification test failed. 1450723797: [INFO] 'SOAM-1' is accessible. FIPS integrity verification test failed. 1450723797: [INFO] 'SOAM-2' is accessible. FIPS integrity verification test failed. 1450723798: [INFO] 'IPFE' is accessible. FIPS integrity verification test failed. 1450723798: [INFO] 'MP-2' is accessible. FIPS integrity verification test failed. 1450723798: [INFO] 'MP-1' is accessible. [admusr@NOAM-2 bin]\$ </pre>
------------------------------------	---	--

Procedure 6. Recovery Scenario 6 (Case 1)

10.	NOAM VIP: <input type="checkbox"/> 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"> 1. Check if existing key file on active NOAM (The NOAM which is intact and was not recovered) server is valid: <pre> \$./sharedKrevo -validate [admsur@NOAM-2 bin]\$./sharedKrevo -validate FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723843: [INFO] Key file for 'NOAM-1' is valid 1450723843: [INFO] Key file for 'NOAM-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723844: [INFO] Key file for 'SOAM-1' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723845: [INFO] Key file for 'SOAM-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723845: [INFO] Key file for 'IPFE' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723846: [INFO] Key file for 'MP-2' is valid FIPS integrity verification test failed. FIPS integrity verification test failed. 1450723847: [INFO] Key file for 'MP-1' is valid [admsur@NOAM-2 bin]\$ </pre> <p>If output of above command shows the existing key file is not valid, contact My Oracle Support (MOS).</p> <ol style="list-style-type: none"> 2. Copy the key file to all the servers in the Topology: <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 [admsur@NOAM-2 bin]\$ </pre> <pre> \$./sharedKrevo -updateData [admsur@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>
11.	<input type="checkbox"/> Backup and archive all the databases from the recovered system	<p>Execute DSR Database Backup to back up the Configuration databases.</p>


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

4.6.2 Recovery Scenario 6: Case 2

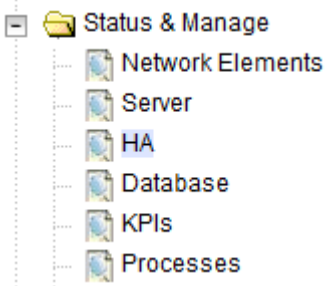
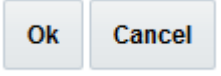
For a partial outage with:

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

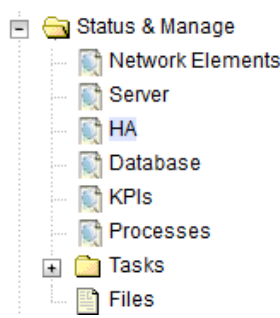
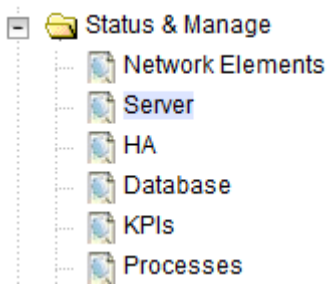

Procedure 7. Recovery Scenario 6 (Case 2)

STEP #	<p>This procedure performs recovery if database got corrupted in the system and system is in the state to get replicated.</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>NOAM VIP GUI: Login</p> <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="552 762 1354 810" style="border: 1px solid black; padding: 2px;"> <p><code>http://<Primary_NOAM_VIP_IP_Address></code></p> </div> <p>2. Login as the guiadmin user:</p> <div data-bbox="516 877 1464 1633">  </div>

Procedure 7. Recovery Scenario 6 (Case 2)

2. <input type="checkbox"/>	NOAM VIP GUI: Set failed servers to OOS	1. Navigate to Status & Manage > HA .  2. Click Edit . Modifying HA attributes <table border="1" data-bbox="511 714 1047 1060"> <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> 3. Set the Max Allowed HA Role option to OOS for the failed servers. 4. Click OK . 	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												
3. <input type="checkbox"/>	Server in Question: Login	Establish an SSH session to the server in question. Login as admusr .												
4. <input type="checkbox"/>	Server in Question: Stop httpd service	Stop the httpd service. <pre>\$ sudo bash -l \$ service httpd stop</pre>												
5. <input type="checkbox"/>	Server in Question: Take server out of service	Take the server out of service. <pre>\$ prod.clobber</pre>												
6. <input type="checkbox"/>	Server in Question: 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)

7.	Server in Question: Start httpd service	<p>1. Start the httpd service.</p> <pre>\$ service httpd start</pre> <p>2. Exit out of root.</p> <pre>\$ exit</pre>												
8. <input type="checkbox"/>	NOAM VIP GUI: Set failed servers to active	<p>1. Navigate to Status & Manage > HA.</p>  <p>2. Click Edit at the bottom of the screen.</p> <p>3. Select the failed server and set it to Active.</p> <p>Modifying HA attributes</p> <table border="1" data-bbox="511 966 990 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> <p>4. Click OK.</p>	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												
9. <input type="checkbox"/>	NOAM VIP GUI: Restart DSR application	<p>1. Navigate to Status & Manage > Server.</p>  <p>2. Select each recovered server and click Restart.</p> 												

Procedure 7. Recovery Scenario 6 (Case 2)

10. <input type="checkbox"/>	Server in Question: Verify the server state	<ol style="list-style-type: none"> 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 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 admusr]#</pre> 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> 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>
11. <input type="checkbox"/>	NOAM VIP: 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"> Establish an SSH session to the NOAM VIP and login as admusr. Check if all the servers in the Topology are accessible: <pre>\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -checkAccess</pre>

Procedure 7. Recovery Scenario 6 (Case 2)

12. <input type="checkbox"/>	NOAM VIP: 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"> 1. Check if existing key file on active NOAM (the NOAM which is intact and was not recovered) server is valid: <div data-bbox="552 420 1120 514" data-label="Text"> <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> 2. Copy the key file to all the servers in the topology: <div data-bbox="511 630 1437 1585" data-label="Text"> <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. 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> <p>Note: If any errors are present, stop and contact My Oracle Support (MOS).</p>
13. <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.

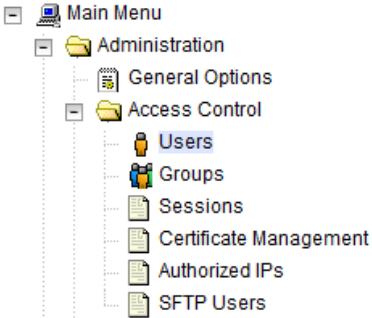
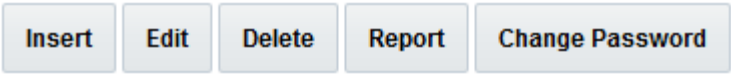
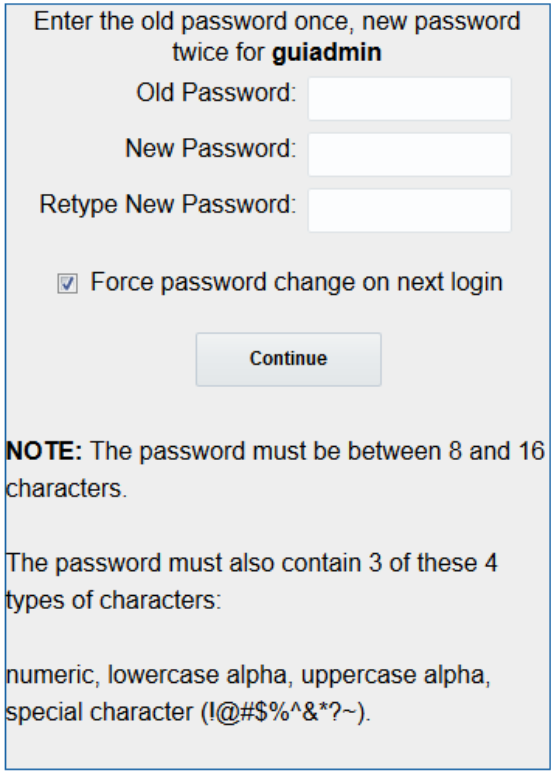
These users were removed before creation of the backup and archive file. They are reintroduced by system restoration of that file.

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"/>	Before Restoration: 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"/>	After Restoration: Log into the NOAM VIP	<ol style="list-style-type: none"> 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://<Primary_NOAM_VIP_IP_Address></div> Login as the guiadmin user: <div style="text-align: center; margin: 20px 0;">  </div> <div style="text-align: center;"> Oracle System Login </div> <div style="text-align: right; margin-top: 5px;">Tue Jun 7 13:49:06 2016 EDT</div> <div style="border: 1px solid black; padding: 10px; margin: 20px auto; width: 80%;"> <p style="text-align: center;">Log In</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; margin-top: 10px;"> <input type="button" value="Log In"/> </p> </div>

Procedure 8. Keep Restored User

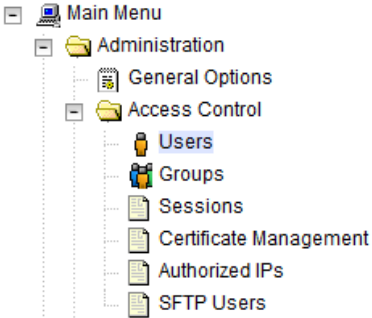
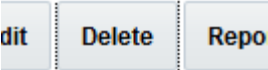
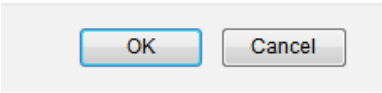
3.	After Restoration: Reset user passwords	<ol style="list-style-type: none"> 1. Navigate to Administration > Access Control > Users.  2. Select the user. 3. Click Change Password.  4. Type a new password.  <p>NOTE: The password must be between 8 and 16 characters.</p> <p>The password must also contain 3 of these 4 types of characters:</p> <p>numeric, lowercase alpha, uppercase alpha, special character (!@#\$%^&*?~).</p> 5. Click Continue.
----	---	---

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>
<p>1. <input type="checkbox"/></p>	<p>After Restoration: Log into the NOAM VIP</p> <ol style="list-style-type: none"> 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://<Primary_NOAM_VIP_IP_Address></div> Login as the guiadmin user: <div style="text-align: center; margin: 20px 0;">  </div> <div style="text-align: center;"> <p>Oracle System Login</p> <hr style="width: 50%; margin: 0 auto;"/> <p style="text-align: right;">Tue Jun 7 13:49:06 2016 EDT</p> </div> <div style="text-align: center; margin: 20px 0;"> <div style="border: 1px solid black; padding: 10px; width: 60%; margin: 0 auto;"> <p>Log In</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><input type="checkbox"/> Change password</p> <p><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 style="width: 50%; margin: 10px auto;"/> <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, Oracle and/or its affiliates. All rights reserved.</p>

Procedure 9. Remove the Restored User

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

5.4 Restore a Modified User

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

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

Before Restoration:

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

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

After Restoration:

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


5.5 Restore an Archive that Does Not Contain a Current User

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

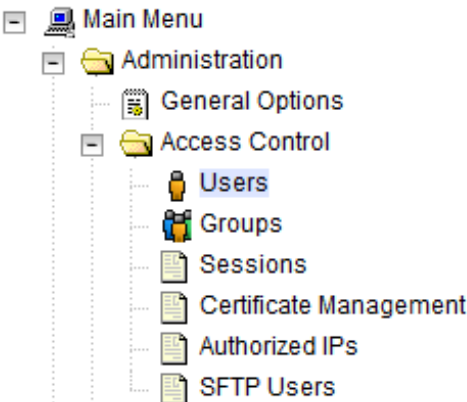
- User 'testuser' exists in current database but not in the selected backup file.

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


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

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>Before Restoration: Notify affected users before restoration</p> <p>Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.</p>
2. <input type="checkbox"/>	<p>Before Restoration: Log into the NOAM VIP</p> <ol style="list-style-type: none"> 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="553 653 1354 695" style="border: 1px solid black; padding: 2px; margin: 5px 0;">http://<Primary_NOAM_VIP_IP_Address></div> 2. Login as the guiadmin user: <div data-bbox="516 766 1412 1486" style="text-align: center; margin-top: 20px;">  <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. 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, it states: 'Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.' and 'Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.'</p> </div>

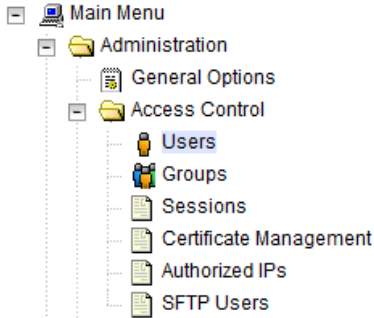
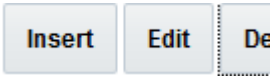
Procedure 10. Restore an Archive That Does Not Contain a Current User

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

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

4. <input type="checkbox"/>	After Restoration: Login	<ol style="list-style-type: none">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="553 323 1354 369" style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>http://<Primary_NOAM_VIP_IP_Address></code></div>2. Login as the guiadmin user: <div data-bbox="516 436 1414 1173"></div>
--------------------------------	------------------------------------	---

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

<p>5. <input type="checkbox"/></p>	<p>After restoration: recreate affected user</p>	<p>1. Navigate to Administration > Access Control > Users.</p>  <p>2. Click Insert.</p>  <p>3. Recreate the user using the data collected from step 3.</p> <p>Adding new user</p> <table border="1" data-bbox="505 863 1019 1650"> <tr> <td>Username *</td> <td><input type="text"/></td> <td>Select long</td> </tr> <tr> <td>Group *</td> <td>admin</td> <td>Select</td> </tr> <tr> <td>Authentication Options</td> <td> <input type="checkbox"/> Allow Remote Authentication <input checked="" type="checkbox"/> Allow Local Authentication </td> <td>Select Authentication [Default]</td> </tr> <tr> <td>Access Options</td> <td> <input checked="" type="checkbox"/> Allow GUI Access <input checked="" type="checkbox"/> Allow MMI Access </td> <td>Select</td> </tr> <tr> <td>Access Allowed</td> <td><input checked="" type="checkbox"/> Account Enabled</td> <td>Is this</td> </tr> <tr> <td>Maximum Concurrent Logins</td> <td>0</td> <td>The</td> </tr> <tr> <td>Session Inactivity Limit</td> <td>120</td> <td>The</td> </tr> <tr> <td>Comment *</td> <td><input type="text"/></td> <td>Comments</td> </tr> </table> <p>4. Click OK.</p>	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 Authentication [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 this	Maximum Concurrent Logins	0	The	Session Inactivity Limit	120	The	Comment *	<input type="text"/>	Comments
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 Authentication [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 this																								
Maximum Concurrent Logins	0	The																								
Session Inactivity Limit	120	The																								
Comment *	<input type="text"/>	Comments																								
<p>6. <input type="checkbox"/></p>	<p>After Restoration: Repeat for additional users</p>	<p>Repeat step 5 to recreate additional users.</p>																								

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


7. <input type="checkbox"/>	After Restoration: Reset the passwords	See Procedure 8 for resetting passwords for a user.
--------------------------------	--	---

6. IDIH Disaster Recovery

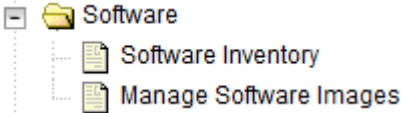
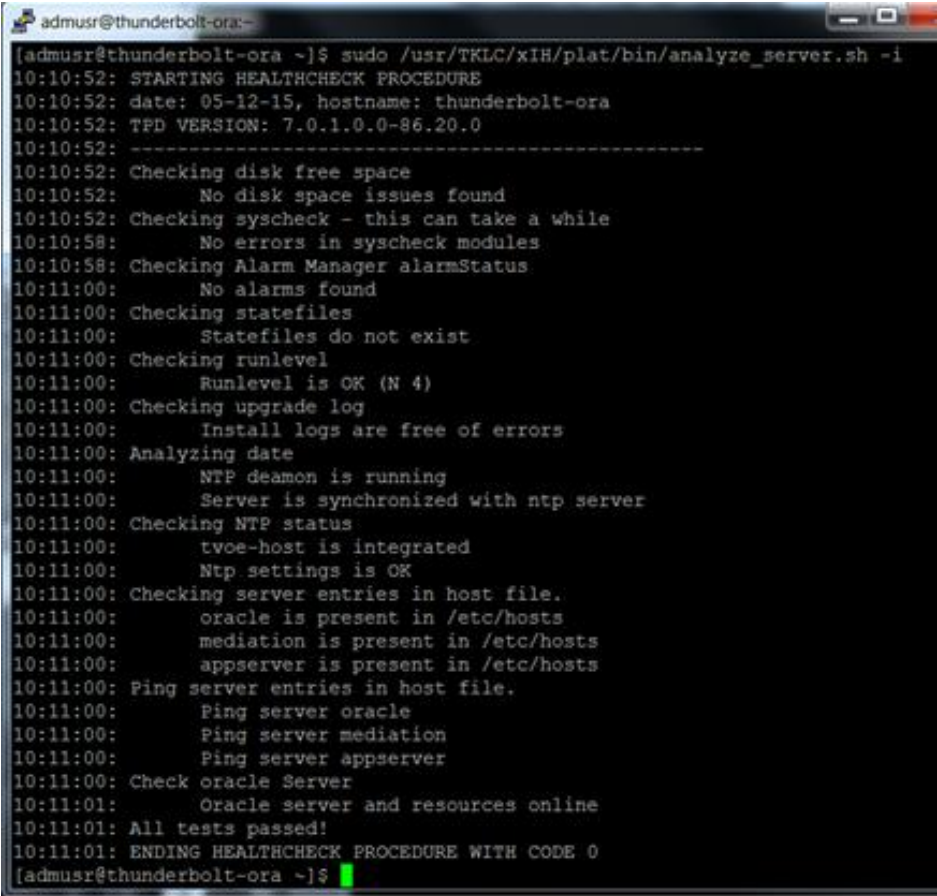
The fdconfig.xml file you use for disaster recovery is different from the one used for fresh installation. The one for disaster recovery has the **hostname-upgrade_xx-xx-xx.xml** file format. It took out the Oracle server installation part since it is not needed for disaster recovery.

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, refer to fresh installation section to re-create it.


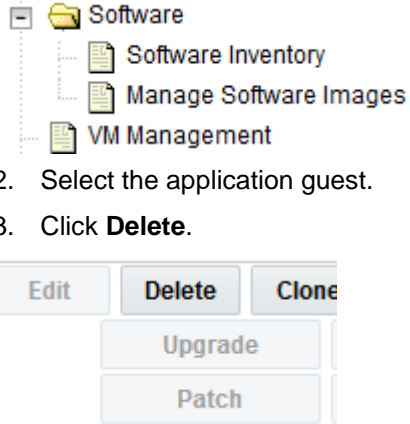
Procedure 11. IDIH Disaster Recovery Preparation

STEP #	<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>PMAC GUI: Login</p> <div data-bbox="462 861 1437 1801"> <p>1. Open web browser and enter:</p> <div data-bbox="511 913 1323 961" style="border: 1px solid black; padding: 2px;">http://<PMAC_Mgmt_Network_IP></div> <p>2. Login as pmacadmin user:</p> <div data-bbox="470 1018 1437 1801">  </div> </div>

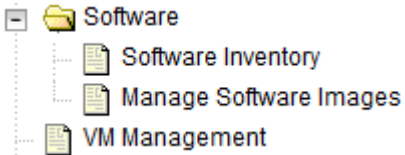
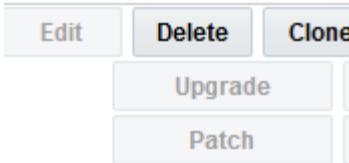
Procedure 11. IDIH Disaster Recovery Preparation

2. <input type="checkbox"/>	PMAC GUI: Verify necessary IDIH images are available	1. Navigate to Software > Manage Software Images .  2. Verify the current IDIH TVOE, TPD, Oracle, Application and Mediation images are listed. Note: If the necessary software images are not available, follow the instructions from the Load Application and TPD ISO onto PMAC Server procedure and steps 1-4 of IDIH Configuration from [8] to acquire and transfer the images.
3. <input type="checkbox"/>	Oracle Guest: Login	Establish an SSH session to the Oracle guest, login as admusr .
4. <input type="checkbox"/>	Oracle Guest: Perform database health check	Perform a database health check: <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> \$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i </div> Example output: 

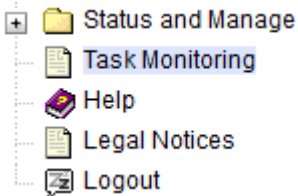
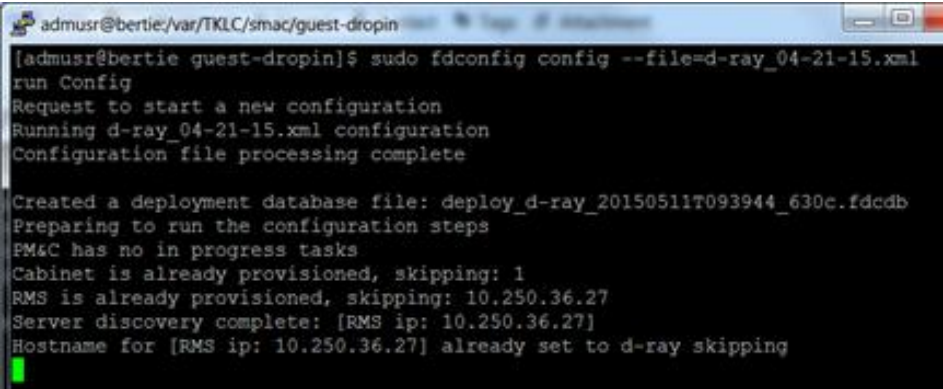
Procedure 12. IDIH Disaster Recovery (Re-Install Mediation and Application Servers)

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>
1. <input type="checkbox"/>	<p>PMAC GUI: Login</p> <ol style="list-style-type: none"> Open web browser and enter: <div style="border: 1px solid black; padding: 2px; margin: 5px 0;">http://<PMAC_Mgmt_Network_IP></div> Login as pmacadmin user:  <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, Oracle and/or its affiliates. All rights reserved.</p>
2. <input type="checkbox"/>	<p>Remove existing application server</p> <ol style="list-style-type: none"> Navigate to Main Menu > VM Management.  <ol style="list-style-type: none"> Select the application guest. Click Delete.

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"> 1. Navigate to Main Menu > VM Management.  2. Select the Mediation guest. 3. Click Delete. 
4. <input type="checkbox"/>	PMAC: Establish SSH session and login	Establish an SSH session to the PMAC, login as admusr .
5. <input type="checkbox"/>	PMAC: 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=<hostname-upgrade_xx-xx-xx>.xml</pre> <div data-bbox="875 1062 1040 1230" data-label="Image"> </div> <p>!!Warning!!</p> <p>If you run the fdconfig without upgrade in the XML filename, the database is destroyed and you lose all of the existing data.</p> <p>Note: This is a long duration command (45-90 minutes). If the screen command was run before executing the fdconfig, perform a screen -dr to resume the screen session in the event of a terminal timeout etc.</p>

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

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

Appendix A. DSR Database Backup

Procedure 13. DSR Database Backup

STEP #	<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>
1. <input type="checkbox"/>	<p>NOAM/SOAM VIP: Login</p> <ol style="list-style-type: none"> 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="516 680 1318 728" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> http://<Primary_NOAM/SOAM_VIP_IP_Address> </div> Login as the guiadmin user: <div data-bbox="477 793 1425 1558" 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 '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. At the bottom of the page, 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>

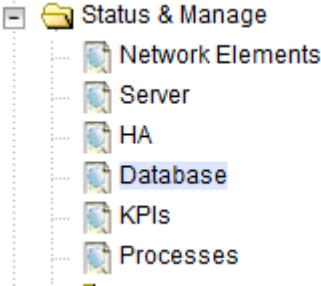
Procedure 13. DSR Database Backup

2.

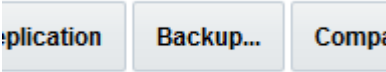
☐

NOAM/SOAM VIP: Backup configuration data for the system

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



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



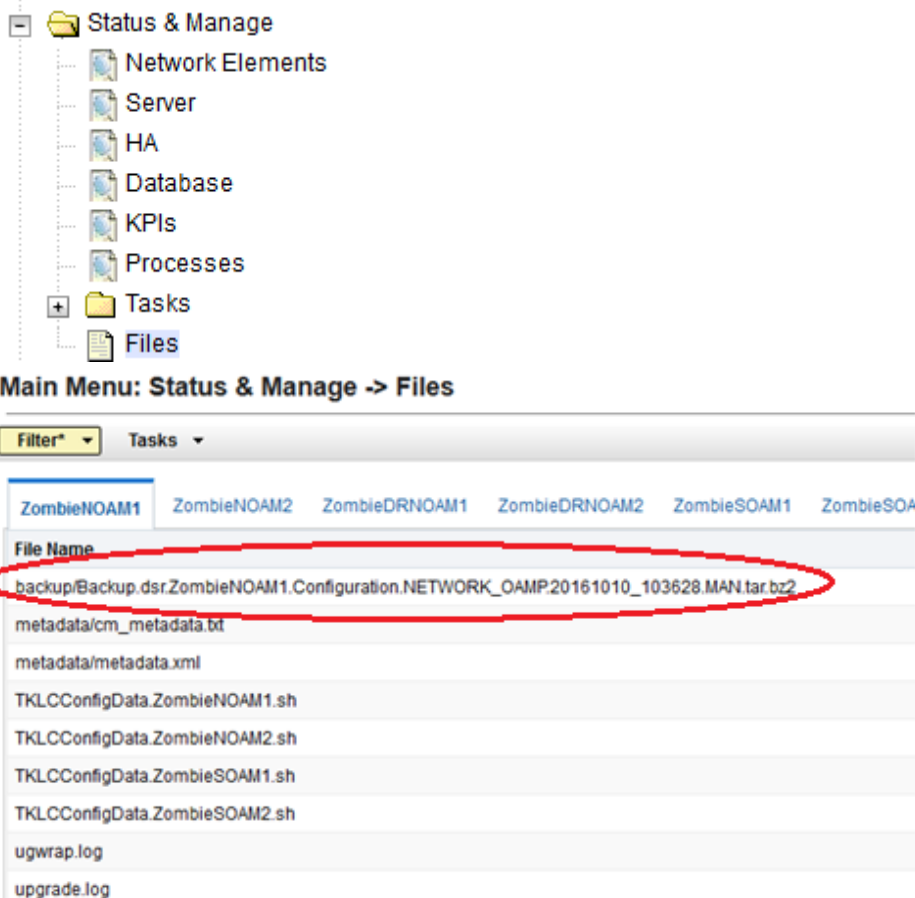
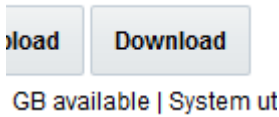
3. Make sure that the **Configuration** checkbox is marked.

Database Backup

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

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

Procedure 13. DSR Database Backup

<p>3. <input type="checkbox"/></p>	<p>NOAM/SOAM VIP: Verify the backup file existence</p>	<p>1. Navigate to Status & Manage > Files.</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>NOAM/SOAM VIP: Download the file to a local machine</p>	<p>1. From the previous step, select the backup file.</p> <p>2. Click Download.</p>  <p>3. Click OK 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

<p>7. <input type="checkbox"/></p>	<p>Take a secured backup of key file (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"> 1. Log into ssh shell of active NOAM server as admusr. 2. Take a secure backup of updated key file RADIUS shared secret encryption key for disaster scenarios. 3. Encrypt the key file before backing up to secure customer setup: <div data-bbox="513 516 904 562" data-label="Text"> <pre>\$./sharedKrevo -encr</pre> </div> 4. Copy the encrypted key file to secure customer setup: <div data-bbox="513 619 1421 695" data-label="Text"> <pre>\$ sudo scp /var/TKLC/db/filemgmt/DpiKf.bin.encr user@<customer IP>:<path of customer setup></pre> </div> <p>Note: The operator must strictly control access to the backed up key file. If the operator needs to encrypt this key file further using operator specified encryption techniques, the operator is recommended to do so; however, the operator is responsible to decrypt this file using operator-specific decryption techniques and copy the resulting DpiKf.bin.encr file securely to the file management folder if the key file needs to be restored for disaster recovery. Once the key file is backed up to the operator-provided server and path, it is the responsibility of the operator to ensure access to the backed up key file is extremely selective and restricted.</p>
------------------------------------	--	---

Appendix B. Recover/Replace Failed 3rd Party Components (Switches, OAs)

The following procedures provide steps to recover 3rd party devices (switches, OAs). Follow the appropriate procedure as needed for your disaster recovery.

Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F)

S T E P #	<p>This procedure recovers a failed aggregation (4948E/4948E-F) switch.</p> <p>Prerequisites for this procedure are:</p> <ul style="list-style-type: none"> • A copy of the networking xml configuration files • A copy of HP Misc Firmware DVD or ISO • IP address and hostname of the failed switch • Rack mount position of the failed switch <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>Recover failed Aggregation Switches: Cisco 4948E/4948E-F</p> <ol style="list-style-type: none"> 1. Log into the PMAC using SSH as admusr. 2. Remove the old SSH key of the switch from the PMAC by executing this command from a PMAC command shell: <pre>sudo ssh-keygen -R <4948_switch_IP></pre> 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>Note: You need a copy of the HP Misc Firmware DVD or ISO (or firmware file obtained from the appropriate hardware vendor) and the original networking XML files custom for this installation. These are either stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.</p> <p>Note: 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 switch1A_4948_4948E_init.xml.</p> 4. The templates can be found using the following method: <p>From the PMAC CLI:</p> <pre>df grep -I DSR</pre> <p>Example output:</p> <pre>/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso 1118514 1118514 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64 /var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso 1118372 1118372 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64 /var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-</pre>

Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F)

	<pre>x86_64.iso 1117976 1117976 0 100% /usr/TKLC/smac/html/TPD/DSR- 8.2.0.0.0_82.4.0-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/<DSR Release dir>/upgrade/overlay/</pre> </div> <p>Example:</p> <pre>cd /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0- 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 TVOEclean.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 <switch_xml_file> /usr/TKLC/smac/etc/switch/xml/</pre>
--	--

Procedure 15. Recover a Failed Enclosure Switch (Cisco 3020)

S T E P #	<p>This procedure recovers a failed enclosure (3020) switch.</p> <p>Prerequisites for this procedure are:</p> <ul style="list-style-type: none"> • A copy of the networking xml configuration files • A copy of HP Misc. Firmware DVD or ISO • IP address and hostname of the failed switch • Interconnect Bay position of the enclosure switch <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>Recover Failed Enclosure Switch: Cisco 3020</p> <ol style="list-style-type: none"> 1. Log into the PMAC using SSH as admusr. 2. Remove the old SSH key of the switch from the PMAC by executing this command from a PMAC command shell: <div data-bbox="537 758 1252 806" data-label="Text"> <pre>sudo ssh-keygen -R <enclosure_switch_ip></pre> </div> 3. Refer to procedure Replace a failed 3020 switch (netConfig) to replace the failed enclosure switch from reference [2]. <p>Note: You need a copy of the HP Misc Firmware DVD or ISO and of the original networking xml files custom for this installation. These either be stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.</p>

Procedure 16. Recover a Failed Enclosure Switch (HP 6120XG , HP 6125XLG, HP 6125G)

S T E P #	<p>This procedure recovers a failed enclosure (6120XG/6125XLG/6125G) switch.</p> <p>Prerequisites for this procedure are:</p> <ul style="list-style-type: none"> • A copy of the networking xml configuration files <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>Recover Failed Enclosure Switch: HP 6120XG/6125XLG /6125G</p> <ol style="list-style-type: none"> 1. Log into the PMAC using SSH as admusr. 2. Remove the old SSH key of the switch from the PMAC by executing this command from a PMAC command shell: <div data-bbox="537 1499 1252 1547" data-label="Text"> <pre>sudo ssh-keygen -R <enclosure_switch_ip></pre> </div> 3. Refer to procedure Replace a failed HP (6120XG, 6125G, 6125XLG switch (netConfig) to replace the failed enclosure switch from reference [2]. <p>Note: You need a copy of the HP Misc Firmware DVD or ISO and of 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>Note: Copy switch appropriate init file and use it for respective switch:</p> <ol style="list-style-type: none"> 4. Older platform init files may not work on platform 7.2 systems. Copy the

Procedure 16. Recover a Failed Enclosure Switch (HP 6120XG , HP 6125XLG, HP 6125G)

switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy 'switch1A_4948_4948E_init.xml'.

5. The templates can be found by the following method:

From the PMAC CLI:

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

Example output:

```
/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso
1118514 1118514 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64
/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso
1118372 1118372 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64
/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso
1117976 1117976 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64
```

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

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

Example:

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

7. Locate the DSR_NetConfig_Templates.zip file.

Example:

```
$ 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 TVOEclean.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
```

8. Unzip the **DSR_NetConfig_Templates.zip** file and retrieve the required switch init file.

Example:

```
$ unzip DSR_NetConfig_Templates.zip
```

9. Edit the desired file with site specific details. The existing file from original

Procedure 16. Recover a Failed Enclosure Switch (HP 6120XG , HP 6125XLG, HP 6125G)

	<p>deployment <code>/usr/TKLC/smac/etc/switch/xml</code> can be used as a reference.</p> <p>10. Copy the new init file to the <code>/usr/TKLC/smac/etc/switch/xml</code> dir.</p> <p>Example:</p> <pre>\$ cp <switch_xml_file> /usr/TKLC/smac/etc/switch/xml/</pre> <p>Note: While restoring 6120XG switch, some features enabled on a 6120XG may not restore properly if they reference a port channel that does not currently exist on the switch ahead of the restore operation. Identify any port channels that need to be created on the switch according to the backup file and create them before restoring the configuration:</p> <pre>\$ sudo /bin/cat <switch_hostname>-backup /bin/grep "^trunk"</pre> <p>Example output:</p> <pre>trunk <int list> Trk<id> LACP trunk <int list> Trk<id> Trunk</pre> <p>11. If any port-channels are found, then for each portchannel identified by the above command, use the netConfig setLinkAggregation command to create it and the netConfig showConfiguration command to verify its configuration:</p> <p>12. If an LACP port channel was found, add the port-channel with this command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- device=6120XG_IOBAY2 setLinkAggregation id=<id> addPort=tenGE<int list> mode=active</pre> <p>13. If a Trunk port-channel was found (as labeled after the Trk<id>), add the port-channel with this command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- device=6120XG_IOBAY2 setLinkAggregation id=<id> addPort=tenGE<int list> mode=static</pre> <p>14. Verify the port-channels were added to the running configuration:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- device=6120XG_IOBAY2 showConfiguration grep "^trunk" trunk <int list> Trk<id> LACP trunk <int list> Trk<id> Trunk</pre> <p>15. For all switch types and configurations found, use netConfig to restore the configuration:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- device=<switch_hostname> restoreConfiguration service=ssh_service filename=<switch_hostname>-backup</pre> <p>Note: This causes the switch to reboot. It takes approximately 120-180 seconds before connectivity is restored.</p>
--	---

Procedure 17. Recover a Failed Enclosure OA

S T E P #	<p>This procedure recovers a failed Enclosure Onboard Administrator.</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"/>	Recover failed enclosure OA	Refer to procedure Restore OA Configuration from Management Server to replace a failed enclosure OA from reference [2].

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

<div>S T E P #</div>	<div>This procedure inhibits A and B level replication on all C-level servers of this site.</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. <div></div></div>	<div>Active NOAM:</div> <div>Login</div>	<div>Log into the active NOAM server using SSH as admusr.</div>																																														
<div>1. <div></div></div>	<div>Active NOAM:</div> <div>Inhibit replication on all C-level servers</div>	<div>Execute this command:</div> <div><pre>\$ for i in \$(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<SOAM Site_NE name of the site>'); do iset -finhibitRepPlans='A B' NodeInfo where "nodeName='\$i'; done</pre></div> <div><div>Note:</div> SOAM Site_NE name of the site can be found out by logging into the active NOAM GUI and navigating to Configuration > Server Groups.</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 -> Servers</div> <div><div>Filter* Info*</div><table><tr><th>Hostname</th><th>Role</th><th>System ID</th><th>Server Group</th><th>Network Element</th></tr><tr><td>ZombieNOAM1</td><td>Network OAM&P</td><td></td><td>ZombieNOAM</td><td>ZombieNOAM</td></tr><tr><td>ZombieNOAM2</td><td>Network OAM&P</td><td></td><td>ZombieNOAM</td><td>ZombieNOAM</td></tr><tr><td>ZombieDRNOAM1</td><td>Network OAM&P</td><td></td><td>ZombieDRNOAM</td><td>ZombieDRNOAM</td></tr><tr><td>ZombieDRNOAM2</td><td>Network OAM&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></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																																												

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

2. <input type="checkbox"/>	Active NOAM: 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.</p> <p>InhibitRepPlans field for all the MP servers for the selected site, for example, Site SO_HPC03 is set as A B.</p> <div><pre>\$ iqt NodeInfo</pre></div> <p>Example output:</p> <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 19. 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.

Active NOAM:
Login

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

2.

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

Execute this command:

```
$ for i in $(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<SOAM_Site_NE_name>'); do iset -finhibitRepPlans='' NodeInfo where "nodeName='<$i'"; done
```

Note:

SOAM Site NE name of the site can be found out by logging into the active NOAM GUI and navigating to **Configuration > Server Groups**.

Please see the snapshot below for more details, for example, if ServerSO1 belongs to the site being recovered, then siteID is SO_HPC03.

Main Menu: Configuration -> Servers

Filter*Info*

Hostname	Role	System ID	Server Group	Network Element
ZombieNOAM1	Network OAMSP		ZombieNOAM	ZombieNOAM
ZombieNOAM2	Network OAMSP		ZombieNOAM	ZombieNOAM
ZombieDRNOAM1	Network OAMSP		ZombieDRNOAM	ZombieDRNOAM
ZombieDRNOAM2	Network OAMSP		ZombieDRNOAM	ZombieDRNOAM
ZombieSOAM1	System OAM		ZombieSOAM	ZombieSOAM
ZombieSOAM2	System OAM		ZombieSOAM	ZombieSOAM
ZombieDAMP1	MP		ZombieDAMP	ZombieSOAM
ZombieDAMP2	MP		ZombieDAMP	ZombieSOAM

Procedure 19. 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. The InhibitRepPlans field for all the MP servers for the selected site, for example, Site SO_HPC03 is set as **A B**.

\$ sudo iqt NodeInfo

Example output:

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

Appendix E. Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost)**Procedure 20. Inhibit A and B Level Replication on C-level Servers**

STEP #	<p>This procedure inhibits A and B level replication on all C-level servers of this site when active, standby, and spare SOAMS are lost</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>Active NOAM:</p> <p>Login</p> <p>Log into the active NOAM server using SSH as admusr.</p>

Procedure 20. Inhibit A and B Level Replication on C-level Servers

2.

Active NOAM:

Inhibit replication on all C-level servers

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

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

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

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

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

Note:

SOAM_SG_NAME 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	<table><tr><td colspan="3">Network Element: DSR_DR_NO_NE</td></tr><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>	Network Element: DSR_DR_NO_NE			Server	Node HA Pref	VIPs	DRNOAM1			DRNOAM2		
Network Element: DSR_DR_NO_NE																	
Server	Node HA Pref	VIPs															
DRNOAM1																	
DRNOAM2																	
NO_SG	A	NONE	DSR (active/standby pair)	1	<table><tr><td colspan="3">Network Element: DSR_NO_NE</td></tr><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>	Network Element: DSR_NO_NE			Server	Node HA Pref	VIPs	NOAM1			NOAM2		
Network Element: DSR_NO_NE																	
Server	Node HA Pref	VIPs															
NOAM1																	
NOAM2																	
SO_SG	B	NO_SG	DSR (active/standby pair)	1	<table><tr><td colspan="3">Network Element: DSR_SO_NE</td></tr><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>	Network Element: DSR_SO_NE			Server	Node HA Pref	VIPs	SOAM1			SOAM2		
Network Element: DSR_SO_NE																	
Server	Node HA Pref	VIPs															
SOAM1																	
SOAM2																	

3.

Active NOAM:

Verify replication has been inhibited

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

Verify replication inhibition on MPs by analyzing NodeInfo output.

InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO_SG is set as **A B**.

Execute this command:

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

Procedure 21. 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><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></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><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></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><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></div>	Server	Node HA Pref	VIPs	SOAM1			SOAM2		
Server	Node HA Pref	VIPs												
SOAM1														
SOAM2														

Procedure 21. 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 22. Restore TVOE Configuration from Backup Media**

STEP #		
1. <input type="checkbox"/>	Install TVOE application	<ul style="list-style-type: none"> If the PMAC is NOT hosted on the failed rack mount server, execute IPM Servers Using PMAC Application from reference [10]. If the PMAC is hosted on the failed rack mount server, execute Installing TVOE on the Management Server from reference [10].
2. <input type="checkbox"/>	Establish network connectivity	<ul style="list-style-type: none"> If the PMAC is NOT hosted on the failed rack mount server, skip this step. If the PMAC is hosted on the failed rack mount server, execute TVOE Network Configuration, steps 1-11, from reference [10]. <p>Note: 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"> Execute Application NetBackup Client Installation Procedures from reference [8]. Interface with the NetBackup master server and initiate a restore of the TVOE backup ISO image. <p>Note: Once restored, the ISO image is in /var/TKLC/bkp/ on the TVOE server.</p>

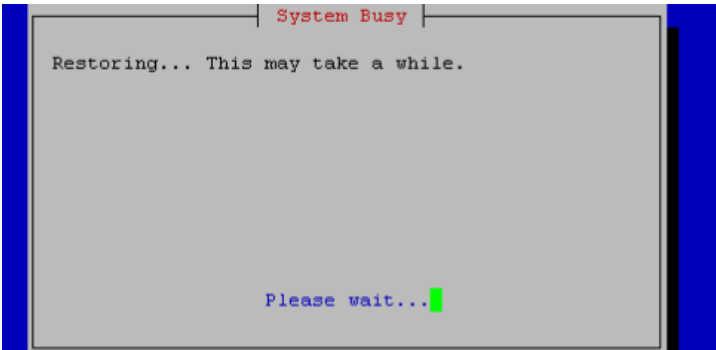
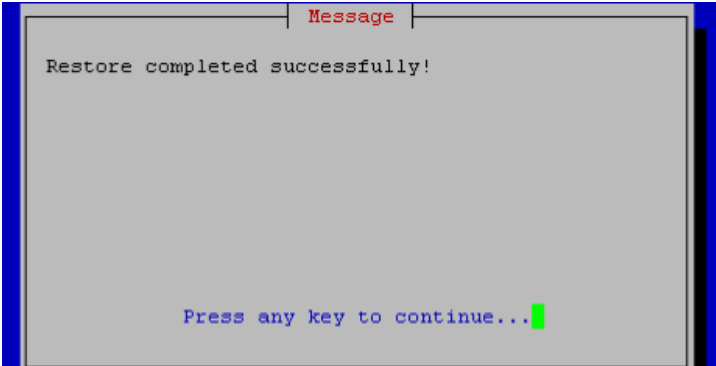
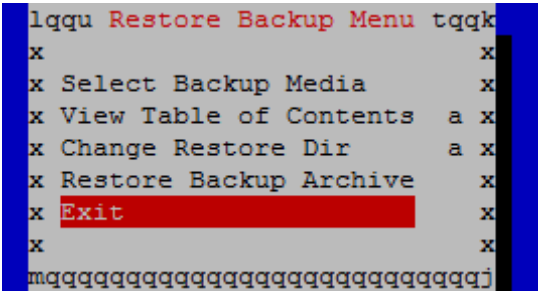
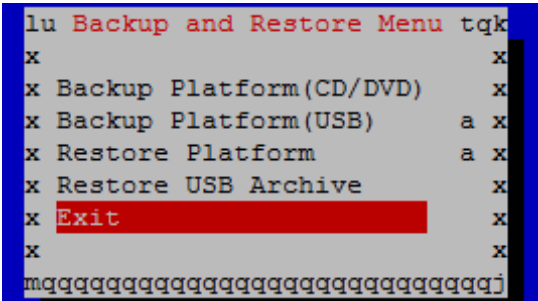
Procedure 22. Restore TVOE Configuration from Backup Media

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>Linux:</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 <path_to_image> tvoexfer@<TVOE_IP>:backup/</pre> <p>where <path_to_image> is the path to the backup ISO image on the local system and <TVOE_IP> is the TVOE IP address.</p> <p>Notes:</p> <ul style="list-style-type: none"> • If the IP is an IPv4 address, then <TVOE_IP> is a normal dot-decimal notation (for example, 10.240.6.170). • If the IP is an IPv6 link local address, then <TVOE_IP> needs to be scoped. For example, [fe80::21e:bff:fe76:5e1c%control] where control is the name of the interface on the machine initiating the transfer and it must be on the same link as the interface on the TVOE host. • The control IP address of the TVOE can be used if the TVOE is NOT hosting the PMAC. This method requires first transferring the backup file to the PMAC, and then to the TVOE host. <p>IPv4 Example:</p> <pre># scp /path/to/image.iso tvoexfer@10.240.6.170:backup/</pre> <p>IPv6 Example:</p> <pre># scp /path/to/image.iso tvoexfer@[fe80::21e:bff:fe76:5e1c%control]:backup/</pre> <p>Windows:</p> <p>Use WinSCP to copy the Backup ISO image into the /var/TKLC/bkp directory. Refer to [10], the Using WinSCP procedure, to copy the backup image to the customer system.</p>
5. <input type="checkbox"/>	TVOE Server: Login	Establish an SSH session to the TVOE server and login as admusr .

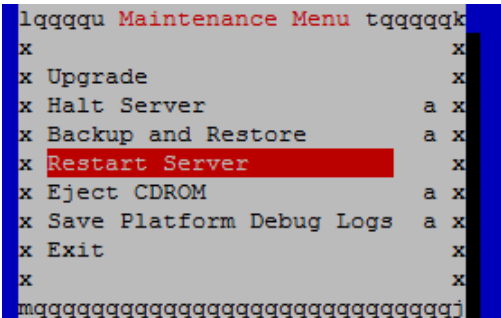
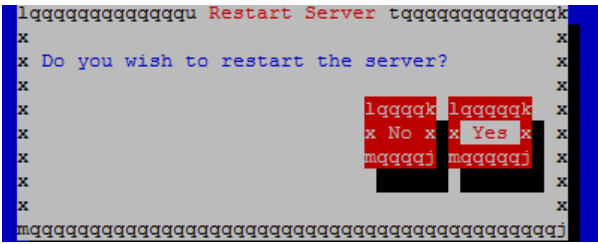
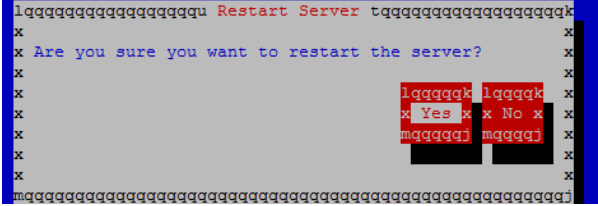
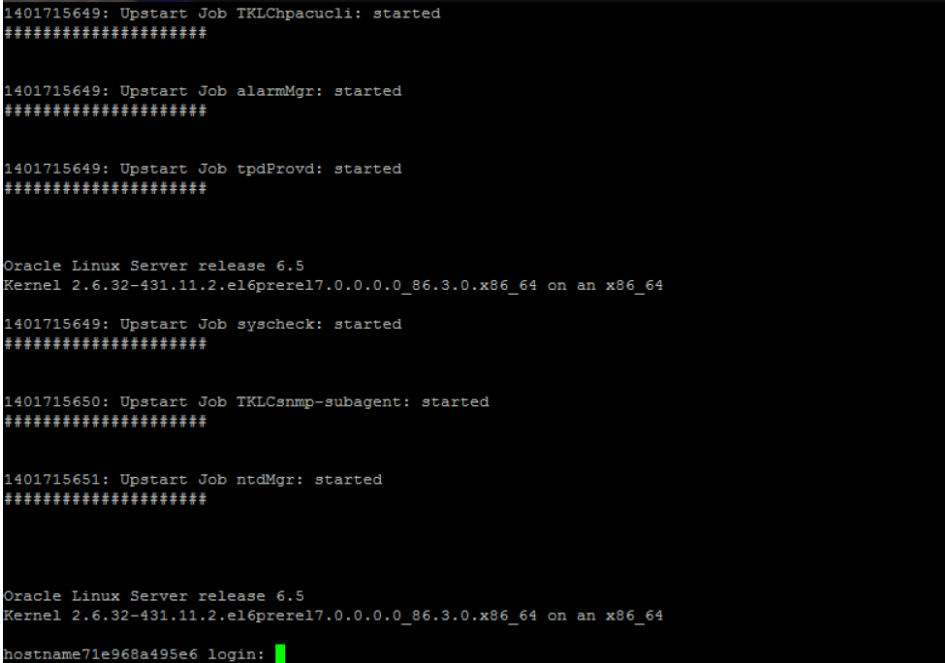
Procedure 22. Restore TVOE Configuration from Backup Media

6.	Restore TVOE backup ISO image	<ol style="list-style-type: none"> Restore the TVOE backup ISO by executing this command: <div data-bbox="490 294 1042 340" data-label="Text"> <pre>\$ sudo su - platcfg</pre> </div> Navigate to Maintenance > Backup and Restore > Restore Platform > Select Backup Media. <div data-bbox="490 424 1026 688" data-label="Image"> <p>A terminal window titled 'lqqu Restore Backup Menu tqgk' with a blue border. The menu options are: 'x', 'x Select Backup Media x', 'x View Table of Contents x', 'x Change Restore Dir a x', 'x Restore Backup Archive a x', 'x Exit x', and 'x'. The option 'Select Backup Media' is highlighted with a red background.</p> </div> Select the desired archive. <div data-bbox="490 739 1393 970" data-label="Image"> <p>A terminal window titled 'lqqu Restore Backup Menu tqgk' with a blue border. The menu options are: 'x', 'x Select Backup Media x', 'x View Table of Contents x', 'x Change Restore Dir a x', 'x Restore Backup Archive a x', 'x Exit x', and 'x'. The option 'Restore Backup Archive' is highlighted with a red background.</p> </div> Click OK. Click Restore Backup Archive. <div data-bbox="490 1075 1026 1381" data-label="Image"> <p>A terminal window titled 'lqqu Restore Backup Menu tqgk' with a blue border. The menu options are: 'x', 'x Select Backup Media x', 'x View Table of Contents a x', 'x Change Restore Dir x', 'x Restore Backup Archive a x', 'x Exit x', and 'x'. The option 'Restore Backup Archive' is highlighted with a red background.</p> </div> Confirm restore. <div data-bbox="490 1432 1393 1686" data-label="Image"> <p>A terminal window titled 'lqqu Restore Backup Menu tqgk' with a blue border. The menu options are: 'x', 'x Select Backup Media x', 'x View Table of Contents a x', 'x Change Restore Dir x', 'x Restore Backup Archive a x', 'x Exit x', and 'x'. The option 'Restore Backup Archive' is highlighted with a red background.</p> </div>
----	-------------------------------	---

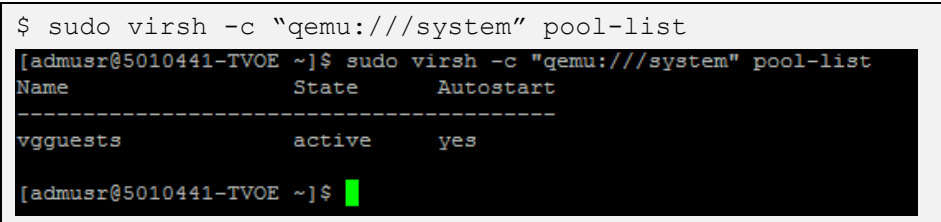
Procedure 22. Restore TVOE Configuration from Backup Media

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

Procedure 22. Restore TVOE Configuration from Backup Media

9. <input type="checkbox"/>	TVOE Server: Restart	<ol style="list-style-type: none"> Restart the TVOE server.  Click Yes to restart.  Confirm restart. 
10. <input type="checkbox"/>	TVOE Server: Wait for restart to successfully complete	

Procedure 22. Restore TVOE Configuration from Backup Media

11. <input type="checkbox"/>	TVOE Server: Verify storage pools are active	<ol style="list-style-type: none"> 1. Login as admusr. 2. Verify all storage pools are listed and are in the active state: <pre>\$ sudo virsh -c "qemu:///system" pool-list</pre>  <pre>[admusr@5010441-TVOE ~]\$ sudo virsh -c "qemu:///system" pool-list Name State Autostart ----- vggquests active yes [admusr@5010441-TVOE ~]\$</pre> <p>Note: If any storage pools are missing or inactive, contact My Oracle Support (MOS).</p>
12. <input type="checkbox"/>	TVOE Server: Enable HIDS (Optional)	<p>Note: 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 New State: ENABLED \$ /usr/TKLC/plat/bin/hidsMgr --update --all HIDS baseline has successfully been updated</pre>

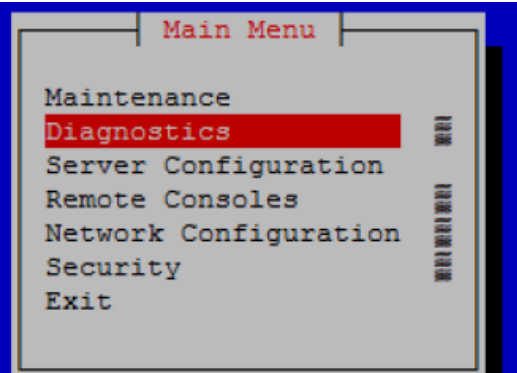
Procedure 22. Restore TVOE Configuration from Backup Media

13. **TVOE Server:**
☐ Verify alarms

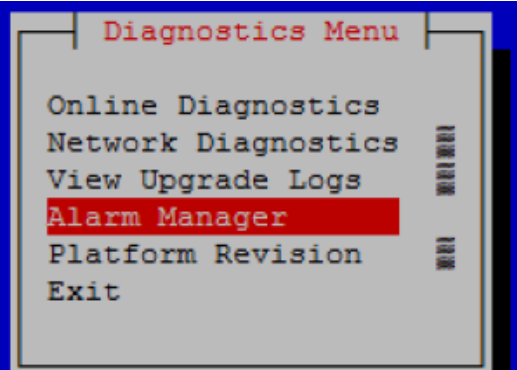
1. Verify alarms:

```
$ sudo su - platcfg
```

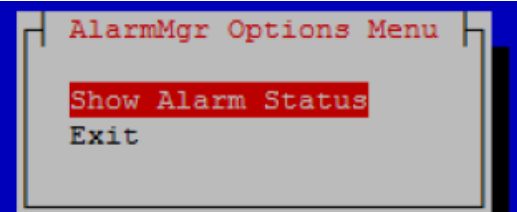
2. Click **Diagnostics**.



3. Click **Alarm Manager**.



4. Click **Show Alarm Status**.




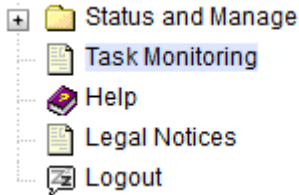
If there are any failures, contact My Oracle Support (MOS).

Appendix H. Restore PMAC from Backup

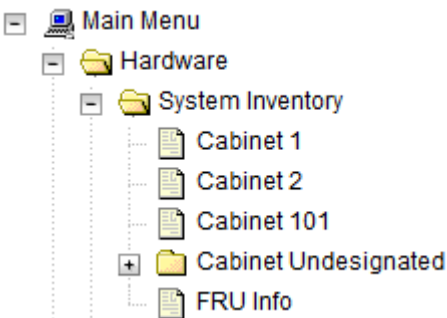
Procedure 23. Restore PMAC from Backup Media

S T E P #	This procedure provides steps to restore the PMAC application configuration from backup media. Prerequisite: TVOE management server has been restored. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. <input type="checkbox"/>	Deploy the PMAC guest	Execute Install PMAC from reference [10].
2. <input type="checkbox"/>	PMAC: Login	Establish an SSH session to the PMAC server and login as admusr .
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. This example is a simple scp from a redundant PMAC backup location. If using IPv6 addresses, the command requires shell escapes, for example, <code>admusr@[<ipV6addr>]:/<file></code></p> <p>Note: Execute the scp command from the recovered PMAC and the backup file is pulled/retrieved from the backup location.</p> <pre>\$ sudo /usr/bin/scp -p \ admsur@<remoteserver>:/var/TKLC/smac/backup/*.pef \ /var/TKLC/smac/backup/</pre> <p>Note: It is important to copy the correct backup file to use in the restore. The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PMAC before the restoration of the data.</p>
4. <input type="checkbox"/>	PMAC: Verify no Alarms are present	<p>Verify no alarms are present.</p> <pre>\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre>
5. <input type="checkbox"/>	Restore the PMAC Data from Backup	<p>1. Restore the PMAC data from backup.</p> <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm restore PM&C Restore been successfully initiated as task ID 1</pre> <p>2. Check the status of the background task.</p> <pre>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</pre> <p>Note: The result eventually displays PMAC Restore successful.</p>

Procedure 23. Restore PMAC from Backup Media

6. <input type="checkbox"/>	PMAC GUI: Login	<ol style="list-style-type: none"> 1. Open web browser and navigate to the PMAC GUI. 2. Login as PMACadmin user: <div data-bbox="467 338 1026 386" style="border: 1px solid black; padding: 2px;"> https://<pmac_network_ip> </div> <div data-bbox="475 411 1425 1167">  <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, Oracle and/or its affiliates. All rights reserved.</p> </div>
7. <input type="checkbox"/>	PMAC GUI: Verify restore task completed	<ol style="list-style-type: none"> 1. Navigate to Task Monitoring.  2. Verify the restore background task completed successfully. <p>Note: After the restore is complete, you should see Add Enclosure tasks start for all previously provisioning servers. These should be allowed to complete before continuing.</p> <p>Note: After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior. ISO images are added in the next step.</p>

Procedure 23. Restore PMAC from Backup Media

8. <input type="checkbox"/>	PMAC GUI: Verify system inventory	1. Navigate to Hardware > System Inventory .  2. Verify previously provisioned enclosures are present.
9. <input type="checkbox"/>	PMAC: 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"/>	PMAC: Add ISO images to the PMAC	Re-add any needed ISO images to the PMAC by executing procedure Load DSR, SDS (Oracle X5-2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only), and TPD ISOs to the PMAC Server from reference [8] for all required ISO images.

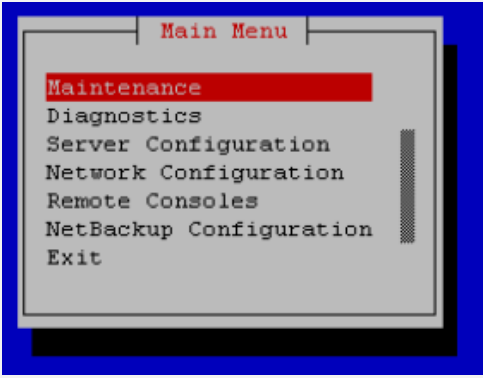
Procedure 24. Restore PMAC from Backup Server

S T E P #	<p>This procedure provides steps to restore the PMAC application configuration from backup server. Prerequisite: 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 Install PMAC from reference [10].</p> <p>Note: 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"/>	PMAC TVOE Host: Login	Establish an SSH session to the PMAC TVOE Host, login as admusr .
3. <input type="checkbox"/>	PMAC TVOE Host: 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 <PMAC-VMID></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 CTRL +].</p>

Procedure 24. Restore PMAC from Backup Server

5. <input type="checkbox"/>	PMAC: 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 24. Restore PMAC from Backup Server

6. <input type="checkbox"/>	PMAC: 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>Note: In the example image above of the TPD platcfg utility Main Menu the backup menu is identified as NetBackup Configuration.</p>
7. <input type="checkbox"/>	PMAC: 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. <input type="checkbox"/>	PMAC: Install backup utility client software on the PMAC guest	<p>Execute PMAC NetBackup Client Installation and Configuration from reference [10] starting at step 4.</p> <p>Note: The Initialize PMAC Application and Configure PMAC Application prerequisites can be ignored.</p>
9. <input type="checkbox"/>	Backup server: verify appropriate PMAC backup exists	<p>This step is likely executed by customer IT personnel.</p> <ol style="list-style-type: none"> 1. Log into the backup server as the appropriate user using the user password. 2. Execute the appropriate commands to verify the PMAC backup exists for the desired date. <p>Note: The actions and commands required to verify the PMAC backups exist and the commands required to perform backup and restore on the backup server are the responsibility of the site customer.</p> <p>Note: It is important to select the correct backup file to use in the restore. The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PMAC before the restoration of the data.</p>

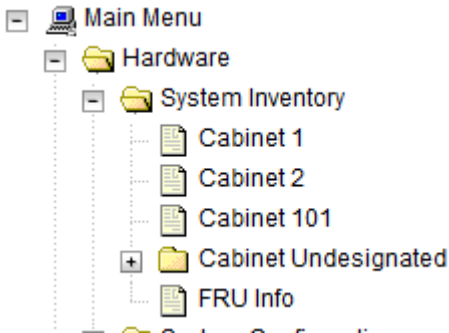
Procedure 24. Restore PMAC from Backup Server

10. <input type="checkbox"/>	Backup Server: Verify appropriate PMAC backup exists	<p>This step is likely executed by customer IT personnel.</p> <ol style="list-style-type: none"> 1. Log into the backup server as the appropriate user using the user password. 2. Execute the appropriate commands to verify the PMAC backup exists for the desired date. 3. Execute the appropriate commands to restore the PMAC management server backup for the desired date. <p>Note: The actions, and commands, required to verify the PMAC backups exist, and the commands required to perform backup and restore on the backup server are the responsibility of the site customer.</p>
11. <input type="checkbox"/>	PMAC: 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"> 1. Restore the PMAC data from backup. <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm restore</pre> <p>PM&C Restore been successfully initiated as task ID 1</p> 2. Check the status of the background task: <pre>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</pre> <p>Note: The result eventually displays PMAC Restore successful.</p>

Procedure 24. Restore PMAC from Backup Server

13. <input type="checkbox"/>	PMAC GUI: Login	<ol style="list-style-type: none"> 1. Open web browser and navigate to the PMAC GUI. <div data-bbox="488 289 1049 340" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> https://<pmac_network_ip> </div> 2. Login as PMACadmin user: <div data-bbox="488 409 1446 1165" 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 instruction 'Enter your username and password to log in'. It contains fields for 'Username:' and 'Password:', a 'Change password' link, 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. 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>
14. <input type="checkbox"/>	PMAC GUI: Verify restore task completed	<ol style="list-style-type: none"> 1. Navigate to Task Monitoring. <div data-bbox="488 1249 803 1438" style="border: 1px solid black; padding: 5px; margin: 5px 0;">  <p>The screenshot shows a sidebar menu with the following items: 'Status and Manage' (with a folder icon), 'Task Monitoring' (with a document icon and highlighted in blue), 'Help' (with a question mark icon), 'Legal Notices' (with a document icon), and 'Logout' (with a door icon).</p> </div> 2. Verify the restore background task completed successfully. <p>Note: After the restore is complete, you should see Add Enclosure tasks start for all previously provisioning servers. These should be allowed to complete before continuing.</p> <p>Note: After the restore is complete, you may see some tasks mentioning ISO images being deleted. This is normal behavior. ISO images are added in the next step.</p>

Procedure 24. Restore PMAC from Backup Server

15. <input type="checkbox"/>	PMAC GUI: Verify system inventory	<p>1. Navigate to Hardware > System Inventory.</p>  <p>2. Verify previously provisioned enclosures are present</p>
16. <input type="checkbox"/>	PMAC: Verify PMAC	<p>Perform a system health check on the PMAC.</p> <pre>\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre> <p>This command should return no output on a healthy system.</p> <pre>\$ sudo /usr/TKLC/smac/bin/sentry status</pre> <p>All processes should be running, displaying output similar to the following:</p> <pre>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.</pre>
17. <input type="checkbox"/>	PMAC: Add ISO images to the PMAC	<p>Re-add any needed ISO images to the PMAC by executing procedure Load Application and TPD ISO onto PMAC Server from reference [8].</p>

Appendix I. Configure TVOE Hosts

Procedure 25. Configure TVOE

STEP#

This procedure configures networking on TVOE hosts.
Prerequisite: Server has been IPM'ed with TVOE OS as described in [10].
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.
☐

Determine bridge names and interfaces for XMI and IMI, and NetBackup (if used) networks

1. Determine the bridge names and physical bridge interfaces to be used on the TVOE server for the NOAM XMI and IMI networks.

2. Based on the site survey, determine if you are using VLAN tagging or not, what bonds are used, and also the actual Ethernet interfaces that make up those bonds.

3. If the NetBackup bridge and interface were not previously configured on this server when PMAC was installed, determine those values as well.

4. Fill in the appropriate values in the table below:

NOAM Guest Interface Name	TVOE Bridge Name	TVOE Bridge Interface
xmi	xmi	<div>Interface Bond (for example, bond0, bond1, etc.): <input type="text"/></div> <div><TVOE_XMI_Bridge_Interface_Bond></div> <div>Interface Name (for example, bond0.3, bond1, bond0.100): <input type="text"/></div> <div><TVOE_XMI_Bridge_Interface></div>
imi	imi	<div>Interface Bond:(for example, bond0, bond1, etc.): <input type="text"/></div> <div><TVOE_IMI_Bridge_Interface_Bond></div> <div>Interface Name: (for example, bond0.4, bond1, bond0.100): <input type="text"/></div> <div><TVOE_IMI_Bridge_Interface</div>
NetBackup	NetBackup	<div>Interface Name (for example, eth11, eth04, eth03, etc.): <input type="text"/></div> <div><TVOE_NetBackup_Bridge_Interface></div>
management	management	<div>Interface Name (for example, bond0.2, bond0.37, etc.): <input type="text"/></div> <div><TVOE_Mgmt_Bridge_Interface></div>

2.
☐

RMS Server: Login

Log in to the TVOE prompt of the RMS server as **admusr** using the iLO facility.

Procedure 25. Configure TVOE

3. <input type="checkbox"/>	RMS Server: Configure XMI bridge interface bond	<p>1. Verify the XMI bridge interface bond.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm query --device=<TVOE_XMI_Bridge_Interface_Bond> Protocol: none On Boot: yes Persistent: yes Bonded Mode: active-backup Enslaving: eth01 eth02</pre> <p>If the bond has already been configured, output, similar to what you see above, displays. If this is so, skip to the next step; otherwise, continue with this step.</p> <p>2. Create bonding interface and associate subordinate interfaces with bond:</p> <p>Note: The output below is for illustrative purposes only. The example output shows the control bridge configured.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_XMI_Bridge_Interface_Bond> --onboot=yes --type=Bonding --mode=active-backup --miimon=100 Interface <TVOE_XMI_Bridge_Bond> added \$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_XMI_Bridge_Bond_Ethernet1> --type=Ethernet --master=<TVOE_XMI_Bridge_Interface_Bond> --slave=yes --onboot=yes Interface <TVOE_XMI_Bridge_Bond_Ethernet1> updated \$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_XMI_Bridge_Bond_Ethernet2> --type=Ethernet --master=<TVOE_XMI_Bridge_Interface_Bond> --slave=yes --onboot=yes Interface <TVOE_XMI_Bridge_Bond_Ethernet2> updated \$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES -- val=<TVOE_XMI_Bridge_Interface_Bond>, [bondX, bondX+1, ..., bondN]</pre> <p>Note: All other existing bonds should be included in the val= statement, for example, if TVOE_XMI_Bridge_Bond = bond1, val=bond0,bond1.</p> <pre>\$ sudo syscheckAdm net ipbond -enable</pre>
--------------------------------	---	---

Procedure 25. Configure TVOE

4. <input type="checkbox"/>	RMS Server: Create XMI bridge interface, if needed. (Only for VLAN tagging interfaces)	<p>If you are using VLAN tagging for the XMI bridge interface, then you must create the VLAN interface first.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_XMI_Bridge_Interface> --onboot=yes Interface <TVOE_XMI_Bridge_Interface> created.</pre>
5. <input type="checkbox"/>	RMS Server: Create XMI bridge	<p>Now , create the XMI bridge:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge -- name=xmi --onboot=yes --bridgeInterfaces=<TVOE_XMI_Bridge_Interface> Interface <TOE_XMI_Bridge_Interface> updated. Bridge xmi created.</pre>

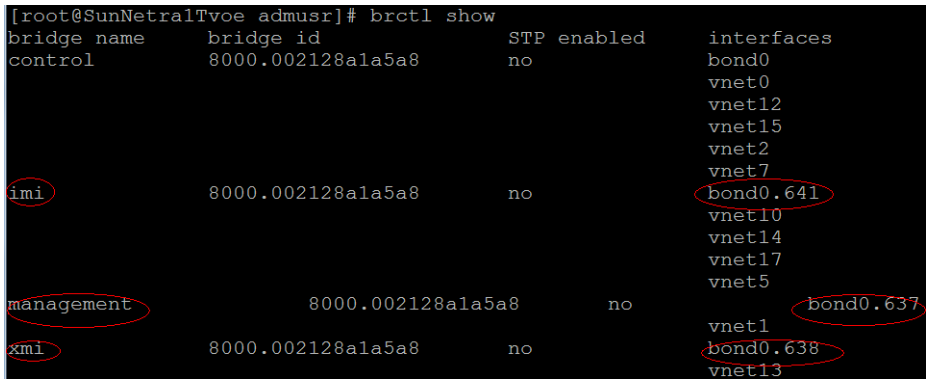
Procedure 25. Configure TVOE

6. <input type="checkbox"/>	RMS Server: Configure IMI bridge interface bond	<p>1. Verify the IMI bridge interface bond.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm query --device=<TVOE_IMI_Bridge_Interface_Bond> Protocol: none On Boot: yes Persistent: yes Bonded Mode: active-backup Enslaving: eth01 eth02</pre> <p>Note: The output below is for illustrative purposes only. The example output shows the control bridge configured.</p> <p>If the bond has already been configured, output, similar to what you see above, displays. If this is so, skip to the next step; otherwise, continue with this step.</p> <p>2. Create bonding interface and associate subordinate interfaces with bond:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_IMI_Bridge_Interface_Bond> --onboot=yes --type=Bonding --mode=active-backup --miimon=100 Interface <TVOE_IMI_Bridge_Bond> added \$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_IMI_Bridge_Bond_Ethernet1> --type=Ethernet --master=<TVOE_IMI_Bridge_Bond> --slave=yes --onboot=yes Interface <TVOE_IMI_Bridge_Bond_Ethernet1> updated \$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_IMI_Bridge_Bond_Ethernet2> --type=Ethernet --master=<TVOE_IMI_Bridge_Bond> --slave=yes --onboot=yes Interface <TVOE_IMI_Bridge_Bond_Ethernet2> updated</pre> <p>3. Execute these 2 commands ONLY IF <TVOE_XMI_Bridge_Bond> is different from <TVOE_IMI_Bridge_Bond>.</p> <pre>\$ sudo syscheckAdm net ipbond --set --var=DEVICES --val=<TVOE_XMI_Bridge_Interface_Bond>, <TVOE_IMI_Bridge_Interface_Bond>,[other bonds...]</pre> <pre>\$ sudo syscheckAdm net ipbond -enable</pre>
7. <input type="checkbox"/>	RMS Server: Create IMI bridge interface	<p>If you are using VLAN tagging for the IMI bridge interface, then you must create the VLAN interface first.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_IMI_Bridge_Interface> --onboot=yes Interface <TVOE_IMI_Bridge_Interface> created.</pre>

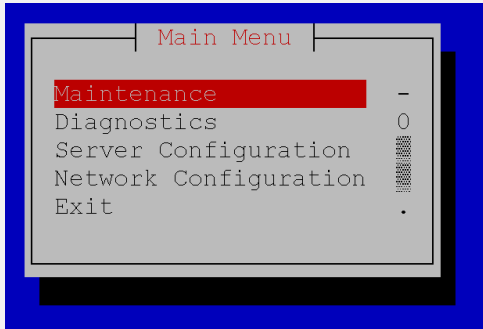
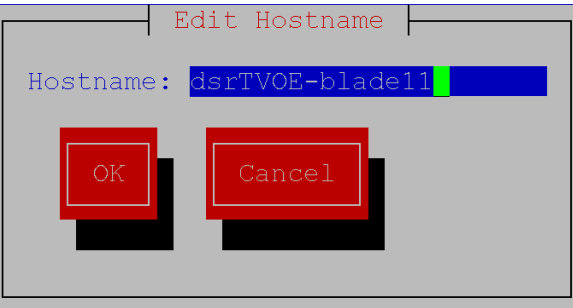
Procedure 25. Configure TVOE

8. <input type="checkbox"/>	RMS Server: Create IMI bridge	<p>Create the IMI bridge:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge -- name=imi --onboot=yes --bridgeInterfaces=<TVOE_IMI_Bridge_Interface> Interface <TVOE_IMI_Bridge_Interface> updated. Bridge imi created.</pre>
9. <input type="checkbox"/>	RMS Server iLO: Create management bridge and assign TVOE management IP	<ol style="list-style-type: none"> 1. Execute this step only if the TVOE host is a rack mount server and is NOT the PMAC server. Note: The output below is for illustrative purposes only. The site information for this system determines the network interfaces (network devices, bonds, and bond enslaved devices) to configure. 2. If <TVOE_Management_Bridge_Interface>, or the bond it is based on (if using tagged interface), has not yet been created, then execute the next 3 commands; otherwise, skip to the EXAMPLE section: <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Mgmt_Bridge_Interface_Bond> --onboot=yes --type=Bonding --mode=active-backup --miimon=100 Interface <TVOE_Management_Bridge_Interface> added</pre> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_Mgmt_Bridge_Bond_Interface1> --type=Ethernet --master=<TVOE_Mgmt_Bridge_Interface_Bond> --slave=yes --onboot=yes Interface <mgmt_ethernet_interface1> updated.</pre> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --device=<TVOE_Mgmt_Bridge_Bond_Interface2> --type=Ethernet --master=<TVOE_Mgmt_Bridge_Interface_Bond> --slave=yes --onboot=yes Interface <mgmt_ethernet_interface2> updated</pre> <p>EXAMPLE 1: Create Management bridge using untagged interfaces</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=management --bootproto=none --onboot=yes --address=<TVOE_Mgmt_IP_Address> --netmask=<TVOE_Mgmt_Netmask/Prefix> --bridgeInterfaces=<TVOE_Mgmt_Bridge_Interface></pre> <p>EXAMPLE 2: Create Management bridge using tagged interfaces</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Management_Bridge_Interface> \$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge</pre>

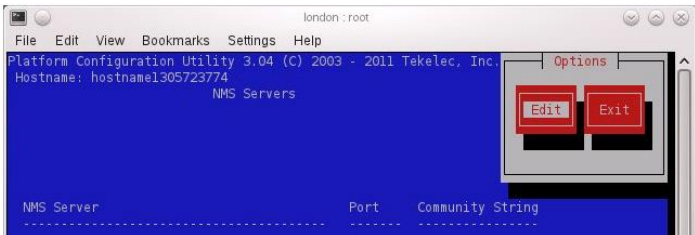

Procedure 25. Configure TVOE

		<pre>--name=management --address=<TVOE_Mgmt_IP_Address> --netmask=<TVOE_Mgmt_Netmask/Prefix> --onboot=yes --bridgeInterfaces=<TVOE_Mgmt_Bridge_Interface></pre>
10.	RMS Server iLO: Add default route	<p>Add a default route using the xmi or management address (if configured).</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=default --gateway=<TVOE_Mgmt_gateway_IP_address> --device=<management or xmi></pre> <p>Route to management created.</p>
11.	RMS Server: Verify bridge creation status	<p>Verify the XMI and IMI bridges have been created successfully.</p> <pre>\$ brctl show</pre> <p>Example output:</p>  <pre>[root@SunNetra1Tvoe admusr]# brctl show bridge name bridge id STP enabled interfaces control 8000.002128a1a5a8 no bond0 8000.002128a1a5a8 no vnet0 8000.002128a1a5a8 no vnet12 8000.002128a1a5a8 no vnet15 8000.002128a1a5a8 no vnet2 8000.002128a1a5a8 no vnet7 imi 8000.002128a1a5a8 no bond0.641 8000.002128a1a5a8 no vnet10 8000.002128a1a5a8 no vnet14 8000.002128a1a5a8 no vnet17 8000.002128a1a5a8 no vnet5 management 8000.002128a1a5a8 no vnet1 8000.002128a1a5a8 no bond0.637 8000.002128a1a5a8 no bond0.638 xmi 8000.002128a1a5a8 no vnet13 8000.002128a1a5a8 no vnet13</pre> <ul style="list-style-type: none"> • Verify imi and xmi are listed under the bridge name column. • Verify <TVOE_XMI_Bridge_Interface> is listed under the interfaces column for xmi. • Verify <TVOE_IMI_Bridge_Interface> is listed under the interfaces column for imi. • Verify the <TVOE_Mgmt_Bridge_Interface> is listed under the interface column for <TVOE_Mgmt_Bridge_Interface>
12.	RMS Server iLO: Create NetBackup bridge (Optional)	<p>Perform this command if you have a dedicated NetBackup interface within your NOAM guests (and if the NetBackup bridge was NOT configured when setting up the PMAC earlier).</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=NetBackup --onboot=yes --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface></pre>

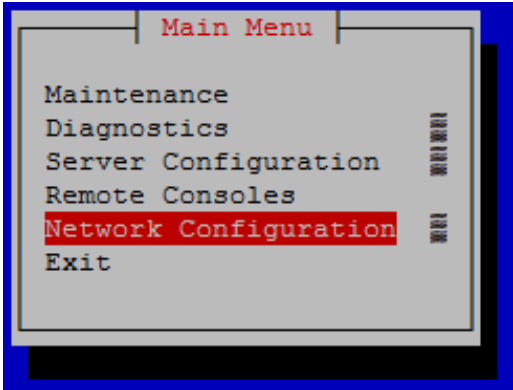
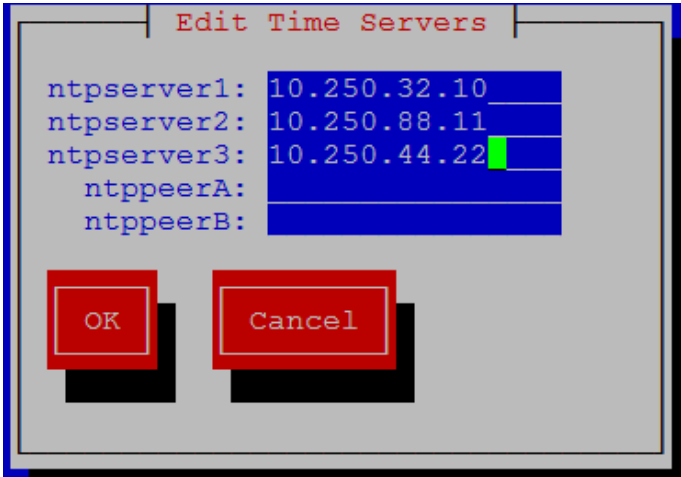
Procedure 25. Configure TVOE

<div data-bbox="180 239 430 283">13. RMS Server</div> <div data-bbox="180 283 430 325"><input type="checkbox"/> iLO: Set</div> <div data-bbox="180 325 430 1171">hostname</div>	<div data-bbox="446 239 1339 619"><pre>\$ sudo su - platcfg</pre></div> <div data-bbox="446 619 1339 693"><p>1. Navigate to Server Configuration > Hostname > Edit and enter a new hostname for your server:</p></div> <div data-bbox="446 693 1031 1018"></div> <div data-bbox="446 1018 1443 1060"><p>2. Click OK and continue to click Exit until you are at the platcfg main menu again.</p></div> <div data-bbox="446 1060 1443 1171"><p>Note: Although the new hostname has been properly configured and committed at this point, it does not display on your command prompt unless you log out and log back in again.</p></div>
---	--


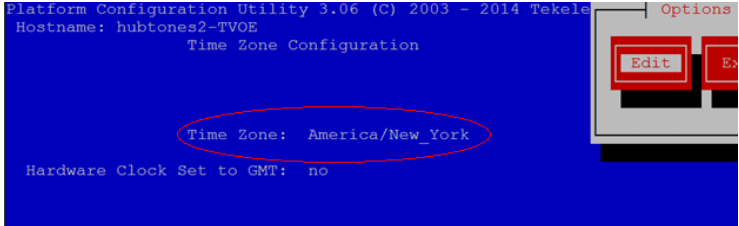
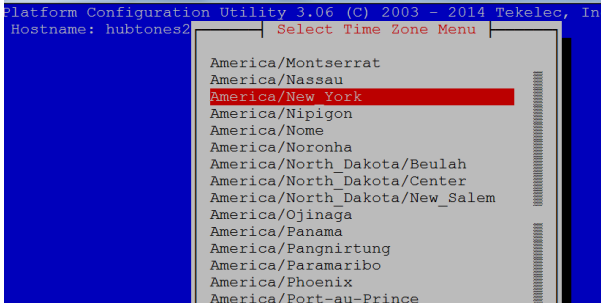
Procedure 25. Configure TVOE

14.	RMS Server iLO: Configure SNMP	<ol style="list-style-type: none"> From the platcfg main menu, navigate to Network Configuration > SNMP Configuration > NMS Configuration.  <ol style="list-style-type: none"> Click Edit. Click Add a New NMS Server.  <ol style="list-style-type: none"> Enter the following NMS servers, clicking OK after each one and then selecting the Add NMS option again: <ul style="list-style-type: none"> Enter the Hostname/IP of the customer NMS server, for port enter 162, and for Community String enter the community string provided in the customer NAPD Document. Enter the IP of the NOAM VIP, for port enter 162, and for Community String enter the community string provided in the customer NAPD Document Click Exit. Click Yes when prompted to restart the Alarm Routing Service. Once Done, click Exit to quit to the platcfg main menu.
-----	--	--

Procedure 25. Configure TVOE


<p>15. RMS Server <input type="checkbox"/> iLO: Configure NTP</p>	<ol style="list-style-type: none"> 1. Select Network Configuration.  2. Select NTP. 3. Click Edit.  <ul style="list-style-type: none"> • ntpserver1: Enter customer provided NTP server #1 IP address. • ntpserver2: Enter customer provided NTP server #2 IP address. • ntpserver3: Enter customer provided NTP server #3 IP address. 4. Click OK. 5. Click Exit to return to the platcfg menu.
--	---

Procedure 25. Configure TVOE

16.	RMS Server iLO: Configure timezone	<pre>\$ sudo su - platcfg</pre> <p>1. Navigate to Server Configuration > Time Zone.</p>   <p>2. If the time zone displayed matches the time zone you desire, then you can continue to hit Exit until you are out of the platcfg program. If you want a different time zone, then proceed with this instruction.</p> <p>3. Click Edit.</p>  <p>4. Select the desired time zone from the list and click Enter.</p> <p>5. Continue clicking Exit until you are out of the platcfg program.</p>
17.	RMS Server iLO: Reboot server	Reboot the server. <pre>\$ sudo su - platcfg</pre>

Appendix J. Create NOAM/SOAM Virtual Machines

Procedure 26. Create NOAM Guest VMs

S T E P #	<p>This procedure creates a DSR NOAM virtual machine (referred to as a guest) on a TVOE server blade or TVOE RMS. It is repeated for every NOAM server you want to install.</p> <p>Prerequisite: TVOE has been installed and configured on the target blade server or RMS</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"/>	<div> <div> PMAC GUI: Login </div> <div> 1. Open web browser and enter: <div> http://<PMAC_Mgmt_Network_IP> </div> </div> <div> 2. Login as pmacadmin user: </div> <div>  </div> </div>

Procedure 26. Create NOAM Guest VMs

2. **PMAC GUI:**
☐ Navigate to VM management of the target server blade

1. Navigate to **Main Menu > VM Management**.
2. Select the TVOE server blade or rack mounted server from the **VM Entities** listing on the left side of the screen. The selected server’s guest machine configuration displays in the remaining area of the window.

View host on RMS pc5010439

VM Info
Software
Network
Media

Summary
Bridges
Storage Pools
Memory

Host Name: **5010439-TVOE**
Location: **RMS pc5010439**

Guests

Name	Status
Zombie_DSRDR NOAM2	Running
Zombie_DSRNO AM2	Running

3. Click **Create Guest**.

Procedure 26. Create NOAM Guest VMs

3.



PMAC GUI:
Configure VM
guest parameters

1. Click **Import Profile**.

Import Profile

ISO/Profile: DSR-8.0.0.0.0_80.11.0-x86_64 => DSR_NOAMP_LARGE

Num CPUs: **12**

Memory (MBs): **24576**

Virtual Disks:

Prim	Size (MB)	Pool	TPD Dev
✓	102400	vsguests	

NICs:

Bridge	TPD Dev
control	control
imi	imi
xmi	xmi

Select Profile Cancel

2. From the **ISO/Profile** drop-down box, select the entry that matches depending on the hardware that your NOAM VM TVOE server is running on and your preference for NetBackup interfaces:

NOAM VM TVOE Hardware Type(s)	Dedicated Netbackup Interface?	Navigate to Profile (<Application ISO NAME>)
HP DL380 Gen 8 RMS HP BL460 Gen 9 RMS HP BL460 Gen 8 Blade HP BL460 Gen 9 Blade	No	DSR_NOAMP_LARGE
HP DL380 Gen 8 RMS HP BL460 Gen 9 RMS HP BL460 Gen 8 Blade HP BL460 Gen 9 Blade	Yes	DSR_NOAMP_LARGE_NBD

Note: Application_ISO_NAME is the name of the DSR Application ISO to be installed on this NOAM

3. Click **Select Profile**.


4. Click **Create**

Create Import Profile Cancel

Procedure 26. Create NOAM Guest VMs

4.	PMAC GUI: Wait for guest creation to complete	<ol style="list-style-type: none"> 1. Navigate to Task Monitoring to monitor the progress of the guest creation task. A separate task displays for each guest creation you start. 2. Wait or refresh the screen until you see the guest creation task has completed successfully. <div data-bbox="500 394 1451 499"> <div>Create Guest</div> <div> RMS: pc5010439 Guest: Zombie_DSRNOAM2 </div> <div>Guest creation completed (Zombie_DSRNOAM2)</div> </div>
5.	PMAC GUI: Verify guest machine is running	<ol style="list-style-type: none"> 1. Navigate to Main Menu > VM Management. 2. Select the TVOE server blade on which the guest machine was just created. 3. Look at the list of guests present on the blade and verify you see a guest that matches the name you configured and that its status is Running. <p>View guest Zombie_DSRNOAM2</p> <div data-bbox="516 741 1198 1318"> <div> VM Info Software Network Media </div> <div> Summary Virtual Disks Virtual NICs </div> <div> <p>Current Power State: Running</p> <p>Set Power State On ▼ Change</p> <p>Guest Name (Required): Zombie_DSRNOAM2</p> <p>Host: RMS: pc5010439</p> <p>Number of vCPUs: 4</p> <p>Memory (MBs): 6,144</p> <p>VM UUID: e9e22407-c289-4d2a-a1f6-6c7121905d40</p> <p>Enable Virtual Watchdog <input checked="" type="checkbox"/></p> </div> <ol style="list-style-type: none"> 4. VM creation for this guest is complete. Repeat from step 2 for any remaining NOAM VMs (for instance, the standby NOAM) that must be created. </div>

Procedure 27. Create SOAM Guest VMs

S T E P #	<p>This procedure creates a DSR SOAM virtual machine (referred to as a guest) on a TVOE server blade. It is repeated for every SOAM server you want to install.</p> <p>Prerequisite: TVOE has been installed and configured on the target blade 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"/>	<p>PMAC GUI: Login</p> <p>1. Open web browser and enter:</p> <div data-bbox="516 527 1318 573" style="border: 1px solid black; padding: 2px; margin: 5px 0;">http://<PMAC_Mgmt_Network_IP></div> <p>2. Login as pmacadmin user:</p> <div data-bbox="477 646 1425 1402" style="text-align: center;">  </div>

Procedure 27. Create SOAM Guest VMs

2. **PMAC GUI:**
□ Navigate to VM management of the target server blade

1. Navigate to **Main Menu > VM Management**.

Software

Software Inventory

Manage Software Images

VM Management

2. Select the TVOE server blade or rack mounted server from the **VM Entities** listing on the left side of the screen. The selected server’s guest machine configuration displays in the remaining area of the window.

VM Info

Software

Network

Media

Summary

Bridges

Storage Pools

Memory

Host Name: 5010439-TVOE

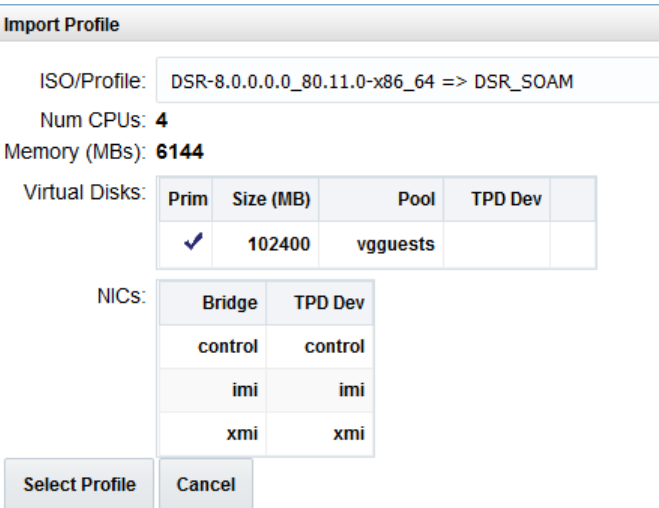
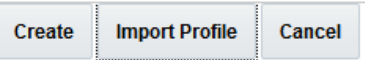

Location: RMS pc5010439

Guests

Name	Status
Zombie_DSRDR NOAM2	Running
Zombie_DSRNO AM2	Running

3. Click **Create Guest**.

Procedure 27. Create SOAM Guest VMs


3. <input type="checkbox"/>	PMAC GUI: Configure VM guest parameters	<ol style="list-style-type: none"> Click Import Profile.  From the ISO/Profile drop-down box, select the entry that matches depending on the hardware that your SOAM VM TVOE server is running on and your preference for NetBackup interfaces. <table border="1" data-bbox="467 915 1344 1222"> <thead> <tr> <th>SOAM VM TVOE Hardware Type(s)</th><th>Dedicated Netbackup Interface?</th><th>Navigate to Profile (<Application ISO NAME>)</th></tr> </thead> <tbody> <tr> <td>HP BL460 Gen 8 Blade, HP BL460 Gen 9 Blade</td><td>No</td><td>DSR_SOAM</td></tr> <tr> <td>HP BL460 Gen 8 Blade, HP BL460 Gen 9 Blade</td><td>Yes</td><td>DSR_SOAM_NBD</td></tr> </tbody> </table> <p>Note: Application_ISO_NAME is the name of the DSR Application ISO to be installed on this SOAM</p> Click Select Profile. Edit the name, if you want. For instance: DSR_SOAM_A or DSR_SOAM_B. This is not the ultimate hostname. It is just an internal tag for the VM host manager. Click Create.  	SOAM VM TVOE Hardware Type(s)	Dedicated Netbackup Interface?	Navigate to Profile (<Application ISO NAME>)	HP BL460 Gen 8 Blade, HP BL460 Gen 9 Blade	No	DSR_SOAM	HP BL460 Gen 8 Blade, HP BL460 Gen 9 Blade	Yes	DSR_SOAM_NBD
SOAM VM TVOE Hardware Type(s)	Dedicated Netbackup Interface?	Navigate to Profile (<Application ISO NAME>)									
HP BL460 Gen 8 Blade, HP BL460 Gen 9 Blade	No	DSR_SOAM									
HP BL460 Gen 8 Blade, HP BL460 Gen 9 Blade	Yes	DSR_SOAM_NBD									
4. <input type="checkbox"/>	PMAC GUI: Wait for guest creation to complete	<ol style="list-style-type: none"> Navigate to Task Monitoring to monitor the progress of the guest creation task. A separate task displays for each guest creation you start. Wait or refresh the screen until you see that the guest creation task has completed successfully.  									

Procedure 27. Create SOAM Guest VMs

<div>5.</div> <div><input type="checkbox"/></div>	<p>PMAC GUI: Verify guest machine is running</p>	<div><div><div>1. Navigate to Main Menu > VM Management.</div><div>2. Select the TVOE server blade on which the guest machine was just created.</div><div>3. Look at the list of guests present on the blade and verify you see a guest that matches the name you configured and that its status is Running.</div></div><div><div><div><div>Virtual Machine Management</div><div><div>Tasks ▾</div><div><div>VM Entities</div><div><div>Refresh</div><div><div>RMS: Jetta-A</div><div><div>Jetta-DAMP</div><div>Jetta-IPFE-A</div><div>Jetta-NO-A</div><div>Jetta-PMAC</div><div>Jetta-SO-A</div></div></div></div><div><div>View VM Guest</div><div><div>Name: Jetta-NO-A</div><div>Host: RMS: Jetta-A</div><div><div>Current Power State: Running</div><div>On ▾ Change</div></div></div><div><div>VM Info</div><div>Software</div><div>Network</div><div>Media</div></div><div><div>Num vCPUs: 4</div><div>Memory (MBs): 6,144</div><div>VM UUID: 913ccfff-ba1f-4844-954f-648ab2fbacda</div><div>Enable Virtual Watchdog: <input checked="" type="checkbox"/></div></div></div></div></div></div></div></div></div>
		<div><div>4. VM creation for this guest is complete. Repeat from Step 2 for any remaining NOAM VMs (for instance, the standby SOAM) that must be created.</div></div>

Appendix K. SNMP Configuration

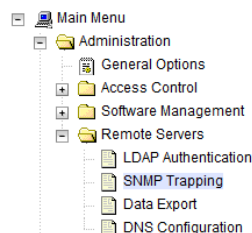
Procedure 28. Configure SNMP

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>NOAM VIP GUI: Login</p> <p>Note: This workaround step should be performed only in the following cases:</p> <ol style="list-style-type: none"> 1. If SNMP is not configured. 2. If SNMP is already configured and SNMPv3 is selected as enabled version. <p>Note: This is a workaround step to configure SNMP with 'SNMPv2c and SNMPv3' as the enabled versions for SNMP Traps configuration, since PMAC does not support SNMPv3.</p> <ol style="list-style-type: none"> 1. If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. 2. Open the web browser and enter a URL of: <div data-bbox="501 909 1307 959" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> http://<Primary_NOAM_VIP_IP_Address> </div> 3. Log into the NOAM GUI as the guiadmin user: <div data-bbox="467 1024 1414 1780" style="text-align: center;">  </div>

Procedure 28. Configure SNMP

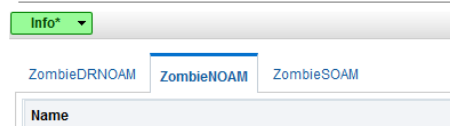
2. **NOAM VIP GUI:**
Configure system-wide SNMP trap receiver(s)

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



2. Select the Server Group tab for SNMP trap configuration:

Main Menu: Administration -> Remote Servers



3. Type the **IP address** or **hostname** of the Network Management Station (NMS) where you want to forward traps. This IP should be reachable from the NOAMP's XMI network. If already configured SNMP with **SNMPv3** as enabled version, another server needs to be configured here.
4. Continue to fill in additional secondary, tertiary, etc., **Manager IPs** in the corresponding slots if desired.

SNMP Trap Configuration Insert for ZombieNOAM

Configuration Mode *	<input checked="" type="radio"/> Global <input type="radio"/> Per-site
Manager 1	<input type="text"/>
Manager 2	<input type="text"/>

5. Set the Enabled Versions as **SNMPv2c and SNMPv3**.

Enabled Versions	SNMPv2c and SNMPv3 ▼
------------------	----------------------

6. Check **Traps Enabled** checkboxes for the Manager servers being configured.


Traps Enabled	<input type="checkbox"/> Manager 1 <input type="checkbox"/> Manager 2 <input type="checkbox"/> Manager 3 <input type="checkbox"/> Manager 4 <input type="checkbox"/> Manager 5
---------------	--

7. Type the **SNMP Community Name**.

SNMPv2c Read-Only Community Name	<input type="text"/>
SNMPv2c Read-Write Community Name	<input type="text"/>

8. Leave all other fields at their default values.
9. Click **OK**.

Procedure 28. Configure SNMP

3.	PMAC GUI: Login	<div data-bbox="451 247 854 279">1. Open web browser and enter:</div> <div data-bbox="505 296 1307 342"><input type="text" value="http://<PMAC_Mgmt_Network_IP>"/></div> <div data-bbox="451 350 795 382">2. Login as guiadmin user:</div> <div data-bbox="735 415 1157 476"></div> <div data-bbox="467 531 719 562">Oracle System Login</div> <div data-bbox="1154 558 1412 579">Tue Jun 7 13:49:06 2016 EDT</div> <div data-bbox="639 623 1240 991"><div data-bbox="898 651 980 682">Log In</div><div data-bbox="693 682 1187 714">Enter your username and password to log in</div><div data-bbox="812 741 1144 772">Username: <input type="text"/></div><div data-bbox="816 798 1144 829">Password: <input type="password"/></div><div data-bbox="893 852 1104 877"><input type="checkbox"/> Change password</div><div data-bbox="849 903 1036 955"><input type="button" value="Log In"/></div></div> <div data-bbox="490 1008 1390 1052">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.</div> <div data-bbox="578 1075 1299 1121"><i>Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</i></div> <div data-bbox="641 1144 1239 1169"><i>Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.</i></div>
----	---------------------------	---

Procedure 28. Configure SNMP

4. <input type="checkbox"/>	PMAC GUI: Update the TVOE host SNMP community string	<ol style="list-style-type: none">1. Navigate to Administration > Credentials > SNMP Community String Update.2. Check the Use Site Specific Read/Write Community String checkbox. <hr/> <p>Select Read Only or Read/Write Community String:</p> <p><input type="radio"/> Read Only <input checked="" type="radio"/> Read/Write</p> <p>Check this box if updating servers using the Site Specific SNMP Community String:</p> <p><input checked="" type="checkbox"/> Use Site Specific Read/Write Community String</p> <p>Community String: <input type="text"/></p> <p>Note: The Community String value can be 1 to 31 uppercase, lowercase, or numeric characters.</p> <hr/> <p><input type="button" value="Update Servers"/></p> <ol style="list-style-type: none">3. Click Update Servers.4. Click OK. <p><small>You are about to update the Read/Write SNMP Credentials on all known supporting TVOE servers and the PM&C guest on the control network of this PM&C. Changing of SNMP Community Strings is only supported across product release versions that support this functionality and attempting to do so with product versions not supporting it may cause the system to become inoperable.</small></p> <p><small>Are you sure you want to continue?</small></p> <p><input type="button" value="OK"/> <input type="button" value="Cancel"/></p>
-----------------------------	--	---

Appendix L. Backup Directory

Procedure 29. Backup Directory

S T E P #	<p>This procedure checks and creates the backup directory.</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>NOAM/SOAM VIP Console: Determine if backup directory exists</p> <ol style="list-style-type: none"> Execute this command an active NOAM/SOAM server console (accessed using the VIP) and compare the output. <div data-bbox="480 632 1417 720" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>\$ cd /var/TKLC/db/filemgmt/ \$ ls -ltr</pre> </div> Look for the backup directory in the output. Make sure the directory is already created with correct permission. The directory looks like this: <div data-bbox="480 850 1417 898" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>drwxrwx--- 2 awadmin awadm 4096 Dec 19 02:15 backup</pre> </div> If the directory is already there with correct permissions, then skip steps 2 and 3. If directory does not have the correct permissions, then go to step 3.
2. <input type="checkbox"/>	<p>NOAM/SOAM VIP Console: Create backup directory</p> <ol style="list-style-type: none"> Go to the backup directory location. <div data-bbox="480 1056 1417 1104" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>cd /var/TKLC/db/filemgmt/</pre> </div> Create backup directory. <div data-bbox="480 1161 1417 1209" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>\$ mkdir backup</pre> </div> Verify directory has been created. <div data-bbox="480 1266 1417 1314" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>\$ ls -ltr /var/TKLC/db/filemgmt/backup</pre> </div> <p>Note: A No such file or directory error message should not display. The directory should show as empty with the total as 0 for content.</p>

Procedure 29. Backup Directory

3. <input type="checkbox"/>	NOAM/SOAM VIP Console: Change permissions of backup directory	1. Verify directory has been created. <pre>\$ ls -ltr /var/TKLC/db/filemgmt/backup</pre> <p>Note: A No such file or directory error message should not display. The directory should show as empty with the total as 0 for content.</p> 2. Change permissions for the backup directory. <pre>\$ chmod 770 /var/TKLC/db/filemgmt/backup</pre> 3. Change ownership of backup directory. <pre>\$ sudo chown -R awadmin:awadm /var/TKLC/db/filemgmt/backup</pre> 4. Directory displays as follows: <pre>drwxrwx--- 2 awadmin awadm 4096 Dec 22 02:15 backup</pre>
4. <input type="checkbox"/>	NOAM/SOAM VIP Console: Copy the backup file to the backup directory	1. Copy the backup file to the backup directory. <pre>\$ cp BACKUPFILE /var/TKLC/db/filemgmt/backup</pre> 2. Change permissions of files in the backup directory. <pre>\$ chmod 666 Backup.*</pre> 3. Change ownership of files in the backup directory. <pre>\$ sudo chown -R awadmin:awadm Backup.*</pre>

Appendix M. My Oracle Support (MOS)**My Oracle Support**

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

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

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

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

Emergency Response

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

coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

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

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

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

Locate Product Documentation on the Oracle Help Center

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

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.