Oracle[®] Communications Diameter Signaling Router

Rack Mount Server Disaster Recovery Guide Release 8.5.1 F51113-01

December 2021



Oracle Communications DSR Rack Mount Server Disaster Recovery User's Guide, Release 8.5.1

Copyright © 2021 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			
	1.1	References	6	
	1.2	Acronyms	6	
	1.3	Terminology	7	
	1.4	How to Use this Document	8	
	1.5	Optional Features	8	
2.	Gen	neral Description	9	
	2.1	Complete Server Outage (All Servers)	10	
	2.2	Partial Server Outage with One NOAM Server Intact and Both SOAMs Failed	10	
	2.3	Partial Server Outage with Both NOAM Servers Failed and One SOAM Server Intact	10	
	2.4	Partial Server Outage with NOAM and One SOAM Server Intact	11	
	2.5	Partial Server Outage with Both NOAMs Failed and DR-NOAM Available	11	
	2.6	Partial Service Outage with Corrupt Database	11	
3.	Pro	cedure Overview	11	
	3.1	Required Materials	11	
	3.2	Disaster Recovery Strategy	12	
4.	Disaster Recovery Procedure		14	
	4.1	Recovery Scenario 1 (Complete Server Outage)	14	
	4.2	Recovery Scenario 2 (Partial Server Outage with One NOAM Server Intact and ALL SOAMs Failed)	56	
	4.3 Recovery Scenario 3 (Partial Server Outage with All NOAM Servers Failed and One SOAM Server Intact)		90	
	4.4 Recovery Scenario 4 (Partial Server Outage with One NOAM Server and One SOAM Server Intact)		123	
4.5 Recovery Scenario 5 (Both NOAM Servers Failed with DR-NOAM Available)		Recovery Scenario 5 (Both NOAM Servers Failed with DR-NOAM Available)	147	
	4.6	Recovery Scenario 6 (Database Recovery)	152	
		4.6.1 Recovery Scenario 6: Case 1	152	
		4.6.2 Recovery Scenario 6: Case 2	158	
5.	Res	olve User Credential Issues after Database Restore	163	
	5.1	Restore a Deleted User	163	
	5.2	Keep a Restored User	163	
	5.3	Remove a Restored User	165	
	5.4	Restore a Modified User	166	
	5.5	Restore an Archive that Does Not Contain a Current User	166	
6.	IDIH	IDIH Disaster Recovery		

Appendix A. DSR Database Backup	177
Appendix B. Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only)	181
Appendix C. Inhibit A and B Level Replication on C-level Servers	183
Appendix D. Un-Inhibit A and B Level Replication on C-level Servers	184
Appendix E. Inhibit A and B Level Replication on C-level Servers (When Active, Standby, and Spare SOAMs are Lost)	185
Appendix F. Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby and Spare SOAMs are Lost)	187
Appendix G. Restore TVOE Configuration from Backup Media	189
Appendix H. Restore PMAC from Backup	197
Appendix I. Restore Provisioning Database	206
Appendix J. Recover PDB Relay	210
Appendix K. SNMP Configuration	211
Appendix L. Backup Directory	214
Appendix M. netConfig backupConfiguration/restoreConfiguration/upgradeFirmware with TPD cipher change	216
Appendix N. My Oracle Support (MOS)	218

List of Tables

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

List of Figures

Figure 1.	Example Procedure Steps Used in This Document	8
Figure 2.	Determining Recovery Scenario 1	3

List of Procedures

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

Procedure 7. Recovery Scenario 6 (Case 2)	158
Procedure 8. Keep Restored User	163
Procedure 9. Remove the Restored User	165
Procedure 10. Restore an Archive That Does Not Contain a Current User	167
Procedure 11. IDIH Disaster Recovery Preparation	172
Procedure 12. IDIH Disaster Recovery (Re-Install Mediation and Application Servers)	174
Procedure 13. DSR Database Backup	177
Procedure 14. Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F) (HP DL380 Gen 9 Only)	181
Procedure 15. Inhibit A and B Level Replication on C-level Servers	183
Procedure 16. Un-Inhibit A and B Level Replication on C-level Servers	184
Procedure 17. Inhibit A and B Level Replication on C-level Servers	185
Procedure 18. Un-Inhibit A and B Level Replication on C-Level Servers	187
Procedure 19. Restore TVOE Configuration from Backup Media	189
Procedure 20. Restore PMAC from Backup Media	197
Procedure 21. Restore PMAC from Backup Server	200
Procedure 22. Restore Provisioning Database	206
Procedure 23. Recover PDB Relay	210
Procedure 24. Configure SNMP	211
Procedure 25. Backup Directory	214
Procedure 26. Turn off cipher list before backupConfiguation/restoreConfiguration/upgradeFirmware command	216
Procedure 27. Resume cipher list after backupConfiguation/restoreConfiguration/upgradeFirmware command	217

1. Introduction

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

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

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

1.1 References

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

1.2 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

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

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

1.3 Terminology

An alphabetized list of terms used in the document.

Table 2. Terminology

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

1.4 How to Use this Document

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

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

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

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

|--|

1.	Change directory	Change to the backout directory. \$ cd /var/TKLC/backout
2.	Verify Network Element data	 View the Network Elements configuration data; verify the data; save and print report. 1. Select Configuration > Network Elements to view Network Elements Configuration screen.

Figure 1. Example Procedure Steps Used in This Document

1.5 Optional Features

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

Table 3. Optional Features

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

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

2. General Description

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

Procedure	State of NOAM and/or SOAM server(s)
Recovery of the entire network from a total	All NOAM servers failed.
outage	All SOAM servers failed.
Outage)	MP servers may or may not have failed.
Recovery of one or more servers with at	• At least 1 NOAM server is intact and available.
Recovery Scepario 2 (Partial Server Outage	All SOAM servers failed.
with One NOAM Server Intact and ALL SOAMs Failed)	MP servers may or may not have failed.
Recovery of the NOAM pair with one or	All NOAM servers failed.
more SOAM servers intact	• At least 1 SOAM server out of active, standby,
with All NOAM Servers Failed and One	spare is intact and available.
SOAM Server Intact)	MP servers may or may not have failed.
Recovery of one or more server with at least	• At least 1 NOAM server is intact and available.
one NOAM and one SOAM server intact	• At least 1 SOAM server out of active, standby,
with One NOAM Server and One SOAM	spare is intact and available.
Server Intact)	1 or more MP servers have failed.
Recovery Scenario 5 (Both NOAM Servers	Both NOAM servers failed.
Failed with DR-NOAM Available)	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	Server is intact
Recovery)	Database gets corrupted on the server
databases that cannot be restored using replication from the active parent node.	Latest database backup of the corrupt server is present
	 Replication is inhibited (either manually or because of Comcol upgrade barrier)

Table 4. Recovery Scenarios

Procedure	State of NOAM and/or SOAM server(s)
Section Recovery Scenario 6: Case 1	Server is intact
	Database gets corrupted on the server
	Replication is occurring to the server with corrupted database
Section Recovery Scenario 6: Case 2	Server is intact
	Database gets corrupted on the server
	 Latest Database backup of the corrupt server is NOT present
	Replication is inhibited (either manually or because of Comcol upgrade barrier)

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

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

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

2.1 Complete Server Outage (All Servers)

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

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

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

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

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

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

2.4 Partial Server Outage with NOAM and One SOAM Server Intact

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

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

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

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

2.6 Partial Service Outage with Corrupt Database

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

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

3. Procedure Overview

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

3.1 Required Materials

The following items are needed for disaster recovery:

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

- 14. Site specific VM Placement and Socket Pinning workbook used during deployment (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 only).
- 15. Latest RADIUS shared secret encryption key file backup (DpiKf.bin.encr).
- 16. List of activated and enabled features.
- *Note:* For all disaster recovery scenarios, we assume the NOAM database backup and the SOAM database backup were performed around the same time, and that no synchronization issues exist among them.

3.2 Disaster Recovery Strategy

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

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



Figure 2. Determining Recovery Scenario

4. Disaster Recovery Procedure

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

WARNING

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

Recovering Base Hardware:

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

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



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

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

- Backup.dsr.DSRNO1.Configuration.NETWORK_OAMP.20180328_021502.AUTO.tar
- Backup.dsr.DSRSO1.Configuration.SYSTEM_OAM.20180328_021502.AUTO.tar
- X7201TVOE-plat-app-201803281022.iso
- backupPmac_20180328_050002.pef5.1.1

4.1 Recovery Scenario 1 (Complete Server Outage)

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

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

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

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

S	This procedure performs recovery if both NOAM servers are failed and all SOAM servers failed. This procedure also covers the C-level server failure.							
E P	Check off ($$) each st step number.	ep as it is completed. Boxes have been provided for this purpose under each						
#	If this procedure fails	ontact My Oracle Support (MOS) and ask for assistance.						
1.	Gather required materials	Gather the documents and required materials listed in the Required Materials section.						
2.	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. □	Replace failed equipment	Work with the hardware vendor to replace the failed equipment.						
4.	Recover PMAC and PMAC TVOE Host: Configure BIOS settings and update firmware	 Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]: 						
		HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings						
		 Oracle X5-2/Netra X5-2/X6-2/X7-2: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings 						
		HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings						
		 Verify and/or upgrade server firmware by executing the Upgrade Rack Mount Server Firmware procedure from reference [8]. 						
		Note: Determine VM placement and pinning by following:						
		 Section 3.1, item 14; and In reference [8], Appendix S VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1 Gbps NICs) and CPU Pinning in HP DL380 Gen 9 (Onboard 1 Gbps NICs) for Pinning Information on HP DL380 Gen 9. 						

Procedure 1. Recovery Scenario 1

5.	Recover PMAC, TVOE Hosts, and	This step assumes TVOE and PMAC backups are available. If backups are NOT available, skip this step .
	Switch: Backups available	 Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.
		2. Restore the PMAC backup by executing Appendix H Restore PMAC from Backup.
		3. Proceed to step 7.
6.	Recover PMAC, TVOE Hosts, and	This step assumes TVOE and PMAC backups are NOT available. If the TVOE and PMAC have already been restored, skip this step .
	Switch: Backups	Execute these procedures from reference [8]:
	NOT available	Install and Configure TVOE on First RMS (PMAC Host)
		Install PMAC
		Initialize the PMAC Application
7.	Recover failed	Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 GEN 9, skip this step.
	Cisco 4948	Recover failed Cisco 4948 aggregation switches, if needed:
	switches (HP	1. Back up available configuration files. Refer to Appendix C
	DL380 only)	Gen 9 Only) to recover failed Cisco 4948 Aggregation Switches (HP DL380
		 Back up configuration files NOT available. Execute the Configure Cisco 4948E-F Aggregation Switches (HP DL 380 Gen 8 Only) section from
		reference [8].
8.	Configure PMAC (no backup)	If PMAC backup was NOT restored in step 5. , execute this step; otherwise, skip this step.
		Execute these procedures from reference [8]:
		Configure PMAC Server (NetBackup Only)
		Add RMS to the PMAC Inventory
9.	Install/Configure additional rack	 Execute the Install TVOE on Additional Rack Mount Servers procedure from reference [8].
	mount servers	 If backups are available, restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.
		If backups are NOT available, execute the Configure TVOE on Additional Rack Mount Servers procedure from reference [8].
10.	Configure BIOS settings and update	 Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]:
	firmware on additional rack	HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings
	mount servers	 Oracle X5-2/Netra X5-2/X6-2/X7-2: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings
		HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings
		2. Verify and/or upgrade server firmware by executing the Upgrade Rack Mount Server Firmware procedure from reference [8].

11.	Determine VM placement and socket pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 only)	 HP DL380 GEN 8, skip this step. Determine VM placement and pinning by following: 1. Section 3.1, item 14; and 2. In reference [8], Appendix S VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1 Gbps NICs) and CPU Pinning in HP DL380 Gen 9 (Onboard 1 Gbps NICs) for Pinning Information on HP DL380 Gen 9. 			
12. □	Deploy redundant PMAC, if required	Refer to the Deploy Redundant PMAC (Optional) procedure to re-deploy and configure any redundant PMACs previously configured.			
13.	PMAC : Determine	1. Туре:			
	exists from the	[admusr@melbourne-pmac-1 ~]\$ ll /usr/TKLC/smac/etc/fdc/			
	initial deployment	 Examine the results and verify if the rms config file <hostname>.cfg exists.</hostname> 			
		<i>Note:</i> There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS.			
14. □	Create fdconfig backup file, if it does not already	 Execute this step ONLY If the fdconfig backup file does NOT exist. 1. Create the needed file(s) by executing the Virtual Machine/Network Fast Deployment section from reference [8]. 			
		WARNING			
		It is very important to ensure the file(s) created only affects the TVOE server(s) and the guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.			
		2. Skip to step 23. if this step was executed.			
15. □	PMAC : Load ISOs into PMAC, if not done already	If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the Virtual Machine/Network Fast Deployment section from reference [8].			
16. □	PMAC: Edit/Update	Edit the fdconfig file to include only the required/failed servers. <i>Notes</i> :			
	configuration file	Comment out configuration items that are not needed.			
		 Create a separate configuration file for EACH rack mount server being deployed. 			
		 The Cabinet ID in the config file needs to match the cabinet already defined in PMAC. 			
		The following items are mandatory: siteName 			
		• tpdlso			
		dsrlso (if DSR VMs are being configured)			
		sdslso (if SDS VMs are being configured)			
		NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured)			

		XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured)
		 XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured)
		DSRNOAM1XMIIPADDRESS (if DSRNOAM1 is being configured)
		DSRNOAM2XMIIPADDRESS (if DSRNOAM2 is being configured)
		• DSRDRNOAM1XMIIPADDRESS (if DSRDRNOAM1 is being configured)
		• DSRDRNOAM2XMIIPADDRESS (if DSRDRNOAM2 is being configured)
		SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured)
		SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured)
		• SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured)
		• SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured)
		Notes:
		 Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].
		 Comment out SDS and DSR profile items if corresponding products are not used.
		• For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6- 2/X7-2/HP DL380 Gen 9, refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].
		• VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName.
		• VM locations should not be changed from their RMSx format. Each RMS should correspond to a separate rack mount server.
		WARNING
		Ensure the file(s) created only affect the TVOE server(s) and guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.
17.	PMAC: Copy the	Copy the fdconfig backup file to the RMS directory.
	backed up fdc file to the RMS directory	<pre>\$ sudo cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file> /usr/TKLC/smac/etc/RMS/</backup_fdc_file></pre>
1		

18.	PMAC: Execute	Execute config.sh against the modified backup config file.				
	the config.sh script	Note: If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again.				
		<pre>\$ sudo ./config.sh <config file=""></config></pre>				
		Example output:				
		[admusr@5010441PMAC_RMS1\$_sudo/config.sh_rms.cfg				
		Validating cfg file				
		Successful validation of cfg file.				
		Added Cabinet 101 to Fast Deployment File. Added Zombie TVOF1 to Fast Deployment File				
		Added Zombie TVOE2 to Fast Deployment File.				
		Added xmi(bond0.4) to Fast Deployment File.				
		Added imi(bond0.3) to Fast Deployment File.				
		Added rep(bond1.10) to Fast Deployment File.				
		Added xsil(bond1.6) to fast Deployment file.				
		Added xsi3(bond1.8) to Fast Deployment File.				
		Added xsi4(bond1.9) to Fast Deployment File.				
		Added xsi5(bond1.11) to Fast Deployment File.				
		Added xsi6(bond1.12) to Fast Deployment File.				
		Added xsi7(bond1.13) to Fast Deployment File.				
		Added xsi9(bond1.15) to Fast Deployment File.				
		Added xsi10(bond1.16) to Fast Deployment File.				
		Added xsil1(bond1.17) to Fast Deployment File.				
		Added xsi12(bond1.18) to Fast Deployment File.				
		Added xsils(bond1.19) to Fast Deployment File.				
		Added xsi15(bond1.21) to Fast Deployment File.				
		Added xsi16(bond1.22) to Fast Deployment File.				
		Added Zombie DSRNOAM1 to Fast Deployment File.				
		Added Zombie DSRNOAM2 to Fast Deployment File.				
		Added Zombie_DSRDRNOAM1 to Fast Deployment File.				
		Added Zombie SDSNOAM1 to Fast Deployment File.				
		Added Zombie_SDSNOAM2 to Fast Deployment File.				
		Added Zombie_SDSDRNOAM1 to Fast Deployment File.				
		Added Zombie_SDSDRNOAM2 to Fast Deployment File.				
		Added Zombie_DSRSOAM1 to Fast Deployment File.				
		Added Zombie SDSSOAM1 to Fast Deployment File.				
		Added Zombie_SDSSOAM2 to Fast Deployment File.				
		Added Zombie_DSRDAMP1 to Fast Deployment File.				
		Added Zombie_DSRDAMP2 to Fast Deployment File.				
		Added Zombie DSRIPFE2 to Fast Deployment File.				
		Added Zombie_SDSDPSV1 to Fast Deployment File.				
		Added Zombie_SDSDPSV2 to Fast Deployment File.				
		Validating Fast Deployment File				
		validate configuration file: "Zomble_DSR_Fast_Deployment_06-15-16.xml"				
		Validation complete				
		Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml				
		SUCCESS: OPERATION SUCCESS!!				
		[admusr@5010441PMAC RMS]\$				

Procedure 1. Recovery Scenario 1

Procedure 1	. Recovery	Scenario 1
--------------------	------------	------------

19. □	PMAC : Execute fast deployment	Wit con	With the file generated from the config.sh script, execute the following command to start fast deployment:								
		\$	\$ screen								
		\$	<pre>\$ sudo fdconfig configfile=<fd_config.xml></fd_config.xml></pre>								
		No	te:	This is before screen	a long durat executing th session in t	tion command. he fdconfig, perfo he event of a te	If the scr orm a sc rminal tin	een cor r een -d neout, e	mmand r to res etc.	was ru ume th	n e
20.	PMAC GUI:	1.	lf ı	not alrea	dy done, est	ablish a GUI se	ssion on	the PM	AC serv	/er.	
	Monitor the	2.	Na	avioate to	Task Moni	itorina.					
	configuration	:			and Managa	5					
				D Tack M	anu Manage						
			- E		onitoning						
				Alenal 1	lotices						
			- E	S Logout	VUICES						
			- F	zj Logoui	<i></i>						
		3.	M	onitor the	e configuration	on to completion):				
		Mai	n Me	nu: Task Moni	toring						
		Filte	er* 🔻	Tack	Tarrat	Statue	State	Tack Output	Punning Timo	Start Timo	Drogroee
			925	Accept	RMS: <u>pc5010441</u> Guest:	Success	COMPLETE	N/A	0:01:04	2016-07-11	100%
			924	Accept	Zombie SDSDRNOAM1 RMS: pc5010441 Guest:	Success	COMPLETE	N/A	0.01.04	2016-07-11	100%
			923	Accept	Zombie SDSNOAM1 RMS: pc5010441	Success	COMPLETE	N/A	0:01:06	11:27:04 2016-07-11	100%
			922	Accept	Guest: Zombie_DSRIPFE1 RMS: pc5010439 Guest:	Success	COMPLETE	N/A	0:01:05	11:26:43 2016-07-11	100%
			024	Accent	Zombie_DSRDAMP2 RMS: pc5010441	Succes	COMPLETE	NIA	0:01:05	2016-07-11	100%
			321	Ассерг	Zombie_DSRDAMP1 RMS: pc5010439	3000000	COMPLETE	N/A	0.01.05	11:26:43	100%
			920	Accept	Guest: Zombie_DSRSOAM2	Success	COMPLETE	N/A	0:01:06	11:26:42	100%
		Nor [addifi1] Dumy Herr Dumy NUM 1 1 ava 2 1 3 1 4 2 4. \$ fi	te: muse=d p S e a p C PH 0 0 0 Re Suile	If a fail /var/Th rr@melbou leploy_me steps in are the s of DB ste S DLY IN pmac Fas pmac Fas pmac Fas estart the ado fdc e=deplo	ALC/log/fdc arne-pmac-1 albourne_201 file: "depl ateps that w - begin aps: AFRA ID SVRT 	vith fdconfig, log onfig/fdconfig. fdconfig]\$ sudd 70329T202458_7(oy_melbourne_2(ere generated 	s can be log file. of dconfi 01b.fdcdt 0170329T2 F PRE STA ete 300 (ped 300 (e_RMS3 1 occurred	access ig dump 202458_ ATE TO Check Check ATE TO ATE TO AT	ed in steps - 701b.fd BGTS CO PM&C i abinet d 900 0 s been .fdcdb	- cdb" MMAND S s Add Ri resolve	rext ns ed:

Procedure 1.	Recovery	Scenario 1
--------------	----------	------------

21.	PMAC : Repeat for each rack mount server configuration file	Repeat steps 1320. for each rack mount server/configuration file, if required.			
22.	PMAC: Back up	1.	Copy the updated fdc file to the fdc backup directory:		
	FDC file		<pre>\$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> /usr/TKLC/smac/etc/fdc/</fdc_file></pre>		
		2.	Change permissions:		
			<pre>\$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/<fdc_file></fdc_file></pre>		
23.	Perform CPU pinning	Co per 2/X	nfigure VM CPU socket pinning on each TVOE host to optimize formance by executing the CPU Pinning (Oracle X5-2/Netra X5-2/X6- (7-2/HP DL380 Gen9 Only) procedure from reference [8].		
24.	Obtain latest database backup	1.	Obtain the most recent database backup file from external backup sources (for example, file servers) or tape backup sources.		
	and network configuration data	2.	Obtain most recent RADIUS shared secret encryption key from the DpiKf.bin.encr file on external backup sources (only when the RADIUS key revocation MOP has been executed on the system).		
		3.	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.		
25.	Execute DSR installation	Vei No	rify the networking data for network elements. <i>tes</i>		
	procedure for the first NOAM	•	Use the backup copy of network configuration data and site surveys from step 2.		
		•	SDS disaster recovery actions can and should be worked simultaneously to allow faster recovery of the complete solution (that is, stale DB on DP servers do not receive updates until SDS-SOAM servers are recovered). The following steps accommodate both DSR and SDS disaster recovery steps.		
		Im	bortant : While creating the first NOAMs in this step, it is important that the server hostname is the same as one of the NOAM hostnames used prior to the disaster.		
		DS	R:		
		1.	Configure the first NOAM server by executing the Configure First NOAM NE and Server procedure from reference [8].		
		2.	Configure the NOAM server group by executing the Configure the NOAM Server Group procedure from reference [8].		
		SD	S:		
		1.	Configure the first SDS NOAM server by executing Configure First SDS NOAM NE and Server procedure from reference [8].		
		2.	Configure the SDS NOAM server group by executing the Configure the SDS NOAM Server Group procedure from reference [8].		
		3.	Skip to step 31.		

26.	NOAM GUI: Login	Log into the NOAM GUI as the guiadmin user.
	DSR only. If SDS,	
	skip to step 31.	
		Oracle System Login
		Mon Jul 11 13:59:37 2016 ED1
		Log In
		Enter your username and password to log in
		Lisemame.
		Password:
		Change password
		Log In
		Welcome to the Oracle System Login.
		This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript
		and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.
		Unauthorized access is prohibited.
		Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.
		Other names may be trademarks of their respective owners.
		Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.

Procedure 1. Recovery Scenario 1

27.		1. Navigate to Status & Manage > Files.
	Upload the backup database file. DSR only. If SDS, skip to step 31.	 Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Select the active NOAM server. Main Menu: Status & Manage -> Files
		ZombieNOAM1
		File Name
		TKLCConfigData.ZombieNOAM1.sh
		ugwrap.log
		upgrade.log
		 Click Upload and select the NO Provisioning and Configuration file backed up after initial installation and provisioning. Delete View Upload Download Deploy ISO Validate ISO 40 KB used (0.00%) of 15.7 GB available System utilization: 867.9 MB (5.39%) of 15.7 GB available. Click Browse and locate the backup file. Note: If there is no backup file, refer to Appendix L Backup Directory to appendix the backup file.
		create the backup directory.
		5. Click Open.
		6. Mark the I his is a backup file checkbox.
		7. Click Upload.
		File: Browse Backup.dsr.ZombieNOAM1.Configuration.NETWORK_OAM This is a backup file Upload Cancel
		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.

28.	NOAM GUI: Disable provisioning. DSR only. If SDS, skip to step 31.1.2.3.	 Navigate to Status & Manage > Database. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click Disable Provisioning.
		Disable Provisioning Report Inhibit/Allow
		3. Click OK to disable Provisioning. Disable provisioning. Are you sure?
		OK Cancel

Procedure 1. Recovery Scenario 1

Procedure 1. Recovery Scenario	1	
--------------------------------	---	--

29. NOAM GUI: Verify	1. Select the Active NOAM server and click Compare.
contents and	lication Backup Compare Restore
database compatibility. DSR only. If SDS, skip to step 31.	 Click the button for the restored database file uploaded as a part of step 27. of this procedure. Database Compare
	Select archive to compare on server: ZombieNOAM1
	Archive * 💿 backup/Backup.dsr.ZombieNOAM1.Configuratio
	Ok Cancel
	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
	The selected database came from ZombieNOAM1 on 10/10/2016 at 10:36:44 EDT and contains the follow
	Archive Contents Configuration data
	Database Compatibility The databases are compatible.
	Node Type Compatibility The node types are compatible.
	Topology Compatibility THE TOPOLOGY IS NOT COMPATIBLE. CONTACT ORACLE CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE.
	Discrepancies: - Server A1860.052 on network XMI is in the current topology but not the selected backup file. - Server A1860.052 on network IMI is in the current topology but not the selected backup file. - Server A0630.238 on network XMI is in the selected backup file but not the current topology. - Server B2934.011 on network XMI is in the selected backup file but not the current topology. - Server C0422.200 on network XMI is in the selected backup file but not the current topology.
	<i>Note:</i> Archive Contents and Database Compatibilities must be the following:
	Archive Contents: Configuration data.
	Database Compatibility: The databases are compatible.
	Note: The following is expected output for Topology Compatibility Check since we are restoring from an existing backed up database to a database with just one NOAM:
	Topology Compatibility THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.
	Note: We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility.
	4. If the verification is successful, click Back and continue to next step in this procedure.

30.	Active NOAM:	1. From Status & Manage > Database.			
	Restore the database.	2. Select the active NOAM server and click Restore.			
	DSR only. If SDS, skip to step 31.	are Restore Man A			
	3. Select the proper backup provisioning and configuration file.				
		Select archive to Restore on server: Zombia			
		Archive *			
		Ok Cancel			
		4. 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. 			
Database Restore Confirm Incompatible archive selected The selected database came from ZombieNOA		Database Restore Confirm			
		Incompatible archive selected			
		The selected database came from ZombieNOA			
		Archive Contents Configuration data			
		Database Compatibility			
		The databases are compatible.			
		Confirm archive "backup/Backup.dsr.ZombleNOAM1.Configurat			
Force Restore? Image: Force Force Ok Cancel Note: After the restore has started, the user is GUI since the restored topology is old do		Force Restore? Force Force restore			
		Ok Cancel			
		Note: After the restore has started, the user is logged out of the XMI NO GUI since the restored topology is old data.			
		6. Go to step 37.			

Procedure 1.	. Recovery	Scenario 1
--------------	------------	------------

	-			
31.	SDS NOAM: Transfer SDS configuration and provisioning backup database files. SDS only. If DSR, skip to step 37.	<pre>Using the IP of the recovered SDS NOAM, transfer the uncompressed backup database files to the /var/TKLC/db/filemgmt directory. Linux: 1. From the command line of a Linux machine, copy the configuration backup file to the SDS NOAM guest:</pre>		
32. □	SDS NOAM: Login. SDS only. If DSR, skip to step 37.	Establish an SSH session to the SDS active NOAM XMI IP address and login as admusr .		
33. □	SDS NOAM : Stop running applications. SDS only. If DSR, skip to step 37.	Issue the following command to stop running applications. Leave database running: \$ sudo prod.stopignore-cap Note: This step may take several minutes to complete.		
34.	SDS NOAM: Restore configuration database. SDS only. If DSR, skip to step 37.	Restore the configuration DB by executing the following command: \$ sudo idb.restore -n -t /var/TKLC/db/filemgmt -v <full archive="" configuration="" file="" name="" path="" to=""></full>		
35.	SDS NOAM: Restore provisioning database. SDS only. If DSR, skip to step 37.	Refer to Appendix I Restore Provisioning Database to restore the provisioning database.		
36. □	SDS NOAM : Start running applications. SDS only. If DSR, skip to step 37.	Start the SDS application by executing the following command: \$ sudo prod.start		

37.	NOAM VIP GUI:	1. E	stablish a GUI session on the NOAM server by using the VIP IP address			
	Login		The NOAM server. Open the web blowser and enter a OKE OI.			
			http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>			
		2. L	ogin as the guiadmin user:			
			ORACLE			
		Ora	ACIE System Login Mon Jul 11 13:59:37 2016 EDT			
			Log In Enter your username and password to log in			
			Username:			
			Password:			
			Change password			
			Log In			
			Welcome to the Oracle System Login.			
		Thi	s application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the <u>Oracle Software Web Browser Support Policy</u> for details.			
			Unauthorized access is prohibited.			
			Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.			
			Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.			
38.	NOAM VIP GUI:	1. V	Vait for 5-10 minutes for the system to stabilize with the new topology:			
	Monitor and confirm database	2. M a	Ionitor the Info tab for Success . This indicates the restore is complete nd the system is stabilized.			
		Ignor config	e these alarms for NOAM and MP servers until all the servers are gured:			
		• A (a	larms with Type Column as REPL , COLL, HA (with mate NOAM), DB about Provisioning Manually Disabled).			
		Note	s:			
		• D c	o not pay attention to alarms until all the servers in the system are ompletely restored.			
		• T w	he Configuration and Maintenance information is in the same state it as when backed up during initial backup.			

Procedure 1. Recovery Scenario 1

39	Active NOAM Set	1. Navigate to Status & Manage > HA.			
39.	Active NOAM: Set failed servers to OOS	 Navigate to Status & Manage Status & Manage Network Elements Server HA Database KPIs Processes Click Edit. Set the Max Allowed HA Role option to OOS for the failed servers. Modifying HA attributes 			
		Hostnamo	Max Allowed HA Polo	Description	
		nostilaille		Description	
		ZombieNOAM1	Active 💌	The maximum des	
		ZombieNOAM2	OOS Active	The maximum des	
		ZombieDRNOAM1	Standby Spare Observer	The maximum des	
		4. Click OK .	005		
		Ok Can	cel		
40 .	NOAM VIP GUI: Recover standby NOAMInstall the second DSR: Execute the C 6, from referend SDS: Execute the C and 3-6, from		nd NOAM server onfigure the Sec ce [8]. onfigure the Sec eference [8].	: ond NOAM Se ond SDS NOA	erver procedure, steps 1 and 3-
41.	Install NetBackup client (optional)	If NetBackup is used, execute the Install NetBackup Client (Optional) procedure from reference [8].			

Procedure 1. Recovery Scenario 1

42.	NOAM VIP GUI:	1. Navigate to Status & Manage > HA.		
	Set HA on standby NOAM	 Retrigate to outline of interlage > rink. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click Edit. Select the standby NOAM server and set it to Active. 		
		Hostname Max Allowed HA Pole Description		
		ZombieNOAM1 Active The maximum		
		ZombieNOAM2 Active The maximum		
		Standby ZombieDRNOAM1 Spare 4. Click OK.		
43.	NOAM VIP GUI: Restart DSR application	 1. Navigate to Status & Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Select the recovered standby NOAM server and click Restart. 		
44.	Active NOAM:	1. Establish an SSH session to the active NOAM and login as admusr .		
	Correct the recognized	2. Execute this command:		
	authority table	<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></dsr_noam_a_hostname></dsr_noam_b_hostname></pre>		

 45. NOAM VIP GUI: Perform Reverser. SDS only. If DSR, skip to step 47. 46. NOAM VIP GUI: Repeat for remote export Server. SDS only. If DSR, skip to step 47. 47. Navigate to SDS > Configuration > Options Connections Destination Map 48. NOAM VIP GUI: Repeat for remote export Server. SDS only. If DSR, skip to step 47. 49. Note: Navigate to SDS > Configuration > Options again to clear the banner. 41. Navigate to SDS > Configuration > Options again to clear the banner. 42. Enter the Remote Import Password. 43. Click Apply. Note: Navigate to SDS > Configuration > Options again to clear the banner. 5. Click Apply. Remote Import Enabled Note: Navigate to SDS > Configuration > Options again to clear the banner. 6. Mark the Remote Import Enabled checkbox. 10. Click Apply. 7. Click Apply. 8. Repeat step 45. for the remote export server. 	-	,	
46 NOAM VIP GUI: 47 NoAM VIP GUI: 6 NOAM VIP GUI: 6 NOAM VIP GUI: 7 Repeat step 45. for the remote export server.	45.	NOAM VIP GUI: Perform Keyexchange with remote import server. SDS only. If DSR, skip to step 47.	 1. Navigate to SDS > Configuration > Options. SDS Configuration Options Connections NAI Hosts Destinations Destination Map 2. Unmark the Remote Import Enabled checkbox.
 S. Click Apply. Note: Navigate to SDS > Configuration > Options again to clear the banner. Enter the Remote Import Password. Bende Import Float® Address 1026.53.25 Bende Import Bassword S. Click Apply. Remote Import Password S. Click Apply. Remote Import Enabled Note: Navigate to SDS > Configuration > Options again to clear the banner. Click Apply. Remote Import Enabled Note: Navigate to SDS > Configuration > Options again to clear the banner. Mark the Remote Import Enabled checkbox. Remote Import Enabled Remote Import Enabled Remote Import Enabled Remote Import Enabled Repeat for remote export server. 			Remote Import Enabled Whether or not import files are in DEFAULT = UNCHECKED
Action Note:: Navigate to SDS > Configuration > Options again to clear the banner. 4. Enter the Remote Import Password. Remote Import Ness Remote Import Ness S. Click Apply. Remote Import Enabled Note:: Navigate to SDS > Configuration > Options again to clear the banner. 6. Mark the Remote Import Enabled checkbox. Remote Import Enabled Remote Import Enabled Remote Import Enabled Remote Import Enabled Note:: Navigate to SDS > Configuration > Options again to clear the banner. 6. Mark the Remote Import Enabled checkbox. Remote Import Enabled Remote Import Enabled Start for remote export server. SDS only. If DSR, skip to step 47.			3. Click Apply.
4. Enter the Remote Import Password. Remote Import Near Remote Import Near Remote Import Near Remote Import Near Remote Import Enabled Note: Navigate to SDS > Configuration > Options again to clear the banner. 6. Mark the Remote Import Enabled Remote Import Enabled Remote Import Enabled Remote Import Enabled Start the Remote Import Enabled checkbox. Remote Import Enabled			<i>Note:</i> Navigate to SDS > Configuration > Options again to clear the banner.
46. NOAM VIP GUI: Remote Import Enabled 47. NOAM VIP GUI: Remote Import Enabled 6. NOAM VIP GUI: Remote Import Enabled 7. Remote Import Enabled Import Enabled			4. Enter the Remote Import Password .
46. NOAM VIP GUI: Remote import Enabled 46. NOAM VIP GUI: Remote import Enabled 5. So only. If DSR, skip to step 47. Remote emport Server.			
46. NOAM VIP GUI: Remote Import Enabled 47. NOAM VIP GUI: Repeat for remote 48. NOAM VIP GUI: Repeat step 45. for the remote export server.			Remote Import Host IP Address 10.250.53.25
46. NOAM VIP GUI: Repeat for remote export server. SDS only. If DSR, skip to step 47. Repeat step 45. for the remote export server.			Remote Import User systest
46. NOAM VIP GUI: Remote Import Enabled Import Enabled 46. NOAM VIP GUI: Repeat for remote export server. SDS only. If DSR, skip to step 47. Repeat step 45. for the remote export server.			Remote Import Password
46. NOAM VIP GUI: Remote Import Enabled SDS only. If DSR, skip to step 47. Remote Import Enabled Import Enabled <th></th> <th></th> <th>5. Click Apply.</th>			5. Click Apply.
46. NOAM VIP GUI: Repeat for remote export server. SDS only. If DSR, skip to step 47. Repeat step 45. for the remote export server.			Remote Import Enabled
 6. Mark the Remote Import Enabled checkbox. Remote Import Enabled 46. NOAM VIP GUI: Repeat for remote export server. SDS only. If DSR, skip to step 47. 			<i>Note:</i> Navigate to SDS > Configuration > Options again to clear the banner.
46. NOAM VIP GUI: Repeat for remote export server. SDS only. If DSR, skip to step 47. Repeat step 45. for the remote export server.			6. Mark the Remote Import Enabled checkbox.
46. NOAM VIP GUI: Repeat for remote export server. SDS only. If DSR, skip to step 47. Repeat step 45. for the remote export server.			
46. NOAM VIP GUI: Repeat for remote export server. SDS only. If DSR, skip to step 47. Repeat step 45. for the remote export server.			Demote Imped Eachied
46. NOAM VIP GUI: Repeat for remote export server. Repeat step 45. for the remote export server. SDS only. If DSR, skip to step 47. Repeat step 45. for the remote export server.			
46. NOAM VIP GUI: Repeat for remote export server. SDS only. If DSR, skip to step 47. Repeat step 45. for the remote export server.			
SDS only. If DSR, skip to step 47.	46. □	NOAM VIP GUI: Repeat for remote export server.	Repeat step 45. for the remote export server.
		SDS only. If DSR, skip to step 47.	

Procedure 1. Recovery Scenario 1

		1
47. □	NOAM VIP GUI: Perform Keyexchange with export server	1. Navigate to Administration > Remote Servers > Data Export.
		🖻 😋 Administration
		🚟 🛗 General Options
		🗈 🧰 Access Control
		🕞 🧰 Software Management
		🖃 😋 Remote Servers
		LDAP Authentication
		SNMP Trapping
		Data Export
		DNS Configuration
		2. Click SSH Key Exchange.
		SSH Kay Evolution
		3. Type the Password and click OK .
		SSH Key Exchange
		Password
		OK Cancel
40		Even to the Configuring SDC Over Service procedure store 4 and 4.7
48.	Recover querv	from reference [8].
	servers.	
	SDS only. If DSR,	
	skip to step 51.	

Procedure 1. Recovery Scenario 1

Procedure 1. Recovery Scenario 1

49.	SDS NOAM VIP	1. Navigate to Status & Manage > HA.
	GUI: Set HA on querv server.	🗐 🚔 Status & Manage
	SDS only. If DSR,	Network Elements
	skip to step 51.	Server
		🔯 HA
		ស Database
		🟹 KPIs
		- Normal Processes
		🖃 🧰 Tasks
		3. Select the query server and select Observer .
		ZombieQS1 Observer - The
		Observer
		OOS
		4. Click OK .
50.	SDS NOAM VIP	1. Navigate to Status & Manage > Server.
	GUI: Restart SDS	😑 😋 Status & Manage
	SDS only. If DSR,	Network Elements
	skip to step 51.	Server Server
		M HA
		Processes
		2 Select the recovered query server and click Restart
		op Restart Reboo
51.	NOAM VIP GUI:	Warning
	Stop replication to the C-level servers	warning
	of this site.	Before continuing this procedure, replication to C-level servers MUST be inhibited at the SOAM site being recovered.
	DSR only. If SDS,	Failure to inhibit replication to the working C-level servers results in the
	step.	database being destroyed!
	111	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,
	STOP	and Spare SOAMs are Lost) to inhibit replication to working C-level servers before continuing.
		If the spare SOAM is NOT deployed in the site, execute Appendix C Inhibit
		A and B Level Replication on C-level Servers to inhibit replication to working C-level servers before continuing.

52.	NOAM VIP GUI: Recover active SOAM server	Install the SOAM servers. DSR: Execute the Configure the SOAM Servers procedure, steps 1-3 and 5-9, from reference [8]. Note: If you are using NetBackup, also execute step 12. SDS: Execute the Configure the SDS DP SOAM Servers procedure, steps 1-3 and 5-8, from reference [8].
53.	NOAM VIP GUI: Set HA on the SOAM server	 Navigate to Status & Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click Edit. Select the SOAM server and set it to Active. Zombie SOAM1 Active The m Active Standby Spare Observer Observer Observer Click OK.
54.	NOAM VIP GUI: Restart DSR application	 1. Navigate to Status & Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Select the recovered NOAM server and click Restart.

55.	NOAM VIP GUI: Upload the backup SOAM database file.	1. Navigate to Status & Manage > Files.
		🖃 🚖 Status & Manage
		Network Elements
	DSR only. If SDS, skip to step 60. 2. 3. 4. 5. 6. Fi	Server
		M HA
		Tasks
		 Select the active SOAM server tab. Click Upload and select the file SO Provisioning and Configuration file backed up after initial installation and provisioning.
		un linked De
		w Upload Dov
		3. Click Browse and locate the backup file.
		4. Mark the This is a backup file checkbox.
		5. Click Open .
		6. Click Upload .
		8
		File: Browse No file selected. ☑ This is a backup file
		Upload
		Cancel
		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.

Procedure 1. Recovery Scenario 1

56.	Recovered SOAM GUI: Login. DSR only. If SDS, skip to step 60.	1. Establish a GUI session on the recovered SOAM server.
		2. Open the web browser and enter a URL of:
		http:// <recovered_soam_ip_address></recovered_soam_ip_address>
		3. Login as the guiadmin user:
		ORACLE
		Oracle System Login
		Log In
		Enter your username and password to log in
		Username:
		Password:
		Log In
		Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.
		Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
		Copyright © 2010, 2016, <u>Oracle</u> and/or its affiliates. All rights reserved.
Procedure 1. Recovery Scenario 1

57. Recovered SOAM	 Navigate to Status & Manage > Database.
archive contents	2. Select the Active SOAM server and click Compare.
and database compatibility.	Ip Compare Resto
DSR only. If SDS skip to step 60.	 3. Click the button for the restored database file uploaded as a part of step 27. of this procedure. Database Compare
	Select archive to compare on server: 2
	Archive *
	Ok Cancel
	4. Verify the output window matches the screen below.
	Database Archive Compare
	Ine selected database came from 20mbleSOAMI on 10
	Archive Contents Configuration data
	configuration data
	Database Compatibility The databases are compatible.
	Note: Archive Contents and Database Compatibilities must be the following:
	Archive Contents: Configuration data.
	Database Compatibility : The databases are compatible.
	Note: The following is expected output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM:
	Topology Compatibility THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.
	Note: We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility.
	5. If the verification is successful, click Back and continue to next step in this procedure.

Procedure 1. Recovery Scenario 1

	· · · · · · · · · · · · · · · · · · ·	
58.	Recovered SOAM GUI: Restore the	 Select the Active SOAM server and click Restore. Select the backup provisioning and configuration file
	database.	
	DSR only. If SDS, skip to step 60.	Database Compare
		Select archive to compare on serv
		Archive * (a) backup/Backup.dsr.Z
		Ok Cancel
		3. Click OK .
		Database Restore Confirm
		Compatible archive.
		The selected database came from Zombi
		Archive Contents Configuration data
		Database Compatibility
		The databases are compatible.
		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.
		Notes:
		After the restore has started, the user is logged out of XMI SOAM GUI since the restored topology is old data.
		 If the spare SOAM is in another network and is unreachable, the database restore cannot be done.
		Workaround : If the spare SOAM is unreachable and ping (from recovered SOAM server to spare SOAM server) hangs (as evidenced by ps -ef grep ping showing the same ping process and its child for more than 10 seconds), then kill the hung ping processes and the restore proceeds.
59.	Recovered SOAM	Wait for 5-10 minutes for the system to stabilize with the new topology:
	GUI: Monitor and confirm database restoral.	Monitor the Info tab for Success . This indicates the restore is complete and the system is stabilized.
		Notes:
	skip to step 60.	 Do not pay attention to alarms until all the servers in the system are completely restored.
		• The Configuration and Maintenance information is in the same state it was when backed up during initial backup.

60.	NOAM VIP GUI: Login	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:		
			http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>		
		2.	Login as the guiadmin user:		
			ORACLE		
		Or	acie System Login Tue Jun 7 13:49:06 2016 EDT		
			Log In Enter your username and password to log in Username: Password: Change password Change password Log In Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies. Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of Oracle Corporation and/or its affiliates.		
			Copyright © 2010, 2016, <u>Oracle</u> and/or its affiliates. All rights reserved.		
61.	NOAM VIP GUI: Recover the remaining SOAM servers (standby, spare)	DS Exe fror No SD Exe	R: ecute the Configure the SOAM Servers procedure, steps 1-3 and 5-9, in reference [8]. fe: If you are using NetBackup, also execute step 12. S: ecute the Configure the SDS DP SOAM Servers procedure, steps 1-3		

Procedure 1. Recovery Scenario 1



63.	NOAM VIP GUI: Start replication on	Un-Inhibit (start) re the same site as of	plication to the wor the failed SOAM se	king C-level Server ervers.	s which belongs to
	working C-level servers.	If the spare SOAN Un-Inhibit A and B Standby and Spare	l is also present in Level Replication of SOAMs are Lost)	n the site and lost , n C-Level Servers (execute Appendix F When Active,
	skip to next step.	If the spare SOAN Inhibit A and B Lev	I is NOT deployed rel Replication on C-	in the site, execute level Servers.	e Appendix D Un-
		1. Navigate to Sta	atus & Manage > D	atabase.	
		📄 😋 Status & M	lanage		
		📄 💽 Netwo	rk Elements		
		Server			
		Datab	ase		
		KPIs			
		🔤 🕅 Proces	sses		
		2. If the Repl Sta order; otherwis continue with tl	tus is set to Inhibito e, if none of the ser he next step:	ed, click Allow Rep vers are inhibited, s	lication using this skip this step and
		Active NO	AM Server		
		Standby N	OAM Server		
		Active SOA	AM Server		
		Standby Se	OAM Server		
		 Spare SOA 2/X7-2/HP 	AM Server (if applic DL380 Gen 9 Only	able) — Oracle X5	-2/Netra X5-2/X6-
		Active DR	NOAM Server		
		Standby D	R NOAM Server		
		MP/IPFE S the active I	Servers (if MPs are o MP; otherwise, the o	configured as active order of the MPs do	/standby, start with es not matter)
		 SBRS (if S standby, th DL 380 Get 	BR servers are con hen spare) — Oracle h 9 Only	figured, start with th e X5-2/Netra X5-2/X	e active SBR, then (6-2/ X7-2/HP
		3 Verify the repli	cation on all the wor	rking servers is allo	wed This can be
		done by exami	ning the Repl Statu	s 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
1					

Procedure 1. Recovery Scenario 1

64.	NOAM VIP GUI: Restart DSR application	 1. Navigate to Status & Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Select the recovered standby NOAM server and click Restart.
		bp Restait Rebo
65.	NOAM VIP GUI: Perform Keyexchange with export server	 Navigate to Administration > Remote Servers > Data Export. Administration General Options Access Control Software Management Remote Servers LDAP Authentication SNMP Trapping Data Export DNS Configuration Click the Task Name and click Key Exchange. Insert Edit Delete Key Exchange Transfer Now Test Transfer Key Report Task Name Remote Server Username Directory on Export Server Fil
		APDE Remote Server Copy 10.10.10.10 admusr ex
		3. Type the Password and click OK. Exchange SSH Keys with Remote Server Enter the password for the user on the remote server: OK

Procedure 1	. Recovery	Scenario 1
--------------------	------------	------------

r	t	ή		
66. □	Activate PCA feature. DSR only	If you have PCA installed in the system being recovered, re-activate PCA by executing the PCA Activation on Entire Network procedure on the recovered NOAM server from [7].		
		<i>Note:</i> If not al activation	II SOAM sites are rea on for each "new" So	covered at this point, then repeat the DAM site that comes online.
67.	67. NOAM VIP GUI: Recover the C-level server (DA-MPs,	DSR: Execute the Co reference [8].	nfigure the MP Ser	vers procedure, steps 1 and 9-13, from
	MP, and SDS DPs	Note: Also ex your Mi networl	ecute steps 14-16 if P that uses a signali <.	you plan to configure a default route on ng (XSI) network instead of the XMI
		SDS (Oracle X8	5-2/Netra X5-2/X6-2/	/ X7-2/HP DL380 Gen 9 Only):
		Execute the Co from reference	nfigure the SDS DF [8].	P Servers procedure, steps 1 and 5-8,
		Repeat this step	p for any remaining f	failed MP servers.
68.	NOAM VIP GUI: Set HA on all C- level servers 2 3	 Navigate to Status and the second secon	Status & Manage - & Manage work Elements ver abase s cesses ecovered C-Level wit	-> HA. h a Max Allowed HA Role set to OOS , set The maximum desired HA Role for ZombieDAMI
		ZombieDAMP2	Standby Spare Observer OOS	The maximum desired HA Role for ZombieDAMI
		4. Click OK .		

Procedure 1.	Recovery	Scenario 1	
--------------	----------	------------	--

69.	NOAM VIP GUI: Restart DSR application on the recovered C-level	1. Navigate to Status & Manage > Server.
		😑 😋 Status & Manage
		🔤 🔯 Network Elements
	servers	Server
		- 🕅 HA
		🔤 🔯 Database
	2	🛐 KPIs
		🛐 Processes
		2. Select the recovered C-level servers and click Restart .
		p Restart Rebo

Procedure '	1. Recovery	Scenario 1
-------------	-------------	------------

70 .	NOAM VIP GUI: Start replication on	Un-Inhibit (start) replication to the ALL C-level servers.			
	all C-Level servers.				
	DSR only. If SDS,		wanage ork Elements		
	step.	Serve	r		
		Datab	ase		
		🔤 🕅 KPIs			
		Proce	sses		
		2. If the Repl Sta order:	itus is set to Inhibit	ed, click Allow Re	plication using this
		Active NO	AMP Server		
		Standby N	IOAMP Server		
		Active SO	AM Server		
		Standby S	OAM Server		
		Spare SO, X7-2/HP E	AM Server (if appli d 0L380 Gen 9 Only)	cable) — Oracle X	5-2/Netra X5-2/X6-2/
		Active DR	NOAM Server		
		Standby D	R NOAM Server		
		MP/IPFE \$	Servers		
		 SBRS (if S standby, the DL380 Get 	SBR servers are con nen spare) — Oracl n 9 Only	figured, start with t e X5-2/Netra X5-2/	the active SBR, then X6-2/ X7-2/HP
		3. Verify the replicing the replication of the section of the sect	ication on all servers Repl Status.	s is allowed. This c	can be done by
		OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
		NotApplicable	NotApplicable	Allowed	NotApplicable
		Normal	NotApplicable	Allowed	NotApplicable
		Normal	NotApplicable	Allowed	NotApplicable
		Normal	NotApplicable	Allowed	NotApplicable
71.	Active NOAM:	1. Establish an S	SH session to the a	ctive NOAM and Ic	ogin as admusr .
	Perform	2. Perform a key	exchange from the a	active NOAM to ea	ch recovered server:
	between the active-	\$ keyexchange	e admusr@ <recov< td=""><td>ered Server Ho</td><td>stname></td></recov<>	ered Server Ho	stname>
	NOAM and recovered servers	Note: If an expo	rt server is configure	ed perform this ste	D
1					۲.

72.	Active NOAM: Activate optional features. DSR only. If SDS, then skip to next step.	Establish an SSH session to the active NOAM and login as admusr .	
		Note for PCA Feature Activation:	
		If you have PCA installed in the system being recovered, re-activate the PCA by executing the PCA Activation on Entire Server procedure on the recovered NOAM server from [6]. <i>Notes</i> :	
		 If not all SOAM sites are recovered at this point, then repeat the activation for each "new" SOAM site that comes online. 	
		If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature.	
		Refer to section 1.5 Optional Features to activate any features that were previously activated.	
73.	NOAM VIP GUI:	1. Navigate to Status & Manage > Database.	
	Fetch and store the	🚊 😋 Status & Manage	
	the newly restored	Network Elements	
	data and save it	Server	
		HA III	
		Database	
		KPIs KPIs	
		Processes	
		2. Select the active NOAM server and click Report .	
		oning Report Inhit	
		The following screen displays:	
		Main Menu: Status & Manage -> Database [Report]	
		dsr Database Status Report	
		Report Generated: Tue Oct 11 13:24:26 2016 EDT From: Active Network OAM&P on host ZombieNOAM1 Report Version: 8.0.0.0.0-80.9.0 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.	

74.	Active NOAM:	1. Log into the active NOAM as admusr using SSH terminal.
	between servers	2. Execute this command:
		\$ sudo irepstat -m
		Example output:
		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-I Active 0 0.25 1%R 0.04%cpu 61B/s
		AB TO Oanu-SOAM-2 ACTIVE 0 0.50 1%R 0.05%cpu /5B/S
		$PR = rom Oabu = SOAM = 2 Active 0 0.50 ^0.032 cou 27R/s$
		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

75.	NOAM VIP GUI:	1. Navigate to Status	& Manager > Database) .	
	Verify the database states	 Status & Manag Network Ele Server Server HA Database KPIs Processes 	je ments		
		 Verify the OAM Max SOAM; Application Normal. 	x HA Role is either Activ Max HA Role for MPs is	ve or Standby for a Active ; and statu	NOAM and s is
		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	ZombielPFE1	MP	Active
		ZombieSOAM	ZombielPFE2	MP	Active

Procedure 1. Recovery Scenario 1

Procedure 1. Recovery Scenario 1

r	1	
76.	NOAM VIP GUI: Upload the backed up RADIUS key file (RADIUS only). DSR only. If SDS, skip to the next step.	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. Navigate to Status & Manage > Files. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Select the active NOAM server tab. Click Uplead and select the PADUUS
		shared secret encryption key file backed up after initial installation and
		provisioning or after key revocation execution.
		v Upload Down
		3. Click Browse.
		4. Locate the DpiKf.bin.encr file.
		5. Click Upload.
		⊗
		File:
		This is a backup file
		Upload
		Cancel
	The file	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.
		<i>Note:</i> This file should be deleted from the operator's local servers as soon as key file is uploaded to the active NOAM server.

Procedure 1. Recovery Scenario 1	Procedure	. Recovery	Scenario 1
----------------------------------	-----------	------------	------------

 77. NOAM VIP: Copy and distribute RADIUS key file on active NOAM (RADIUS only) — Part 1 	 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. Log into the active NOAM VIP as admusr user using SSH terminal. 2. Copy the key file: \$ cd /usr/TKLC/dpi/bin
	Ş ./Sharedkrevo -decr
	<pre>\$ sudo rm /var/TKLC/db/filemgmt/<backed file="" key="" name="" up=""></backed></pre>
	3. Make sure all servers in the topology are accessible.
	\$./sharedKrevo -checkAccess
	<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] '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. Note: If all the servers are not accessible, then contact My Oracle Support (MOS)</pre>

Procedure 1. Recovery Scenario 1

78.	NOAM VIP: Copy	Distribute key file to all the servers	in the topolog	y:	
	and distribute the RADIUS key file on active NOAM (RADIUS only) — Part 2	\$./sharedKrevo -synchronize			
		\$./sharedKrevo -updateData			
		Example output:			
		1450723210: [INFO] Key file o 1450723210: [INFO] NO NEED to FIPS integrity verification t FIPS integrity verification t 1450723210: [INFO] Key file o 1450723210: [INFO] NO NEED to FIPS integrity verification t 1450723211: [INFO] NO NEED to 1450723211: [INFO] Key file o 1450723211: [INFO] NO NEED to [admusr@NOAM-2 bin]\$./shared 1450723226: [INFO] Updating d 1450723227: [INFO] Data updat FIPS integrity verification t FIPS integrity verification t 145072328: [INFO] Updating d FIPS integrity verification t 145072320: [INFO] 1 rows updat 1450723230: [INFO] 1 rows updat [admusr@NOAM-2 bin]\$ Note: For any errors refer My Ora	n Active NOA sync key fi est failed. est failed. n Active NOA sync key fi est failed. est failed. n Active NOA sync key fi Krevo -updat ata on serve ed to 'NOAM- est failed. est failed. est failed. est failed. ated on 'SOA ed to 'SOAM- acce Support (M and IPFE a le to IPFE. M and MP-2 a le to MP-2. M and MP-1 a le to MP-1. eData r 'NOAM-2' 2' r 'SOAM-2' m-2' 2' MOS).	are same. are same.
79.	NOAM VIP GUI: Verify the HA status	 Navigate to Status and Manage Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the row for all of the server 	je > HA . vers.		
		3. Verify the HA Role is either Active or Standby .			
		Hostname	OAM HA Role	Application HA Role	Max Allowed HA Role
		ZombieNOAM1	Active	N/A	Active
		ZombieNOAM2	Standby	N/A	Active
		ZombieDRNOAM1	Active	N/A	Active
		ZombieDRNOAM2	Standby	N/A	Active
		ZombieSOAM1	Active	N/A	Active
		ZombieSOAM2	Standby	N/A	Standby

Procedure 1. Recovery Scenario 1

80.	NOAM GUI:	1. Navigate to Status & Manage > Database.
	Enable provisioning	 Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Click Enable Provisioning. 8. Click CK.
81		1 Navigate to Status & Manage > Database
	Enable site provisioning. DSR only. If SDS, then skip to step 91.	 Navigate to Status & Manage Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Click Enable Site Provisioning. Report Inhibit/Alk 3. Click OK.
82		1 Navigate to Diameter > Configuration > Local Node
	Verify the local node information. DSR only. If SDS, then skip to step 91.	 Diameter Configuration Capacity Summary Connection Capacity Dashb Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes 2. Verify all the local nodes are shown.

83.	SOAM VIP GUI: Verify the peer node information. DSR only. If SDS, then skip to step 91.	 Navigate to Diameter > Configuration > Peer Node. Diameter Configuration Capacity Summary Connection Capacity E Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes Verify all the peer nodes are shown.
84.	SOAM VIP GUI: Verify the connections information. DSR only. If SDS, then skip to step 91.	 1. Navigate to Diameter > Configuration > Connections. Diameter Configuration Capacity Summary Connection Capacity Dash Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Node Groups Connections 2. Verify all the connections are shown.
85.	MP Servers: Disable SCTP Auth Flag. DSR only. If SDS, then skip to step 91.	For SCTP connections without DTLS enabled, refer to the Enable/Disable DTLS (SCTP Diameter Connections Only) section in reference [8]. Execute this procedure on all failed MP servers.

Procedure 1. Recovery Scenario 1

 86. SOAM VIP GUI: Enable connections, if needed. DSR only. If SDS, then skip to step 91. 1. Navigate to Diameter > Maintenance > Connection Route Lists Peer Nodes Connections 	ns. ^r ely, enable all the
□ Connections, if needed. □ DSR only. If SDS, then skip to step 91.	ely, enable all the
needed.Route ListsDSR only. If SDS, then skip to step 91.Route GroupsPeer NodesConnections	rely, enable all the
DSR only. If SDS, then skip to step 91.	ely, enable all the
then skip to step Image: Peer Nodes 91. Image: Connections	ely, enable all the
91. Connections	ely, enable all the
	ely, enable all the
2 Select each connection and click Enable Alternativ	ely, enable all the
connections by clicking EnableAll .	
ble EnableAll Disable	
	-
Note: If a disaster recovery was performed on an IPFI necessary to disable and re-enable the connect link distribution	: server, it may be ions to ensure proper
87. SOAM VIP GUI: 1. Navigate to Diameter > Maintenance > Applicatio	ns.
Enable optional	
Route Lists	
then skip to step	
91.	
Connections	
Egress Throttle Groups	
Applications	
2. Select the optional feature application configured in	step 72.
3. Click Enable.	
Enable Disable Pause updates	
88. SOAM VIP GUI: 1. Navigate to Transport Manager > Maintenance >	Fransport.
transports if	
needed.	
DSR only. If SDS, 📄 🔄 Maintenance	
then skip to step	
91. 2. Select each transport and click Enable .	
Enable Disable Block	
Lindble Disable Diock	
3. Verify the Operational Status for each transport is U	p .

89.	SOAM VIP GUI: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 91.	 Navigate to SS7/Sigtran > Maintenance > Local SCCP Users. SS7/Sigtran Configuration Maintenance Local SCCP Users Remote Signaling Points Remote MTP3 Users Linksets Links
		 Click the Enable button corresponding to MAPIWF Application Name.
		Enable Disable
		3. Verify the SSN Status is Enabled .
90.	SOAM VIP GUI: Re-enable links, if needed. DSR only. If SDS, then skip to step 91.	 Navigate to SS7/Sigtran > Maintenance > Links. SS7/Sigtran Configuration Maintenance Local SCCP Users Remote Signaling Points Remote MTP3 Users Linksets Linksets Click Enable for each link. 3. Verify the Operational Status for each link is Up.
91.	SOAM VIP GUI: Examine all alarms	 Navigate to Alarms & Events > View Active. Alarms & Events View Active View History View Trap Log Examine all active alarms and refer to the on-line help on how to address them. If needed, contact My Oracle Support (MOS).

92.	NOAM VIP GUI: Examine all alarms	 Navigate to Alarms & Events > View Active. Alarms & Events View Active View History View Trap Log Examine all active alarms and refer to the on-line help on how to address them.
		If needed, contact My Oracle Support (MOS).
93. □	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.
94. □	Back up and archive all the databases from the recovered system	Execute the DSR Database Backup procedure to back up the configuration databases.
95.	Recover IDIH, if configured	If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.
96.	SNMP workaround	 Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases: 1. If SNMP is not configured in DSR/SDS. 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 will recover the database on these servers. The major activities are summarized in the list below. Use this list to understand the recovery procedure summary. Do not use this list to execute the procedure; detailed steps are in Procedure 2. The major activities are summarized as follows:

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

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

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

• Recover IDIH if necessary

STEP#	 This procedure performs recovery if at least one NOAM server is available, but all SOAM servers a site have failed. This includes any SOAM server that is in another location. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance. 					
1.	Workarounds	 Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist. Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases: 1. If SNMP is not configured in DSR. 2. If SNMP is already configured and SNMPv3 is selected as enabled version. 				
2.	Gather required materials	Gather the documents and required materials listed in Required Materials.				

3.	NOAM VIP GUI: Login	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:				
		http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>				
		2. Login as the guiadmin user:				
		Oracle System Login				
		Log In Enter your username and password to log in Username: Password: Change password Log In				
		Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.				
		Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.				
		Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.				

Procedure 2. Recovery Scenario 2

4.	Active NOAM:	1. Navigate to Status & Manage > HA.			
	Set failed servers to OOS	 Status & Manage Network Elements Server HA Database KPIs Processes Click Edit. 			
		Hostname Max Allowed HA Role Description			
		ZombieNOAM1 Active The maximum des			
		ZombieNOAM2 OOS The maximum des Active			
		ZombieDRNOAM1 Spare The maximum des Observer			
		 Set the Max Allowed HA Role option to OOS for the failed servers. 			
		4. Click OK .			
		Ok Cancel			
5. □	Replace failed equipment	Work with the hardware vendor to replace the failed equipment.			
6.	Recover PMAC TVOE Host: (if required) Configure BIOS settings and update firmware	 Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]: HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings Oracle X5-2/Netra X5-2/X6-2/X7-2: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings Verify and/or upgrade server firmware by executing the Upgrade Rack Mount Server Firmware procedure from reference [8]. 			

Procedure 2. Recovery Scenario 2

_		
/ [A Recover PMAC and PMAC TVOE	If PMAC is located on the failed rack mount server(s), execute this step; otherwise, skip to step 11.
	☐ Host: Backups available	This step assumes TVOE and PMAC backups are available. If backups are NOT available, skip this step.
		 Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.
		 Restore the PMAC backup by executing Appendix H Restore PMAC from Backup.
		3. Proceed to step 11.
8	Recover PMAC and PMAC TVOE	This step assumes TVOE and PMAC backups are NOT available, if the TVOE and PMAC have already been restored, skip this step .
	Host: Backups	1. Execute these procedures from reference [8]:
		Install and Configure TVOE on First RMS (PMAC Host)
		Install PMAC
		Initialize the PMAC Application
		2. Proceed to next step.
9	. Configure PMAC:	If PMAC backup was NOT restored in step 7. , execute this step; otherwise, skip this step.
		Execute these procedures from reference [8]:
		Configure PMAC Server (NetBackup Only)
		 Configure PMAC Server (NetBackup Only) Add RMS to the PMAC Inventory
1	0. Install/Configure → additional rack	 Configure PMAC Server (NetBackup Only) Add RMS to the PMAC Inventory This step assumes TVOE backups are available on any additional rack mount servers; otherwise, skip this step.
1	0. Install/Configure additional rack mount servers	 Configure PMAC Server (NetBackup Only) Add RMS to the PMAC Inventory This step assumes TVOE backups are available on any additional rack mount servers; otherwise, skip this step. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on additional rack mount servers.
1	 0. Install/Configure additional rack mount servers 1. Install/Configure additional rack 	 Configure PMAC Server (NetBackup Only) Add RMS to the PMAC Inventory This step assumes TVOE backups are available on any additional rack mount servers; otherwise, skip this step. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on additional rack mount servers. If TVOE backups were NOT performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step.
1 [1 [Install/Configure additional rack mount servers Install/Configure additional rack mount servers 	 Configure PMAC Server (NetBackup Only) Add RMS to the PMAC Inventory This step assumes TVOE backups are available on any additional rack mount servers; otherwise, skip this step. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on additional rack mount servers. If TVOE backups were NOT performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step. Execute these procedures from reference [8]:
1 [1 [0. Install/Configure additional rack mount servers 1. Install/Configure additional rack mount servers	 Configure PMAC Server (NetBackup Only) Add RMS to the PMAC Inventory This step assumes TVOE backups are available on any additional rack mount servers; otherwise, skip this step. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on additional rack mount servers. If TVOE backups were NOT performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step. Execute these procedures from reference [8]: Install TVOE on Additional Rack Mount Servers
1 [1 [0. Install/Configure additional rack mount servers 1. Install/Configure additional rack mount servers	 Configure PMAC Server (NetBackup Only) Add RMS to the PMAC Inventory This step assumes TVOE backups are available on any additional rack mount servers; otherwise, skip this step. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on additional rack mount servers. If TVOE backups were NOT performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step. Execute these procedures from reference [8]: Install TVOE on Additional Rack Mount Servers Configure TVOE on Additional Rack Mount Servers
1 [1	0. Install/Configure additional rack mount servers 1. Install/Configure additional rack mount servers	 Configure PMAC Server (NetBackup Only) Add RMS to the PMAC Inventory This step assumes TVOE backups are available on any additional rack mount servers; otherwise, skip this step. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on additional rack mount servers. If TVOE backups were NOT performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step. Execute these procedures from reference [8]: Install TVOE on Additional Rack Mount Servers Configure TVOE on Additional Rack Mount Servers Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]:
1	0. Install/Configure additional rack mount servers 1. Install/Configure additional rack mount servers	 Configure PMAC Server (NetBackup Only) Add RMS to the PMAC Inventory This step assumes TVOE backups are available on any additional rack mount servers; otherwise, skip this step. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on additional rack mount servers. If TVOE backups were NOT performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step. Execute these procedures from reference [8]: Install TVOE on Additional Rack Mount Servers Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]: HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings
1	 0. Install/Configure additional rack mount servers 1. Install/Configure additional rack mount servers 	 Configure PMAC Server (NetBackup Only) Add RMS to the PMAC Inventory This step assumes TVOE backups are available on any additional rack mount servers; otherwise, skip this step. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on additional rack mount servers. If TVOE backups were NOT performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step. Execute these procedures from reference [8]: Install TVOE on Additional Rack Mount Servers Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]: HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings Oracle X5-2/Netra X5-2/X6-2/X7-2: Configure Oracle X5-2/Netra X5-2/X6-2/X7-2 Server BIOS Settings
1	 Install/Configure additional rack mount servers Install/Configure additional rack mount servers 	 Configure PMAC Server (NetBackup Only) Add RMS to the PMAC Inventory This step assumes TVOE backups are available on any additional rack mount servers; otherwise, skip this step. Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on additional rack mount servers. If TVOE backups were NOT performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step. Execute these procedures from reference [8]: Install TVOE on Additional Rack Mount Servers Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]: HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings Oracle X5-2/Netra X5-2/X6-2/X7-2: Configure Oracle X5-2/Netra X5- 2/X6-2/X7-2 Server BIOS Settings HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings

Determine VM placement and socket pinning (Oracle X5- 2/Netra X5-2/X6-2/ X7-2/HP DL380 Gen 9 Only)	HP DL380 GEN 8, skip this step . Determine VM placement and pinning by following section 3.1, item 14.			
Deploy redundant PMAC	If the redundant PMAC is located on the failed rack mount server(s), execute this step; otherwise, skip to the next step. Refer to the Deploy Redundant PMAC (Optional) procedure to re-deploy and configure any redundant PMACs previously configured.			
PMAC:	1. Туре:			
fdconfig file exists	[admusr@melbourne-pmac-1 ~]\$ ll /usr/TKLC/smac/etc/fdc/			
from the initial deployment	 Examine the results and verify if the rms config file <hostname>.cfg exists.</hostname> 			
	Note: There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS.			
	3. If the file exists, skip to step 16.			
Create fdconfig backup file, if it does not already	 Execute this step ONLY If the fdconfig backup file does NOT exist. 1. Create the needed file(s) by executing the Virtual Machine/Network Fast Deployment section from reference [8]. 			
EXIST	WARNING			
	It is very important to ensure the file(s) created only affects the TVOE server(s) and the guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.2. Skip to step 24.			
PMAC : Load ISOs into PMAC, if not done already	If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the Virtual Machine/Network Fast Deployment section from reference [8].			
PMAC: Edit/Update configuration file	 Edit the fdconfig file to include only the required/failed servers. Notes: Comment out configuration items that are not needed. Create a separate configuration file for EACH rack mount server being deployed. The Cabinet ID in the config file needs to match the cabinet already defined in PMAC. The following items are mandatory: siteName 			
	PMAC: Load ISOs into PMAC, if not done already PMAC: Demonstration file			

Procedure 2. Recovery Scenario 2

		•	sdsIso (if SDS VMs are being configured)					
		•	NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured)					
		•	XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured)					
		•	XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured)					
		•	DSRNOAM1XMIIPADDRESS (if DSRNOAM1 is being configured)					
		•	DSRNOAM2XMIIPADDRESS (if DSRNOAM2 is being configured)					
		•	DSRDRNOAM1XMIIPADDRESS (if DSRDRNOAM1 is being configured)					
			DSRDRNOAM2XMIIPADDRESS (if DSRDRNOAM2 is being configured)					
		•	SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured)					
		•	SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured)					
		•	SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured)					
			SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured)					
			Notes:					
		•	Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].					
		•	Comment out SDS and DSR profile items if corresponding products are not used.					
		•	For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6- 2/X7-2/HP DL380 Gen 9, refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].					
		•	VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName.					
		• VM locations should not be changed from their RMSx format. Each should correspond to a separate rack mount server.						
		WARNING						
Ensure the f recovered. I result in those			sure the file(s) created only affect the TVOE server(s) and guests being covered. Failure to ensure working servers are not included in the file could sult in those servers/guests being taken out of service.					
18.	PMAC: Copy the	Со	py the fdconfig backup file to the RMS directory.					
	backed up fdc file to the RMS directory	\$ /	<pre>\$ sudo cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file> /usr/TKLC/smac/etc/RMS/</backup_fdc_file></pre>					

□ the config.sh script Note: If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again. \$ suido ./config.sh <config file=""> Example output: [admmsf\$5010f4:FIRGC IN[] suido ./config.sh rms.cfg [which charter of rite</config>	19.	PMAC : Execute the config.sh script	Execute config.sh against the modified backup config file.
<pre>\$ sudo ./config.sh <config file=""> Example output: [admusr@s010411FMAC FMS]\$ uudo ./config.sh rms.cfg Vildating off file Added Cabite TOUE to Fast Deployment File. Added stafi (bond1.9) to Fast Deployment File. Added stafi (bond1.6) to Fast Deployment File. Added stafi (bond1.1) to Fast Deployment File. Added stafi (bond1.2) to Fast Deployment File. Added sta</config></pre>			Note: If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again.
<pre>Example output: [sdmsr@\$010441FMAC FMS]\$ mudo ./config.sh rms.cfg Vildating off file Added Cabine 101 to Fast Deployment File. Added Combie_TVOE1 to Fast Deployment File. Added combie_TVOE1 to Fast Deployment File. Added combie_TVOE1 to Fast Deployment File. Added simi(bond0.3) to Fast Deployment File. Added simi(bond1.6) to Fast Deployment File. Added simi(bond1.1) to Fast Deployment File. Added simi(bond1.2) to Fast Deployment File. Added zombie_DSRNOMM to Fast Deployment File. Added zombie</pre>			<pre>\$ sudo ./config.sh <config file=""></config></pre>
<pre>[admusr@S010441PMAC RMS]\$ sudo ./config.sh rms.cfg Validating cfg file Successful validation of cfg file. Added Cabinet 101 to Fast Deployment File. Added Zombie_TVOE1 to Fast Deployment File. Added zombie_TVOE2 to Fast Deployment File. Added imi (bond0.3) to Fast Deployment File. Added imi (bond0.3) to Fast Deployment File. Added imi (bond0.3) to Fast Deployment File. Added xsii (bond1.7) to Fast Deployment File. Added xsii (bond1.6) to Fast Deployment File. Added xsii (bond1.7) to Fast Deployment File. Added xsii (bond1.8) to Fast Deployment File. Added xsii (bond1.3) to Fast Deployment File. Added xsii (bond1.13) to Fast Deployment File. Added xsii (bond1.15) to Fast Deployment File. Added xsii (bond1.16) to Fast Deployment File. Added xsii (bond1.17) to Fast Deployment File. Added xsii (bond1.19) to Fast Deployment File. Added xsii (bond1.10) to Fast Deployment File. Added xsii (bond1.2) to Fast Deployment File. Added zombie_DSBNOAMI to Fast Deployment File. Added Zombie_SBNOAMI to Fast Deployment Fil</pre>			Example output:
<pre>Validating ofg file Successful validation of cfg file. Added Cabinet 101 to Fast Deployment File. Added Zombie_TVOE1 to Fast Deployment File. Added Zombie_TVOE2 to Fast Deployment File. Added imi(bond0.4) to Fast Deployment File. Added imi(bond0.3) to Fast Deployment File. Added imi(bond1.6) to Fast Deployment File. Added xsi2(bond1.7) to Fast Deployment File. Added xsi2(bond1.12) to Fast Deployment File. Added xsi2(bond1.13) to Fast Deployment File. Added xsi3(bond1.14) to Fast Deployment File. Added xsi3(bond1.15) to Fast Deployment File. Added xsi3(bond1.16) to Fast Deployment File. Added xsi1(bond1.16) to Fast Deployment File. Added xsi12(bond1.16) to Fast Deployment File. Added xsi12(bond1.16) to Fast Deployment File. Added xsi12(bond1.20) to Fast Deployment File. Added xsi13(bond1.20) to Fast Deployment File. Added xsi15(bond1.21) to Fast Deployment File. Added xsi15(bond1.21) to Fast Deployment File. Added xsi15(bond1.20) to Fast Deployment File. Added xsi15(bond1.20) to Fast Deployment File. Added xsi15(bond1.20) to Fast Deployment File. Added zombie_DSRNOAMI to Fast Deployment File. Added Zombie_DSRNOAMI to Fast Deployment File. Added Zombie_DSRNOAMI to Fast Deployment File. Added Zombie_SDSNNAMI to Fast Deployment File</pre>			[admusr@5010441PMAC RMS]\$ sudo ./config.sh rms.cfg
Added Cabinet 101 to Fast Deployment File. Added Zombie_TVO21 to Fast Deployment File. Added Zombie_TVO21 to Fast Deployment File. Added Xmi(bond0.4) to Fast Deployment File. Added xmi(bond0.4) to Fast Deployment File. Added xmi(bond0.7) to Fast Deployment File. Added xmi(bond0.12) to Fast Deployment File. Added xmi(bond0.13) to Fast Deployment File. Added xmi(bond0.14) to Fast Deployment File. Added xmi(bond0.15) to Fast Deployment File. Added xmi(bond0.16) to Fast Deployment File. Added xmi1(bond1.16) to Fast Deployment File. Added xmi1(bond1.16) to Fast Deployment File. Added xmi1(bond1.17) to Fast Deployment File. Added xmi1(bond1.10) to Fast Deployment File. Added xmi1(bond1.10) to Fast Deployment File. Added xmi1(bond1.12) to Fast Deployment File. Added xmi1(bond1.12) to Fast Deployment File. Added xmi1(bond1.21) to Fast Deployment File. Added xmi10(bond1.22) to Fast Deployment File. Added zmim_DSNROAM1 to Fast Deployment File. Added Zombie_DSNROAM1 to Fast Deployment File. Added Zombie_DSNROAM2 to Fast Deployment Fil			Validating cfg file Successful validation of cfg file
Added Zombie_TVCR1 to Fast Deployment File. Added Zmik_CVCR1 to Fast Deployment File. Added xmi(bond0.4) to Fast Deployment File. Added rep(bond1.10) to Fast Deployment File. Added rep(bond1.10) to Fast Deployment File. Added xil(bond1.7) to Fast Deployment File. Added xil(bond1.7) to Fast Deployment File. Added xil(bond1.1) to Fast Deployment File. Added xill(bond1.1) to Fast Deployment File. Added xill(bond1.2) to Fast Deployment File. Added zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_SSNOAM1 to Fast Deployment File. Added Zombie_SSNOAM2 to Fast Deployment File. Added Zombie_SSNOAM2 to Fast Deployment File. Added Zombie_SSNOAM1 to Fast Deployment File. Added Zombie_SSNOA			Added Cabinet 101 to Fast Deployment File.
<pre>Added Zombie_TVC22 to Fast Deployment File. Added xii(bond0.3) to Fast Deployment File. Added xii(bond1.6) to Fast Deployment File. Added xii(bond1.6) to Fast Deployment File. Added xii(bond1.8) to Fast Deployment File. Added xii(bond1.8) to Fast Deployment File. Added xii(bond1.1) to Fast Deployment File. Added xii(bond1.2) to Fast Deployment File. Added xii1(bond1.7) to Fast Deployment File. Added xii1(bond1.7) to Fast Deployment File. Added xii16(bond1.2) to Fast Deployment File. Added zombie_DSRNKOAMI to Fas</pre>			Added Zombie_TVOE1 to Fast Deployment File.
Added xmi(bond0.3) to Fast Deployment File. Added rep(bond1.10) to Fast Deployment File. Added xs12(bond1.6) to Fast Deployment File. Added xs12(bond1.7) to Fast Deployment File. Added xs13(bond1.8) to Fast Deployment File. Added xs16(bond1.12) to Fast Deployment File. Added xs16(bond1.13) to Fast Deployment File. Added xs10(bond1.16) to Fast Deployment File. Added xs11(bond1.17) to Fast Deployment File. Added xs11(bond1.18) to Fast Deployment File. Added xs11(bond1.18) to Fast Deployment File. Added xs112(bond1.18) to Fast Deployment File. Added xs112(bond1.18) to Fast Deployment File. Added xs112(bond1.18) to Fast Deployment File. Added xs112(bond1.21) to Fast Deployment File. Added xs115(bond1.21) to Fast Deployment File. Added xs115(bond1.22) to Fast Deployment File. Added xs116(bond1.22) to Fast Deployment File. Added zs116(bond1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_SSNOAM1			Added Zombie_TVOE2 to Fast Deployment File.
Addet Tam (Donors) of to Fast Deployment File. Added xsii (bond1.6) to Fast Deployment File. Added xsii (bond1.7) to Fast Deployment File. Added xsii (bond1.8) to Fast Deployment File. Added xsii (bond1.1) to Fast Deployment File. Added xsii (bond1.2) to Fast Deployment File. Added zsii (bond1.2) to Fast Deployment File. Added zombie DSRNOM2 to Fast Deployment File. Added Zombie DSRNOM2 to Fast Deployment File. Added Zombie DSRNOM2 to Fast Deployment File. Added Zombie SSNOM1 to Fast Deployment File. Added Zombie SSNOM2 to Fast Deployment File			Added xm1(bond0.4) to Fast Deployment File.
<pre>Added xsii(bond1.6) to Fast Deployment File. Added xsi2(bond1.7) to Fast Deployment File. Added xsi2(bond1.8) to Fast Deployment File. Added xsi3(bond1.12) to Fast Deployment File. Added xsi5(bond1.12) to Fast Deployment File. Added xsi5(bond1.13) to Fast Deployment File. Added xsi7(bond1.13) to Fast Deployment File. Added xsi8(bond1.14) to Fast Deployment File. Added xsi8(bond1.16) to Fast Deployment File. Added xsi8(bond1.16) to Fast Deployment File. Added xsi10(bond1.16) to Fast Deployment File. Added xsi10(bond1.16) to Fast Deployment File. Added xsi12(bond1.16) to Fast Deployment File. Added xsi12(bond1.16) to Fast Deployment File. Added xsi12(bond1.17) to Fast Deployment File. Added xsi12(bond1.10) to Fast Deployment File. Added xsi12(bond1.10) to Fast Deployment File. Added Xsi16(bond1.20) to Fast Deployment File. Added Zsi16(bond1.21) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Dep</pre>			Added rep(bond1.10) to Fast Deployment File.
Added xs12 (bond1.7) to Fast Deployment File. Added xs13 (bond1.9) to Fast Deployment File. Added xs14 (bond1.12) to Fast Deployment File. Added xs16 (bond1.12) to Fast Deployment File. Added xs16 (bond1.12) to Fast Deployment File. Added xs18 (bond1.13) to Fast Deployment File. Added xs19 (bond1.14) to Fast Deployment File. Added xs110 (bond1.16) to Fast Deployment File. Added xs111 (bond1.17) to Fast Deployment File. Added xs112 (bond1.17) to Fast Deployment File. Added xs112 (bond1.19) to Fast Deployment File. Added xs112 (bond1.19) to Fast Deployment File. Added xs114 (bond1.20) to Fast Deployment File. Added xs114 (bond1.21) to Fast Deployment File. Added xs116 (bond1.21) to Fast Deployment File. Added Xs116 (bond1.21) to Fast Deployment File. Added Zs116 (bond1.21) to Fast Deployment File. Added Zs116 (bond1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNDAM1 to Fast Deployment File. Added Zombie_SDSNDAM1			Added xsil(bond1.6) to Fast Deployment File.
<pre>Added xs13(bond1.8) to Fast Deployment File. Added xs15(bond1.11) to Fast Deployment File. Added xs15(bond1.12) to Fast Deployment File. Added xs17(bond1.13) to Fast Deployment File. Added xs17(bond1.13) to Fast Deployment File. Added xs10(bond1.16) to Fast Deployment File. Added xs10(bond1.16) to Fast Deployment File. Added xs110(bond1.16) to Fast Deployment File. Added xs111(bond1.17) to Fast Deployment File. Added xs112(bond1.18) to Fast Deployment File. Added xs112(bond1.20) to Fast Deployment File. Added xs113(bond1.20) to Fast Deployment File. Added xs114(bond1.20) to Fast Deployment File. Added xs116(bond1.20) to Fast Deployment File. Added zs116(bond1.21) to Fast Deployment File. Added zs116(bond1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSNNOAM2 to Fast Deployment File. Added Zombie_DSNNOAM1 to Fast Deployment File. Added Zombie_DSNNOAM1 to Fast Deployment File. Added Zombie_DSNNOAM1 to Fast Deployment File. Added Zombie_DSNNOAM2 to Fast Deployment File. Added Zombie_DSNOAM2 to Fast Deployment</pre>			Added xsi2(bond1.7) to Fast Deployment File.
Added Xs14 (bond.1) to Fast Deployment File. Added Xs16 (bond.11) to Fast Deployment File. Added Xs16 (bond.13) to Fast Deployment File. Added Xs17 (bond.13) to Fast Deployment File. Added Xs10 (bond.14) to Fast Deployment File. Added Xs110 (bond.15) to Fast Deployment File. Added Xs110 (bond.17) to Fast Deployment File. Added Xs112 (bond.17) to Fast Deployment File. Added Xs112 (bond.19) to Fast Deployment File. Added Xs112 (bond.19) to Fast Deployment File. Added Xs112 (bond.19) to Fast Deployment File. Added Xs113 (bond.20) to Fast Deployment File. Added Xs114 (bond.20) to Fast Deployment File. Added Xs115 (bond.21) to Fast Deployment File. Added Xs116 (bond.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRNAM2 to Fast Deployment File.			Added xsi3(bond1.8) to Fast Deployment File.
Added X316(bond:12) to Fast Deployment File. Added X316(bond:12) to Fast Deployment File. Added X316(bond:13) to Fast Deployment File. Added X318(bond:14) to Fast Deployment File. Added X3110(bond:15) to Fast Deployment File. Added X3112(bond:17) to Fast Deployment File. Added X3112(bond:19) to Fast Deployment File. Added X3112(bond:20) to Fast Deployment File. Added X3112(bond:21) to Fast Deployment File. Added X3112(bond:21) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_SSNOAM1 to Fast Deployment File. Added Zombie_SSNOAM2 to Fast Deployment File. Added Zombie_SSNOAM2 to Fast Deployment File. Added Zombie_SSNOAM1 to Fast Deployment File. Added Zombie_SSNOAM1 to Fast Deployment File. Added Zombie_SSNOAM2 to Fast Deployment File. Added Zombie_SSNOAM2 to Fast Deployment File. Added Zombie_SSNOAM1 to Fast Deployment File. Added Zombie_SSNOAM1 to Fast Deployment File. Added Zombie_SSNOAM2 to Fast Deployment File. Added Zombie_SSNOAM1 to Fast Deployment File. Added Zombie_SSNOAM2 to			Added xsi4(bond1.9) to Fast Deployment File.
Added xsi7(bond1.13) to Fast Deployment File. Added xsi3(bond1.14) to Fast Deployment File. Added xsi3(bond1.15) to Fast Deployment File. Added xsi11(bond1.16) to Fast Deployment File. Added xsi11(bond1.17) to Fast Deployment File. Added xsi13(bond1.19) to Fast Deployment File. Added xsi13(bond1.20) to Fast Deployment File. Added xsi13(bond1.21) to Fast Deployment File. Added xsi14(bond1.22) to Fast Deployment File. Added zombie_DSRNOM1 to Fast Deployment File. Added Zombie_DSRSNOM2 to Fast Deployment File. Added Zombie_DSRSNOM2 to Fast Deployment File. Added Zombie_DSRSNM1 to Fast Deployment File. Added Zombie_DSRDMP1 to Fast Deployment File. Added Zombie_DSRDMP1 to Fast Deployment File. Added Zombie_DSRDMP1 to Fast Deployment File. Added Zombie_DSRDMP2 to Fast Deployment File. Added Zombie_DSRDP5V1 to Fast Deployment File. Added Zombie_SDSDP5V2 to Fast Deployment_Of=15=16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_			Added x515(bond1.12) to Fast Deployment File.
<pre>Added xsi8(bond1.14) to Fast Deployment File. Added xsi9(bond1.15) to Fast Deployment File. Added xsi10(bond1.17) to Fast Deployment File. Added xsi11(bond1.17) to Fast Deployment File. Added xsi13(bond1.19) to Fast Deployment File. Added xsi14(bond1.20) to Fast Deployment File. Added xsi14(bond1.20) to Fast Deployment File. Added xsi16(bond1.21) to Fast Deployment File. Added zsi16(bond1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRSNOAM2 to Fast Deployment File. Added Zombie_DSRSNOAM2 to Fast Deployment File. Added Zombie_DSRSOAM2 to Fast Deployment File. Added Zombie_DSRSOAM1 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDFY2 to Fast Deployment File. Added Zombie_DSRDFY2 to Fast Deployment File. Added Zombie_SDSDFSV2 to Fast Deployment File. Added Zombie_SDSDFSV2</pre>			Added xsi7(bond1.13) to Fast Deployment File.
Added xsi9(bond1.15) to Fast Deployment File. Added xsi1(bond1.17) to Fast Deployment File. Added xsi11(bond1.17) to Fast Deployment File. Added xsi12(bond1.19) to Fast Deployment File. Added xsi13(bond1.20) to Fast Deployment File. Added xsi15(bond1.21) to Fast Deployment File. Added xsi15(bond1.22) to Fast Deployment File. Added xsi15(bond1.22) to Fast Deployment File. Added zmbie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_SDSSOM2 to Fast Deployment File. Added Zombie_SDSSOM2 to Fast Deployment File. Added Zombie_SDSPSY2 to Fast Deployment File. Yalidation file validation successful. Validation file validation successful. Validation file validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!!			Added xsi8(bond1.14) to Fast Deployment File.
Added xsill(bond1.16) to Fast Deployment File. Added xsil2(bond1.18) to Fast Deployment File. Added xsil3(bond1.20) to Fast Deployment File. Added xsil5(bond1.21) to Fast Deployment File. Added xsil6(bond1.22) to Fast Deployment File. Added zsil6(bond1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_DSRSOAM1 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_DSRSOAM1 to Fast Deployment File. Added Zombie_DSRSOAM1 to Fast Deployment File. Added Zombie_DSRSPAMP1 to Fast Deployment File. Added Zombie_DSRIFFE1 to Fast Deployment File. Added Zombie_SDSDFSV1 to Fast Deployment File. Added Zombie_SDSDFSV1 to Fast Deployment File. Added Zombie_SDSDFSV2 to Fast Deployment_06-15-16.xml SUCCESS: OFERATION SUC			Added xsi9(bond1.15) to Fast Deployment File.
<pre>Added xsil(bond1.19) to Fast Deployment File. Added xsil2(bond1.19) to Fast Deployment File. Added xsil5(bond1.20) to Fast Deployment File. Added xsil5(bond1.21) to Fast Deployment File. Added xsil5(bond1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_SDSDSV1 to Fast Deployment File. Added Zombie_SDSDSV2 to Fast Deployment File. Added Zombie_SDSDFSV2 to Fast Deployment File. Added ZOMENESSUMENT SUC</pre>			Added xsil0(bond1.16) to Fast Deployment File.
Added xsi13 (bond1.19) to Fast Deployment File. Added xsi14 (bond1.20) to Fast Deployment File. Added xsi16 (bond1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNNOAM2 to Fast Deployment File. Added Zombie_DSRNNOAM2 to Fast Deployment File. Added Zombie_DSRNNOAM2 to Fast Deployment File. Added Zombie_SDSNNOAM2 to Fast Deployment File. Added Zombie_SDSNNOAM1 to Fast Deployment File. Added Zombie_SDSNNOAM2 to Fast Deployment File. Added Zombie_SDSNNOAM1 to Fast Deployment File. Added Zombie_SDSNAM1 to Fast Deployment File. Added Zombie_SDSNAM1 to Fast Deployment File. Added Zombie_SDSNAM1 to Fast Deployment File. Added Zombie_SDSSOAM1 to Fast Deployment File. Added Zombie_SDSNAM1 to Fast Deployment File. Added Zombie_SDSNAM2 to Fast Deployment File. Added Zombie_SDSNAM2 to Fast Deployment File. Added Zombie_SDSNFY1 to Fast Deployment File. Added Zombie_SDSNFY2 to Fast Deployment_06-15-16.xml" Configuration file validation successful. Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS:! Iamusrefigenter Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml			Added xsill(bond1.17) to Fast Deployment File.
Added xsi14(bond1.20) to Fast Deployment File. Added xsi16(bond1.21) to Fast Deployment File. Added zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSSOAM1 to Fast Deployment File. Added Zombie_SDSSOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSNAM2 to Fast Deployment File. Added Zombie_SDSPSV1 to Fast Deployment File. Added Zombie_SDSDFSV2 to Fast Deployment File. Added Zombie_SDSDFSV2 to Fast Deployment file. Added Zombie_SDSDFSV2 to Fast Deployment_S10. Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!!			Added xsi13(bond1.19) to Fast Deployment File.
Added xsi15(bond1.22) to Fast Deployment File. Added xsi16(bond1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRDRNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNNOAM2 to Fast Deployment File. Added Zombie_SDSNNAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSNAM1 to Fast Deployment File. Added Zombie_SDSNAM1 to Fast Deployment File. Added Zombie_SDSNAM2 to Fast Deployment File. Added Zombie_SSNIFFE1 to Fast Deployment File. Added Zombie_SSNIFFE2 to Fast Deployment File. Added Zombie_SDSDFSV2 to Fast Deployment File. Validating Fast Deployment File. Validation complete Successful Validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!!			Added xsi14(bond1.20) to Fast Deployment File.
Added XS116(CON1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRDRNOAM2 to Fast Deployment File. Added Zombie_DSRDRNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSDRNOAM1 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_SDSDRNOAM1 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_SDSDAMP1 to Fast Deployment File. Added Zombie_SDSDAMP1 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_SDSDFSV1 to Fast Deployment File. Added Zombie_SDSDFSV2 to Fast Deployment File. Added Zombie_SDSDFSV2 to Fast Deployment File. Added Zombie_SDSDFSV2 to Fast Deployment File. Validating Fast Deployment File Validating Fast Deployment File. Validation configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml			Added xsi15(bond1.21) to Fast Deployment File.
Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRDRNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSDRNOAM1 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSSOAM1 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM1 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_SDSNDAMP2 to Fast Deployment File. Added Zombie_SDSNDAMP2 to Fast Deployment File. Added Zombie_SDSNDAMP2 to Fast Deployment File. Added Zombie_SDSNPFE1 to Fast Deployment File. Added Zombie_SDSNPFE2 to Fast Deployment File. Added Zombie_SDSNPF2 to Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!!			Added Xsil6(bond1.22) to fast Deployment File. Added Zombie DSRNOLM1 to Fast Deployment File
Added Zombie_DSRDRNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_DSRSOAM1 to Fast Deployment File. Added Zombie_DSRSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDAMP2 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Validating Fast Deployment File			Added Zombie DSRNOAM1 to Fast Deployment File.
Added Zombie_DSRDRNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSDRNOAM1 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_DSRSOAM1 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_SDSDFSV1 to Fast Deployment File. Added Zombie_SDSDFSV1 to Fast Deployment File. Added Zombie_SDSDFSV2 to Fast Deployment File. Added Zombie_SDSDFSV2 to Fast Deployment File. Added Zombie_SDSDFSV2 to Fast Deployment File. Validating Fast Deployment File Validation file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" SUCCESS: OPERATION SUCCESS!! Ladmusr&SUCCESS: OPERATION SUCCESS!!			Added Zombie DSRDRNOAM1 to Fast Deployment File.
Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_DSRSOAM1 to Fast Deployment File. Added Zombie_DSRSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM1 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_DSRSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_DSRIPFE2 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Validating Fast Deployment File Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!!			Added Zombie_DSRDRNOAM2 to Fast Deployment File.
Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSDRNOAM1 to Fast Deployment File. Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_DSRSOAM1 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDAMP2 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Validating Fast Deployment File Validation file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!!			Added Zombie SDSNOAM1 to Fast Deployment File.
Added Zombie_SDSDRNOAM2 to Fast Deployment File. Added Zombie_DSRSOAM1 to Fast Deployment File. Added Zombie_DSRSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_DSRIPFE2 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Validating Fast Deployment File			Added Zombie_SDSNOAM2 to Fast Deployment File.
Added Zombie DSRSOAM1 to Fast Deployment File. Added Zombie DSRSOAM2 to Fast Deployment File. Added Zombie SDSSOAM1 to Fast Deployment File. Added Zombie SDSSOAM2 to Fast Deployment File. Added Zombie DSRDAMP1 to Fast Deployment File. Added Zombie DSRDAMP2 to Fast Deployment File. Added Zombie DSRIPFE1 to Fast Deployment File. Added Zombie SDSDPSV1 to Fast Deployment File. Added Zombie SDSDPSV1 to Fast Deployment File. Added Zombie SDSDPSV2 to Fast Deployment File. Added Zombie SDSDPSV2 to Fast Deployment File. Validating Fast Deployment File			Added Zombie SDSDRNOAM2 to Fast Deployment File.
Added Zombie_DSRSOAM2 to Fast Deployment File. Added Zombie_SDSSOAM1 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDAMP2 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Validating Fast Deployment File Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!! Ladmusrd65010441PMAC_RMSIS			Added Zombie DSRSOAM1 to Fast Deployment File.
Added Zombie_SDSSOAM1 to Fast Deployment File. Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_DSRIPFE2 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Validating Fast Deployment File Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete SUCCESS: OPERATION SUCCESS!! Ladmusrd65010441PMAC_RMSIS			Added Zombie_DSRSOAM2 to Fast Deployment File.
Added Zombie_SDSSOAM2 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_DSRIPFE2 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Validating Fast Deployment File Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!!			Added Zombie_SDSSOAM1 to Fast Deployment File.
Added Zombie_DSRDAMP2 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_DSRIPFE2 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Validating Fast Deployment File Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!! Ladmusrd65010441PMAC_RMSIS			Added Zomble_SDSSOAM2 to Fast Deployment File.
Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_DSRIPFE2 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Validating Fast Deployment File Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!! Iadmusrd65010441PMAC_RMSIS			Added Zombie DSRDAMP2 to Fast Deployment File.
Added Zombie_DSRIPFE2 to Fast Deployment File. Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Validating Fast Deployment File Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!!			Added Zombie DSRIPFE1 to Fast Deployment File.
Added Zombie_SDSDPSV1 to Fast Deployment File. Added Zombie_SDSDPSV2 to Fast Deployment File. Validating Fast Deployment File Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!! [admusrd5010441PMAC_RMS15]			Added Zombie DSRIPFE2 to Fast Deployment File.
Validating Fast Deployment File. Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!!			Added Zombie SDSDPSV1 to Fast Deployment File.
Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!!			Validating Fast Deployment File.
Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!! [admusr@5010441PMAC_RMSIS]			Validate configuration file: "Zombie DSR Fast Deployment 06-15-16.xml"
Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!!			Configuration file validation successful.
Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!!			Validation complete
			Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml
			[admusr@5010441PMAC RMS]\$

Procedure 2. Recovery Scenario 2

20 .	PMAC : Execute fast deployment	With the file generated from the config.sh script, execute the following command to start fast deployment:							
]		<pre>\$ screen \$ sudo fdconfig configfile=<fd_config.xml></fd_config.xml></pre>							
		Note: This is a long duration command. 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.							
21.	PMAC GUI: Monitor the configuration	1. If no 2. Nav	 If not already done, establish a GUI session on the PMAC server. Navigate to Task Monitoring. 						
		 Status and Manage Task Monitoring Help Legal Notices Logout Monitor the configuration to completion: 							
		Main Menu:	: Task Monitoring						
		Filter* •			61-14	Teloned	Questine Time	Charle Times	Deserves
		 925 Acc 	cept Zombie SDSDRNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:35	100%
		📄 924 Acc	RMS: pc5010441 Guest: Zombie_SDSNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:04	100%
		923 Act	cept RMS: pc5010441 Guest: Zomble_DSRIPFE1	Success.	COMPLETE	N/A	0:01:06	2018-07-11 11:26:43	100%
		922 Act	cept RMS: pc5010439 Guest: Zomble_DSRDAMP2	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%
		921 Acc	Cept RMS: pc5010441 Guest: Zombie: DSR0AMP1	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%
		920 Act	cept Guest: Zombie_DSRSOAM2	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:42	100%
		Note: [admusrd file=dep Dump Ste Here ard Dump of NUM PHS 1 1 0 pr availab: 2 1 0 pr 3 1 0 pr 4 2 0 pr 4. Res \$ sud file=dep Dump Ste Here ard \$ sud file=dep Dump Ste Here ard Ste Ste Ste Ste Ste Ste Ste Ste	If a failure occurs of /var/TKLC/log/fdc @melbourne-pmac-1 ploy_melbourne_20: eps in file: "depl e the steps that of DB steps: DLY INFRA ID SVR: mac Fast_Deployment mac Fast_Deployment mac Fast_Deployment mac Fast_Deployment mac Fast_Deployment mac Fast_Deployment mac Fast_Deployment tart the fdconfig rest rdeploy_melbour	with fdconfig, le config/fdconfi fdconfig]\$ su 170329T202458 loy_melbourne_ were generated TYPE CMD ELEMI nt 0 21 0 Comp nt 0 1 1 1 Sk: nt 0 3 melbourn t 1 ter a failure ha start cne_2017032	ogs can b g.log file. ado fdcom _701b.fdcd _20170329 d = ENT PRE S ⁴ plete 300 ipped 300 cne_RMS3 = s occurree	e acces fig dum db T202458 TATE TO 0 Chec 0 Add 1 Skipp d and h 8_7013	BGTS (k PM&C Cabinet ed 900 as been	 Edcdb" COMMAND is 0 Add n resolv	TEXT Rms /ed:

Procedure	2.	Recovery	Scenario 2
-----------	----	----------	------------

PMAC : Repeat for each rack mount server configuration file	Repeat steps 1421. for each rack mount server/configuration file, if required.				
PMAC: Back up FDC file	1. Copy the updated fdc file to the fdc backup directory:				
	<pre>\$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> /usr/TKLC/smac/etc/fdc/</fdc_file></pre>				
	2. Change permissions:				
	<pre>\$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/<fdc_file></fdc_file></pre>				
Perform CPU pinning	Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only) procedure from reference [8].				
NOAM GUI : Login	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:				
If the failed server is not OAM. then	http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>				
Skip to Step 47.	ORACLE®				
	Oracle System Login Mon Jul 11 13:59:37 2016 EDT				
	Log In Enter your username and password to log in Username:				
	PMAC: Repeat for each rack mount server configuration file PMAC: Back up FDC file Perform CPU pinning NOAM GUI: Login If the failed server is not OAM, then skip to step 47.				

Procedure 2.	Recovery	Scenario 2
--------------	----------	------------

26.	NOAM VIP GUI: Recover standby NOAM, if needed	Install the second NOAM server: DSR : Execute the Configure the Second NOAM Server procedure, steps 1 and 3- 6, from reference [8]. SDS : Execute the Configure the Second SDS NOAM Server procedure, steps 1 and 3-6, from reference [8].				
27.	Install NetBackup client (optional)	If NetBackup is used procedure from reference	l, execute the Install N ence [8].	etBackup Client (Optional)		
28.	NOAM VIP GUI: Set HA on standby NOAM	 Navigate to Status & Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click Edit. Select the standby NOAM server and set it to Active. Modifying HA attributes 				
		Hostname	Max Allowed HA Role	Description		
		ZombieNOAM1	Active	The maximum		
ZombieNOAM			Active Active	The maximum		
		ZombieDRNOAM1 4. Click OK.	Standby Spare	The maximum		

Procedure 2. Recovery Scenario 2

29.	1. Navigate to Status & Manage > Server.					
	Restart DSR	🖻 😋 Status & Manage				
	application	Network Elements				
		Server				
		HA HA				
		Database				
		Files				
		 Select the recovered standby NOAM server and click Restart. 				
		on Postart Poho				
		op Restart Rebo				
30. □	NOAM VIP GUI: Recover query servers. SDS only. If DSR, skip to step 33.	Execute the Configuring SDS Query Servers procedure, steps 1 and 4-7, from reference [8].				
31.	SDS NOAM VIP	1. Navigate to Status & Manage > HA.				
	GUI: Set HA on	🔤 📥 Status & Manage				
	SDS only If DSR	Claus & manage Metwork Elements				
	skip to step 33.	Server				
		Tatabase				
		KPIs				
		Processes				
		🗈 🧰 Tasks				
		🔤 🔛 Files				
		2. Click Edit.				
		3. Select the query server and select Observer .				
		ZombieQS1 Observer The Observer OOS				
		4. Click OK .				

32.	SDS NOAM VIP	1. Navigate to Status & Manage > Server.		
	GUI: Restart SDS	😑 😋 Status & Manage		
	application.	Network Elements		
	skip to step 33	Server		
		HA HA		
		Database		
		KPIs		
		Processes		
		2. Select the recovered query server and click Restart .		
		an Destart Debar		
		op Restart Rebot		
22				
□ □	Stop replication to	Before continuing this procedure, replication to C-level servers MUST be		
	the C-level servers	inhibited at the SOAM site being recovered.		
	of this site.	Failure to inhibit replication to the working C-level servers results in the		
		database being destroyed!		
		If the spare SOAM is also present in the site and lost, execute Appendix 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.		
		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.		
		Ear SDS		
		Inhibit database replication for defective SOAM servers and DP servers associated with this SOAM network element.		
		NOTE: It is expected that each SOAM and subtending DP will have a DB Level of "UNKNOWN" until the SOAMs are restored.		
		1. Go to the NOAMP GUI.		
		2. Select [Main Menu: Status & Manage → Database] screen		
		3. Filter on the SOAM Network Element name.		
		4. Record the DP server hostnames (Role: MP).		
		5. Click "Inhibit Replication" button for each DP server until all DP servers associated with this SOAM Network Element have been inhibited		
		"Inhibiting" SOAM server: Click "Inhibit Replication" button for each defective SOAM servers.		

34.	NOAM VIP GUI: Recover active SOAM server	Install the SOAM servers. DSR : Execute the Configure the SOAM Servers procedure, steps 1-3 and 5-9, from reference [8]. <i>Note:</i> If you are using NetBackup, also execute step 12. SDS :				
		Execute the Configure the SDS DP SOAM Servers procedure, steps 1-3 and 5-8, from reference [8].				
35.	NOAM VIP GUI: Set HA on the SOAM server	 1. Navigate to Status & Manage > HA. 				
		2 Click Edit				
		 Select the SOAM server and set it to Active. 				
		Zombie SOAM1 Active The m				
		Zombie SOAM2 Spare The m Observer OOS				
		4. Click OK .				
36.	NOAM VIP GUI: Restart DSR application	 1. Navigate to Status & Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Select the recovered SOAM server and click Restart. 				

37.	NOAM VIP GUI:	1. Navigate to Status & Manage > Files.		
37.	NOAM VIP GUI: Upload the backup SOAM database file. DSR only. If SDS, skip to step 42.	 1. Navigate to Status & Manage > Files. Status & Manage Network Elements Server HA Database KPIs Processes Tasks 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. Upload Do 3. Click Browse and locate the backup file. 4. Mark the This is a backup file checkbox. 5. Click Open. 6. Click Upload. 		
		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.		

-					
38. □	Recovered SOAM GUI: Login. DSR only. If SDS, skip to step 42.	1.	Establish a GUI session on the recovered SOAM server.		
		2.	Open the web browser and enter a URL of:		
			http:// <recovered_soam_ip_address></recovered_soam_ip_address>		
		3.	Login as the guiadmin user:		
		ORACLE			
	Oracle System Login Tue Jun 7 13:49:0				
			racle System Login Tue Jun 7 13:49:06 2016 EDT		
			Log In		
			Enter your username and password to log in		
			Username:		
			Password:		
			Change password		
			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.		10.0, or 11.0 with support for JavaScript and cookies.		
	Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.				
			Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.		

Procedure 2. Recovery Scenario 2

	,				
39. □	Recovered SOAM GUI: Verify the archive contents and database compatibility. DSR only. If SDS, skip to step 42.	1. Na 2. Se	vigate to Status & Manage > Database . lect the Active SOAM server and click Compare .		
		ıp	Compare Resto		
		3. Cli 27.	ck the button for the restored database file uploaded as a part of step . of this procedure.		
		Data	abase Compare		
		Selec	t archive to compare on server: Z		
		Archiv	ve* backup/Backup.DSR.Zom 		
		Ok	Cancel		
		- On			
			rify the output window matches the screen below.		
		Datat	base Archive Compare		
		The	selected database came from ZombieSOAM1 on 10		
		Conf	iguration data		
		Data	base Compatibility		
		The	databases are compatible.		
		Note:	Archive Contents and Database Compatibilities must be the following:		
			Archive Contents: Configuration data.		
			Database Compatibility: The databases are compatible.		
		Note:	The following is expected output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one SOAM:		
			Topology Compatibility		
			The topology should be compatible minus the NODEID.		
		Note:	We are trying to restore a backed up database onto an empty SOAM database. This is an expected text in Topology Compatibility.		
		5. If this	he verification is successful, click Back and continue to next step in s procedure.		
Procedure 2. Recovery Scenario 2

10	, ,	
40.	Recovered SOAM GUI:	1. Select the Active SOAM server and click Restore.
	Restore the	2. Select the backup provisioning and configuration file.
	database.	Database Compare
	DSR only. If SDS, skip to step 42	
		Select archive to compare on serv
		Archive *
		Ok Cancel
		3. Click OK .
		Database Restore Confirm
		Compatible archive
		Compatible archive.
		The selected database came from Zomb:
		Archive Contents Configuration data
		Database Compatibility
		The databases are compatible.
		 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.
		Notes:
		 After the restore has started, the user is logged out of XMI SOAM GUI since the restored topology is old data.
		 If the spare SOAM is in another network and is unreachable, the database restore cannot be done.
		Workaround: If the spare SOAM is unreachable and ping (from
		recovered SOAM server to spare SOAM server) hangs (as evidenced by
		than 10 seconds), then kill the hung ping processes and the restore proceeds.
41.	Recovered	Wait for 5-10 minutes for the system to stabilize with the new topology:
	SOAM GUI:	Monitor the Info tab for Success. This indicates the restore is complete and
	confirm database	the system is stabilized.
	restoral.	NOTES:
	DSR only. If SDS, skip to step 42	completely restored.
		The Configuration and Maintenance information is in the same state it
		was when backed up during initial backup.

42. 	NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:		
		http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>		
		2. Login as the guiadmin user:		
		ORACLE		
		Uracle System Login Tue Jun 7 13:49:06 2016 EDT		
		Log In Enter your username and password to log in Username: Password: Change password Change password Log In Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies. Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.		
43.	NOAM VIP GUI:	DSR:		
Recover the		Execute the Configure the SOAM Servers procedure, steps 1-3 and 5-9,		
	servers (standby,	Note: If you are using NetBackup also execute step 12		
	spare)	SDS:		
		Execute the Configure the SDS DP SOAM Servers procedure, steps 1-3 and 5-8, from reference [8].		

44.	NOAM VIP GUI: Un-Inhibit (start) replication to the recovered SOAM servers Start replication on the recovered SOAMs, if replication is inhibited Un-Inhibit (start) replication to the recovered SOAM servers Navigate to Status & Manage Network Elements Network Elements Server HA Database	
		Processes
		6. Click Allow Replication on the recovered SOAM servers.
		 Verify the replication on all SOAMs servers is allowed. This can be done by checking Repl status column of respective server
45.	NOAM VIP GUI: Set HA on the recovered standby SOAM server	 Navigate to Status & Manage Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click Edit at the bottom of the screen Select the recovered standby SOAM server and set it to Active. Zombie SOAM1 Active The m Active Standby Spare Observer Observer OS Click OK.

Procedure 2. Recovery Scenario 2

46.	NOAM VIP GUI:	1. Navigate to Status & Manage > Server.	
	application	🖃 😋 Status & Manage	
		🔤 💽 Network Elements	
		Server Server	
		HA 📉	
		Database	
		KPIS	
		2. Select the recovered NOAM server and click Restart .	
		p Restart Rebo	
47 . □	NOAM VIP GUI: Start replication on	Un-Inhibit (start) replication to the working C-level Servers which belongs to the same site as of the failed SOAM servers.	
	working C-level 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.	
		🖃 😋 Status & Manage	
		Network Elements	
		Server	
		Database	
		KPIs	
		Processes	
		2. If the Repl Status is set to Inhibited , click Allow Replication using this order; otherwise, if none of the servers are inhibited, skip this step and continue with the next step:	
		Active NOAM Server	
		Standby NOAM Server	
		Active SOAM Server	
		Standby SOAM Server	
		 Spare SOAM Server (if applicable) — Oracle X5-2/Netra X5-2/X6- 2/X7-2/HP DL380 Gen 9 Only 	
		Active DR NOAM Server	
		Standby DR NOAM Server	

-	,				
		MP/IPFE S the active I	Servers (if MPs are MP; otherwise, the	configured as active order of the MPs do	e/standby, start with bes not matter)
		 SBRS (if S standby, th DL380 Ger 	BR servers are con len spare) — Oracle n 9 Only	figured, start with tl e X5-2/Netra X5-2/>	he active SBR, then K6-2/ X7-2/HP
		 Verify the replic done by exami 	cation on all the wo ning the Repl Statu	rking servers is allo s table.	wed. This can be
		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
10		Allow database rep associated with this 1. Go to the NOA 2. Select [Main M 3. Filter on the SC 4. Record the DP 5. Wait until audit "Allow Replicat servers Allowing Replicatio all DP servers associnhibited	blication for SOAM- s SOAM network el MP GUI. Ienu: Status & Mar DAM Network Elem server hostnames becomes active or tion" button for each m: Click "Allow Rep pociated with this SO	A and SOAM-B servement. nage → Database] ent name. (Role: MP). a SOAM's. Allowing a newly replaced SC lication" button for e AM Network Eleme	vers and DP servers screen Replication: Click DAM-A and SOAM-B each DP server until ent have been
48.	feature. DSR only	executing the PCA in executing the PCA recovered standby	Activation on Ent	n being recovered, ire Network proced [7].	dure on the
49. □	NOAM VIP GUI: Recover the C- level server (DA- MPs, SBRs, IPFE,	DSR: Execute the Config reference [8].	gure the MP Serve	rs procedure, steps	s 1 and 9-13, from
	SS7-MP, and SDS DPs	Note: Also execu your MP th network.	ite steps 14-16 if yc at uses a signaling	ou plan to configure (XSI) network inste	a default route on ead of the XMI
		SDS (Oracle X5-2/	Netra X5-2/X6-2/ X	7-2/HP DL380 Gen	9 Only):
		Execute the Config from reference [8].	gure the SDS DP S	servers procedure,	steps 1 and 5-8,
		Repeat this step fo	r any remaining fail	ed MP servers.	

Procedure 2. Recovery Scenario 2

50.	NOAM VIP GUI:	1. Navigate to Status & Manage -> HA.	
	Set HA on all C- level servers	 Status & Manage Network Elements Server HA Database KPIs Processes 2. Click Edit. 3. For each recovered C-Level with a Max Allowed HA Role set to OOS, set it to Active.	
		ZombieDAMP1 Active The maximum desired HA Role for ZombieDAMI Active Standby Spare ZombieDAMP2 Spare The maximum desired HA Role for ZombieDAMI 4. Click OK. Click OK.	
51.	NOAM VIP GUI: Restart DSR application on the recovered C-level servers	e 1. Navigate to Status & Manage e Status & Manage e Network Elements e Server e HA e Database e KPIs e Processes 2. Select the recovered C-level servers and click Restart. p Restart	

52.	NOAM VIP GUI: Start replication on	Un-Inhibit (start) replication to the ALL C-level servers.1. Navigate to Status & Manage > Database.			
	all C-Level servers.	📄 🔄 Status (& Manage		
	DSR only. If SDS,	Net	work Elements		
	then skip to next	Sen	ver		
	Step.	🟹 HA			
		🔤 💽 Dat	abase		
		🔤 🕅 KPI	S		
		🕅 Pro	cesses		
		2. If the Repl Sta order:	atus is set to Inhibi t	ted, click Allow Re	plication using this
		Active NC	AMP Server		
		Standby N	NOAMP Server		
		Active SO	AM Server		
		Standby S	SOAM Server		
		Spare SO X7-2/HP [AM Server (if appli DL380 Gen 9 Only)	cable) — Oracle X	5-2/Netra X5-2/X6-2/
		Active DR	NOAM Server		
		Standby E	OR NOAM Server		
		MP/IPFE	Servers		
		SBRS (if \$ standby, t DL380 Ge	SBR servers are cor hen spare) — Oracl en 9 Only	nfigured, start with t e X5-2/Netra X5-2/	he active SBR, then X6-2/ X7-2/HP
		3. Verify the repl checking the I	ication on all server Repl Status .	s is allowed. This c	can be done by
		OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
		NotApplicable	NotApplicable	Allowed	NotApplicable
		Normal	NotApplicable	Allowed	NotApplicable
		Normal	NotApplicable	Allowed	NotApplicable
		Normal	NotApplicable	Allowed	NotApplicable
53.	Active NOAM:	1. Establish an S	SSH session to the a	active NOAM and Ic	gin as admusr .
	Perform keyexchange between the active-NOAM and recovered servers	2. Perform a keyexchange from the active NOAM to each recovered server:			
		\$ keyexchange	e admusr@ <recov< td=""><td>vered Server Ho</td><td>stname></td></recov<>	vered Server Ho	stname>
		Note: If an export server is configured perform this step			
		wote. In an expo	it server is coningun	eu, periorni inis sie	μ .

Procedure 2.	Recovery	Scenario 2
--------------	----------	------------

54.	Active NOAM: Activate optional features. DSR only. If SDS, then skip to next step.	stablish an SSH session to the active NOAM and login as admu	sr.
		ote for PCA Feature Activation:	
		you have PCA installed in the system being recovered, re-activally executing the PCA Activation on Stand By NOAM Server pro- e recovered standby NOAM server; and the PCA Activation on OAM Server procedure on the recovered active SOAM server from the the technology of the server from the technology of tech	te the PCA ocedure on Active om [6].
		otes:	
		If not all SOAM sites are recovered at this point, then repeat the activation for each "new" SOAM site that comes online.	ne
		If any of the MPs have failed and recovered, then restart these servers after activation of the feature.	e MP
		efer to section 1.5 Optional Features to activate any features tha reviously activated.	t were
		ote: While running the activation script, the following error mes corresponding messages) output may display. This can s ignored:	sage (and afely be
		iload#31000{S/W Fault}	

55.	NOAM VIP GUI: Fetch and store the database report for the newly restored data and save it	 1. Navigate to Status & Manage > Database. Status & Manage
2. S oning T Mai		2. Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Report . Image: Select the active NOAM server and click Rep
		dsr Database Status Report
		Report Generated: Tue Oct 11 13:24:26 2016 EDT From: Active Network OAM&P on host ZombieNOAM1 Report Version: 8.0.0.0.0-80.9.0 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 2. Recovery Scenario 2

56.	Active NOAM: Verify replication between servers	 Log into the active NOAM as admusr using SSH terminal. Execute this command:
		\$ sudo irepstat -m
		Example output:
		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
		Vanu-NOAM-2 Active
		AA = 10 $Cahu - NOAM - 1$ $ACCIVE = 0$ 0.25 $16K = 0.048$ Cpu $01B/S$
		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

57.	NOAM VIP GUI:	1. Navigate to Status	& Manager	> Database.		
	Verify the database states	 Status & Manag Network Ele Server HA Database KPIs Processes Verify the OAM Max SOAM; Application Normal: 	je ments k HA Role is Max HA Rol	either Active le for MPs is <i>i</i>	e or Standby fo Active ; and sta	or NOAM and atus is
		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	ZombielPFE1		MP	Active
		ZombieSOAM	ZombieIPFE2		MP	Active
58.	Verify the HA status	 Navigate to Status Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the row for al Verify the HA Role i 	and Manag Il of the serv is either Act	e > HA. [.] ers. ive or Stand	Dy.	
		Hostname		OAM HA Role	Application HA	Max Allowed HA
		7			Role	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
-----------	-------------	----------	---

50		A Ne leste la Otatura O Manague - Database
59.	SOAM GUI: Enable site	1. Navigate to Status & Manage > Database.
	provisioning.	📃 😋 Status & Manage
	DSR only. If SDS,	🔤 🔯 Network Elements
	skip to step 69.	Server 🔂
		The second secon
		Database
		KPIs
		Collist Freedore Description
		2. Click Enable Site Provisioning.
		Enable Site Provisioning Report Inhibit/Allo
		3. A confirmation window displays. Click OK to enable provisioning.
60.	SOAM VIP GUI:	1. Navigate to Diameter > Configuration > Local Node .
	Verify local node	🖶 🕞 Diameter
	Information.	n Configuration
	DSR ONLY. IT SDS, skin to sten 69	Capacity Summary
	3kip to 3tep 03.	Connection Capacity Dashb
		Application Ids
		CEX Parameters
		Command Codes
		Configuration Sets
		🖺 Local Nodes
		2. Verify all the local nodes are shown.
61.	SOAM VIP GUI:	1. Navigate to Diameter > Configuration > Peer Node .
	verify the peer	📄 😋 Diameter
		🖻 🔄 Configuration
	then skip to step	Capacity Summary
	69.	Connection Capacity E
		Application Ids
		CEX Parameters
		Peer Nodes
		2. Verity all the peer nodes are shown.

62.	SOAM VIP GUI: Verify the connections information. DSR only. If SDS, then skip to step 69.	 1. Navigate to Diameter > Configuration > Connections. Diameter Configuration Capacity Summary Connection Capacity Dash Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Node Peer Node Groups Connections 2. Verify all the connections are shown.
63. □	MP Servers: Disable SCTP Auth Flag. DSR only. If SDS, then skip to step 69.	For SCTP connections without DTLS enabled, refer to the Enable/Disable DTLS (SCTP Diameter Connections Only) section in reference [8]. Execute this procedure on all failed MP servers.
64.	SOAM VIP GUI: Enable connections, if needed. DSR only. If SDS, then skip to step 69.	 3. Navigate to Diameter > Maintenance > Connections. Maintenance Route Lists Route Groups Peer Nodes Connections 4. Select each connection and click Enable. Alternatively, enable all the connections by clicking EnableAll. EnableAll Disable. 5. 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

 65. SOAM VIP GUI: Enable optional features. DSR only. If SDS, then skip to step 69. 1. Navigate to Diameter > Maintenance > Applications. Route Groups 69. Select the optional feature application configured in step 72. 3. Click Enable. Enable Disable Pause updates 66. 67. SoAM VIP GUI: Benable Disable Block 7. Solar VIP GUI: Benable Disable Block 7. Verify the Operational Status for each transport is Up. 67. Solar VIP GUI: Benable Disable Block 7. Verify the Operational Status for each transport is Up. 7. Configuration 8. C		-	
 Interesting the step of the s	65.	SOAM VIP GUI: Enable optional features.	1. Navigate to Diameter > Maintenance > Applications .
DSR only. If SDS, then skip to step 69. Route Groups 69. Connections Egress Throttle Groups Connections Egress Throttle Groups 2. Select the optional feature application configured in step 72. 3. Click Enable. Enable Pause updates 66. SOAM VIP GU: Pause updates 1. Navigate to Transport Manager Maintenance Pause updates 2. Select each transport Manager Maintenance Maintenance Maintenance Maintenance Select each transport and click Enable. Enable Disable Block 3. Verify the Operational Status for each transport is Up. 67. SOAM VIP GU: 1. Navigate to SST/Sigtran > Maintenance > Local SCCP Users. MAPINF SST/Sigtran > Maintenance DSR only. If SDS, then skip to step 69. Configuration Select each transport Signaling Points Remote Signaling Points Remote Signaling Points Remote MTP3 Users Select Use Enable button corresponding to MAPIWF Application Name.			🖃 🚖 Maintenance
then skip to step 69. Route Groups Peer Nodes Connections Egress Throttle Groups 2. Select the optional feature application configured in step 72. 3. Click Enable. Enable Disable Pause updates Invariance > Transport. Re-enable transports, if needed. Navigate to Transport Manager DSR only. If SDS, then skip to step 69. Invariante ance Enable Disable Block Stransport 3. Verify the Operational Status for each transport is Up. 67. SOAM VIP GU: APPINF application, if needed. Invarigate to SS7/Sigtran > Maintenance > Local SCCP Users. Select each transport Manager SS7/Sigtran > Maintenance > Local SCCP Users. Select each transport and click Enable. Status for each transport is Up. 67. SOAM VIP GU: APPINF application, if needed. Invarigate to SS7/Sigtran > Maintenance > Local SCCP Users. Select Block Status SCP Users Remote Signaling Points Select ME Enable Local SCCP Users Select Block Status is Enabled. 3. Verify the SSN Status is Enabled.		DSR only. If SDS,	Route Lists
69. Peer Nodes Connections Connections Egress Throttle Groups Applications 2. Select the optional feature application configured in step 72. Click Enable Bee-nable Pause updates 66. SOAM VIP GUI: Navigate to Transport Manager > Maintenance > Transport. Pause updates Transport Manager DSR only. If SDS, then skip to step Maintenance 69. SodM VIP GUI: Select each transport and click Enable. Enable Disable Block 3. Verify the Operational Status for each transport is Up. Select each transport and click Enable. Franke Disable Block 3. Verify the Operational Status for each transport is Up. Navigate to SS7/Sigtran > Maintenance > Local SCCP Users. Franke Soft of SSN mays. Bit to step 69. Maintenance DSR only. If SDS, then skip to step 69. Configuration Select each transport Signaling Points Remote Signaling Points Remote MTP3 Users Remote MTP3 Users Disable Disable Solution of the sets Links ets Solution of the sets Solutis the SN Status is Enabled. Sou		then skip to step	Route Groups
 66. SOAM VIP GUI: Re-enable Transport Manager readed. DSR only. If SDS, then skip to step 69. 70. SOAM VIP GUI: Transport Manager readed. DSR only. If SDS, then skip to step 69. 71. Navigate to Transport Manager > Maintenance > Transport. Transport Manager Transport Man		69.	🔤 🔯 Peer Nodes
 Soam VIP GU: Re-enable transports, if readed. DSR only. If SDS, then skip to step G9. Soam VIP GU: Re-enable transport Manager Transport Manager Configuration DSR only. If SDS, then skip to step G9. Navigate to Transport Manager Transport Manager Configuration Select each transport and click Enable. Enable Disable Block Soam VIP GU: Soam VIP GU: Soam VIP GU: Select each transport and click Enable. Enable Disable Block Soam VIP GU: Re-enable Maintenance Soam VIP GU: Soam VIP GU: Re-enable Soam VIP GU: Re-enable Maintenance Soam VIP GU: Re-enable Maintenance Soam VIP GU: Re-enable Maintenance Soam VIP GU: Re-enable Maintenance Soam VIP GU: Remote Signaling Points Remote MIP3 Users Linksets Linksets Linksets			Connections
 SOAM VIP GUI: Select the optional feature application configured in step 72. Click Enable. Enable Pause updates 66. SOAM VIP GUI: Re-enable transport Manager Maintenance > Transport. Maintenance Maintenance Select each transport and click Enable. 67. SOAM VIP GUI: Navigate to SS7/Sigtran Maintenance SS7/Sigtran SS7/Sigtran SS7/Sigtran SS7/Sigtran SS7/Sigtran SS7/Sigtran SS7/Sigtran SS7/Sigtran Maintenance SS7/Sigtran SS7/Sigtran			🔤 🔯 Egress Throttle Groups
 2. Select the optional feature application configured in step 72. 3. Click Enable. Enable Disable Pause updates 66. SOAM VIP GUI: Re-enable transports, if needed. DSR only. If SDS, then skip to step 69. 67. SOAM VIP GUI: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 69. 67. SOAM VIP GUI: Re-enable MAPIWF A Verify the Operational Status for each transport is Up. 67. SOAM VIP GUI: Navigate to SS7/Sigtran > Maintenance > Local SCCP Users. Re-enable MAPIWF Application, if needed. DSR only. If SDS, then skip to step 69. 67. SOAM VIP GUI: Navigate to SS7/Sigtran > Maintenance > Local SCCP Users. Re-enable MAPIWF Application, if needed. DSR only. If SDS, then skip to step 69. Configuration Remote MITP3 Users Links 45 Links 45 Links 45 Links 45 Verify the SSN Status is Enabled. 			Applications
66. SOAM VIP GUI: Re-enable 1. Navigate to Transport Manager > Maintenance > Transport. 7. Re-enable Image: Configuration image: Configu			2. Select the optional feature application configured in step 72.
60. SOAM VIP GUI: Re-enable inansports, if needed. DSR only. If SDS, then skip to step 69. 1. Navigate to Transport Manager > Maintenance > Transport. Configuration 67. SOAM VIP GUI: NAPIWF application, if needed. DSR only. If SDS, then skip to step 69. 1. Navigate to ST/Sigtran > Maintenance Inable Disable Block 67. SOAM VIP GUI: NAPIWF equilibrium Skip to step 69. 1. Navigate to ST/Sigtran > Maintenance > Local SCCP Users. 67. SOAM VIP GUI: NAPIWF equilibrium Skip to step 69. 1. Navigate to ST/Sigtran > Maintenance > Local SCCP Users. 67. SOAM VIP GUI: NAPIWF equilibrium Skip to step 69. 1. Navigate to ST/Sigtran > Maintenance > Local SCCP Users. 67. SOAM VIP GUI: NAPIWF equilibrium Skip to step 69. 1. Navigate to ST/Sigtran > Maintenance > Local SCCP Users. 69. Configuration Preceded. DSR only. If SDS, then skip to step 69. 2. Click the Enable button corresponding to MAPIWF Application Name. 69. Linksets Links 2. Click the Enable button corresponding to MAPIWF Application Name.			3. Click Enable.
 66. SOAM VIP GUI: Re-enable transports, if needed. DSR only. If SDS, then skip to step 69. 67. SOAM VIP GUI: Re-enable Maintenance 67. SOAM VIP GUI: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 69. 7. SOAM VIP GUI: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 69. 8. Verify the Operational Status for each transport is Up. 1. Navigate to SS7/Sigtran > Maintenance > Local SCCP Users. 6. Configuration Maintenance 6. Configuration 6			Enable Disable Pause updates
 Re-enable transports, if needed. DSR only. If SDS, then skip to step 69. Select each transport and click Enable. Enable Disable Block Verify the Operational Status for each transport is Up. 1. Navigate to SS7/Sigtran > Maintenance > Local SCCP Users. Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 69. Configuration Maintenance Configuration Remote Signaling Points Remote MTP3 Users Linksets Click the Enable button corresponding to MAPIWF Application Name. Enable Disable Verify the SSN Status is Enabled. 	66.	SOAM VIP GUI:	1. Navigate to Transport Manager > Maintenance > Transport.
 analogous, in needed. DSR only. If SDS, then skip to step 69. Select each transport and click Enable. Enable Disable Block Verify the Operational Status for each transport is Up. 67. SOAM VIP GUI: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 69. Navigate to SS7/Sigtran Configuration Configu		Re-enable transports if	🖻 😋 Transport Manager
DSR only. If SDS, then skip to step 69. Maintenance 67. SOAM VIP GUI: Re-enable MAPIWF application, if needed. 1. Navigate to SS7/Sigtran > Maintenance > Local SCCP Users. DSR only. If SDS, then skip to step 69. SOT Configuration Image: Configuration if needed. SSR only. If SDS, then skip to step 69. Image: Configuration if needed. Configuration Image: Configuration Configu		needed.	主 🧰 Configuration
then skip to step 69. Image: Transport 2. Select each transport and click Enable. Enable Disable Block 3. Verify the Operational Status for each transport is Up. 1. Navigate to SS7/Sigtran > Maintenance > Local SCCP Users. 67. SOAM VIP GUI: MAPIWF application, if needed. DSR only. If SDS, then skip to step 69. 1. Navigate to SS7/Sigtran Configuration Maintenance Maintenance > Local SCCP Users Maintenance Image: DSR only. If SDS, then skip to step 69. Image: Configuration Maintenance Image: Configuration Maintenance Image: DSR only. If SDS, then skip to step 69. Image: Configuration Maintenance Image: Configuration Maintenance Image: DSR only. If SDS, then skip to step 69. Image: Configuration Maintenance Image: Configuration Maintenance Image: DSR only. If SDS, then skip to step 69. Image: Configuration Maintenance Image: Configuration Maintenance Image: DSR only. If SDS, then skip to step 69. Image: Configuration Maintenance Image: Configuration Maintenance Image: DSR only. If SDS, then skip to step 69. Image: Configuration Maintenance Image: Configuration Maintenance Image: DSR only. If SDS, then skip to step 69. Image: Configuration Maintenance Image: Configuration Maintenance Image: DSR only. If SDS, then skip to step 69. Image: Configuration Maintenance Image: Configurat		DSR only. If SDS,	🖃 😋 Maintenance
 69. 69. 2. Select each transport and click Enable. Enable Disable Block 3. Verify the Operational Status for each transport is Up. 67. SOAM VIP GUI: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 69. 1. Navigate to SS7/Sigtran > Maintenance > Local SCCP Users. Maintenance Configuration Remote Signaling Points Remote MTP3 Users Linksets Links 2. Click the Enable button corresponding to MAPIWF Application Name. Enable Disable 3. Verify the SSN Status is Enabled. 		then skip to step	Transport
67. SOAM VIP GUI: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 69. 1. Navigate to SS7/Sigtran > Maintenance > Local SCCP Users. Configuration Maintenance DC Configuration Maintenance DSR only. If SDS, then skip to step 69. 69. Cocal SCCP Users Remote Signaling Points 69. Cocal SCCP Users Remote MTP3 Users 61. Links ets Links 2. Click the Enable button corresponding to MAPIWF Application Name. Enable Disable 3. Verify the SSN Status is Enabled.		69.	2. Select each transport and click Enable .
Enable Disable Block 3. Verify the Operational Status for each transport is Up. 3. Verify the Operational Status for each transport is Up. 67. SOAM VIP GUI: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 69. 1. Navigate to SS7/Sigtran > Maintenance > Local SCCP Users Maintenance 9. SST, Sigtran Maintenance 9. Configuration 10. Remote Signaling Points 11. Remote MTP3 Users 12. Linksets 13. Links 2. Click the Enable button corresponding to MAPIWF Application Name. Enable Disable 3. Verify the SSN Status is Enabled.			
 SOAM VIP GUI: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 69. I. Navigate to SS7/Sigtran > Maintenance > Local SCCP Users. Maintenance Configuration Remote Signaling Points Remote MTP3 Users Linksets Linksets Click the Enable button corresponding to MAPIWF Application Name. Enable Disable Verify the SSN Status is Enabled. 			Enable Disable Block
 67. Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 69. 69. 1. Navigate to SS7/Sigtran > Maintenance > Local SCCP Users. Configuration Configuration Local SCCP Users Remote Signaling Points Inks Click the Enable button corresponding to MAPIWF Application Name. Enable Disable Verify the SSN Status is Enabled. 			 Verify the Operational Status for each transport is Up.
 Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 69. Cocal SCCP Users Remote Signaling Points Remote MTP3 Users Linksets Links Click the Enable button corresponding to MAPIWF Application Name. Enable Disable Verify the SSN Status is Enabled. 	67.	SOAM VIP GUI:	1. Navigate to SS7/Sigtran > Maintenance > Local SCCP Users.
MAPIWF application, if needed. DSR only. If SDS, then skip to step 69. 2. Click the Enable button corresponding to MAPIWF Application Name. Enable Disable 3. Verify the SSN Status is Enabled.		Re-enable	
 application, in needed. DSR only. If SDS, then skip to step 69. Generation and the state of the		MAPIWF	
DSR only. If SDS, then skip to step 69.		needed.	
then skip to step 69. Remote Signaling Points Remote MTP3 Users Linksets Links 2. Click the Enable button corresponding to MAPIWF Application Name. Enable Disable 3. Verify the SSN Status is Enabled.		DSR only. If SDS,	
 69. 69. Remote Signaling Points Remote MTP3 Users Linksets Links 2. Click the Enable button corresponding to MAPIWF Application Name. Enable Disable 3. Verify the SSN Status is Enabled. 		then skip to step	Demote Signaling Points
 Linksets Click the Enable button corresponding to MAPIWF Application Name. Enable Disable Verify the SSN Status is Enabled. 		69.	Remote Signaling Folias Remote MTP3 Lisers
 Click the Enable button corresponding to MAPIWF Application Name. Enable Disable Verify the SSN Status is Enabled. 			
 2. Click the Enable button corresponding to MAPIWF Application Name. Enable Disable 3. Verify the SSN Status is Enabled. 			Links
EnableDisable3. Verify the SSN Status is Enabled.			2. Click the Enable button corresponding to MAPIWF Application Name.
3. Verify the SSN Status is Enabled .			Enable Disable

Procedure 2. Recovery Scenario 2

68. □	SOAM VIP GUI: Re-enable links, if needed. DSR only. If SDS, then skip to step 69.	 Navigate to SS7/Sigtran > Maintenance > Links. SS7/Sigtran Configuration Maintenance
		Local SCCP Users Remote Signaling Points Remote MTP3 Users Linksets
		2. Click Enable for each link.
		Enable Disable
		3. Verify the Operational Status for each link is Up .
69.	SOAM VIP GUI:	1. Navigate to Alarms & Events > View Active.
	alarms	🖃 🔄 Alarms & Events
		View Active
		View History
		View Irap Log
		 Examine all active alarms and refer to the on-line help on how to address them.
		If needed, contact My Oracle Support (MOS).
70.		1. Navigate to Alarms & Events > View Active.
	Examine all alarms	🖃 😋 Alarms & Events
		View Active
		View History
		🔛 🖺 View Trap Log
		2. Examine all active alarms and refer to the on-line help on how to address them.
		If needed, contact My Oracle Support (MOS).

Procedure 2. Recovery Scenario 2

Procedure 2. Recovery Scenario 2

 71. NOAM VIP: Verify all servers in topology are accessible (RADIUS only) If the RADIUS key has never been revoked, skip this step. If never configured on any site in the network, the RADIUS key most likely never been revoked. Check with your system adr 1. Establish an SSH session to the NOAM VIP and login as 2. Check if all the servers in the topology are accessible: \$\$\frac{1}{\$\$\$ /usr/TKLC/dpi/bin/\$		 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. Establish an SSH session to the NOAM VIP and login as admusr. 2. Check if all the servers in the topology are accessible: \$ /usr/TKLC/dpi/bin/\$./sharedKrevo -checkAccess
		Example output:
		<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] '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>
		<i>Note:</i> If any server is not accessible, stop and contact My Oracle Support (MOS).
72.	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. Check if existing key file on active NOAM (the NOAM, which is intact and was not recovered) server is valid: \$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -validate
		Example output:

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] Kev file for 'IPFE' is valid
	FIPS integrity verification test failed.
	FIPS integrity verification test failed.
	1450723461: [INFO] Kev 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 above the existing key file is not valid
	in output of above command shows the existing key life is not valid,
	contact my Oracle Support (MOS).
2	. Copy the key file to all the servers in the topology:
	\$./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.
	FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722735: [INFO] Synched key to MP-2 FUPC integrity movid integrity over 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.
	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. FURD integrity representation test failed.
	FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722735: [UNFO] 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. 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. 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. 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. 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. 1450722738: [INFO] Synched key to MP-1 [admusr@NOAM-2 bin]\$
	<pre>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. 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. 1450722738: [INFO] Synched key to MP-1 [admusr@NOAM-2 bin]\$</pre>
	<pre>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. 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. 1450722738: [INFO] Synched key to MP-1 [admusr@NOAM-2 bin]\$</pre>

		<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. 1450203520: [INFO] Updating data on server 'SOAM-2' FIPS integrity verification test failed. 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' Note: If any errors display, stop and contact My Oracle Support (MOS).</pre>
73.	Back up and archive all the databases from the recovered system	Execute Appendix A DSR Database Backup to back up the Configuration databases.
74.	Recover IDIH	If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.

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

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

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

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

• Recover IDIH if necessary

	This procedure performant intact. This includes	orms recovery if ALL NOAM servers are failed but 1 or more SOAM servers are s any SOAM server that is in another location (spare SOAM server).		
S T F	Check off (√) each s step number.	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.		
Р #	If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.			
1.	Gather required materials	Gather the documents and required materials listed in the Required Materials section.		
2.	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.	Replace failed equipment	HW vendor to replace the failed equipment.		
4.	Recover PMAC and PMAC TVOE	 Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]: 		
	Host: Configure BIOS settings and update firmware	HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings		
		 Oracle X5-2/Netra X5-2/X6-2/ X7-2: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings 		
		HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings		
		 Verify and/or upgrade server firmware by executing the Upgrade Rack Mount Server Firmware procedure from reference [8]. 		
5.	PMAC, TVOE Hosts, and	This step assumes TVOE and PMAC backups are available. If backups are NOT available, skip this step .		
	Switch Recovery: Backups available	 Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers. 		
		 Restore the PMAC backup by executing Appendix H Restore PMAC from Backup. 		
		3. Proceed to step 7.		
6.	PMAC, TVOE Hosts, and	This step assumes TVOE and PMAC backups are NOT available. If the TVOE and PMAC have already been restored, skip this step .		
	Switch Recovery: Backups NOT	 Execute the Install and Configure TVOE on First RMS (PMAC Host) procedure from reference [8]. 		
		2. Execute the Install PMAC procedure from reference [8].		
		3. Execute the Initialize the PMAC Application section from reference [8].		

Procedure 3.	Recovery	Scenario 3
--------------	----------	------------

7.	Recovery failed Cisco 4948 aggregation switches (HP DL380 only)	 Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 GEN 9, skip this step. Recover failed Cisco 4948 aggregation switches, if needed: 1. Back up available configuration files. Refer to Appendix C Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only) to recover failed Cisco 4948 aggregation switches. 2. Back up configuration files NOT available. Execute Configure Cisco 4948E-F Aggregation Switches (HP DL 380 Gen 8 Only) section from reference [8].
8.	Configure PMAC (no backup)	If PMAC backup was NOT restored in step 5, execute this step; otherwise skip this step. Execute the Configure PMAC Server (NetBackup Only) and Add RMS to the PMAC Inventory sections from reference [8].
9.	Install/Configure additional rack	 Execute the Install TVOE on Additional Rack Mount Servers procedure from reference [8].
	mount servers	 If backups are available, restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers.
		If backups are NOT available, execute the Configure TVOE on Additional Rack Mount Servers procedure from reference [8].
10.	Configure BIOS settings and update firmware on additional rack mount servers	 Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]: HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings Oracle X5-2/Netra X5-2/X6-2/ X7-2: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings Verify and/or upgrade server firmware by executing the Upgrade Rack Mount Server Firmware procedure from reference [8].
11.	Determine VM	HP DL380 GEN 8, skip this step.
	Placement and Socket Pinning (Oracle X5- 2/Netra X5-2/X6- 2/X7-2/HP DL380 Gen 9 only)	 Determine VM placement and pinning by following: From this document, section 3.1, item 14, to determine the VM placement; and In reference [8], Appendix S VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1 Gbps NICs) and CPU Pinning in HP DL380 Gen 9 (Onboard 1 Gbps NICs) for Pinning Information on HP DL380 Gen 9.
12.	Deploy redundant PMAC, if required	Refer to the Deploy Redundant PMAC (Optional) procedure to re-deploy and configure any redundant PMACs previously configured.

13.	PMAC : Determine if the fdconfig file exists	1. Туре:
		[admusr@melbourne-pmac-1 ~]\$ ll /usr/TKLC/smac/etc/fdc/
	from the initial deployment	 Examine the results and verify if the rms config file <hostname>.cfg exists.</hostname>
		Note: There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS.
14.	Create fdconfig backup file, if it does not already exist	 Execute this step ONLY If the fdconfig backup file does NOT exist. Create the needed file(s) by executing the Virtual Machine/Network Fast Deployment section from reference [8]. WARNING
		It is very important to ensure the file(s) created only affects the TVOE server(s) and the guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.2. Skip to step 23. if this step was executed.
15. 🗌	PMAC : Load ISOs into PMAC, if not done already	If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the Virtual Machine/Network Fast Deployment section from reference [8].
16.	PMAC: Edit/Update configuration file	 Edit the fdconfig file to include only the required/failed servers. <i>Notes</i>: Comment out configuration items that are not needed. Create a separate configuration file for EACH rack mount server being deployed. The Cabinet ID in the config file needs to match the cabinet already defined in PMAC. The following items are mandatory: siteName tpdlso dsrlso (if DSR VMs are being configured) sdslso (if SDS VMs are being configured) NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured) XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured) XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured) DSRNOAM1XMIIPADDRESS (if DSRNOAM1 is being configured) DSRDRNOAM1XMIIPADDRESS (if DSRDRNOAM1 is being configured)

Procedure 3. Recovery Scenario 3

Procedure 3. Recovery Scenario 3

		•	SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured)		
		•	SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured)		
		•	SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured)		
		•	SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured)		
		No	otes:		
•			Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].		
			Comment out SDS and DSR profile items if corresponding products are not used.		
			For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6- 2/X7-2/HP DL380 Gen 9: Refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].		
			VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName.		
		 VM locations should not be changed from their RMSx f should correspond to a separate rack mount server. 			
		WARNING			
		En rec res	sure the file(s) created only affect the TVOE server(s) and guests being covered. Failure to ensure working servers are not included in the file could sult in those servers/guests being taken out of service.		
17.	PMAC: Copy the	Co	py the fdconfig backup file to the RMS directory.		
	backed up fdc file to the RMS directory	\$ /	<pre>sudo cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file> usr/TKLC/smac/etc/RMS/</backup_fdc_file></pre>		

18.	B. PMAC : Execute the config.sh script	Execute config.sh against the modified backup config file.
		Note: If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again.
		<pre>\$ sudo ./config.sh <config file=""></config></pre>
		Example output:
		[admusr@5010441PMAC RMS]\$ sudo ./config.sh rms.cfg
		Validating cfg file
		Added Cabinet 101 to Fast Deployment File.
		Added Zombie_TVOE1 to Fast Deployment File.
		Added Zombie_TVOE2 to Fast Deployment File.
		Added xmi(bond0.4) to Fast Deployment File.
		Added 1m1(bond0.3) to Fast Deployment File.
		Added rep(bondl.f) to fast Deployment File.
		Added x512(bond1.7) to Fast Deployment File.
		Added xsi3(bond1.8) to Fast Deployment File.
		Added xsi4(bond1.9) to Fast Deployment File.
		Added xsi5(bond1.11) to Fast Deployment File.
		Added xsi6(bond1.12) to Fast Deployment File.
		Added xsi8(bond1.14) to Fast Deployment File.
		Added xsi9(bond1.15) to Fast Deployment File.
		Added xsi10(bond1.16) to Fast Deployment File.
		Added xsil1(bond1.17) to Fast Deployment File.
		Added xsi12(bond1.18) to Fast Deployment File.
		Added xsil3(bond1.19) to Fast Deployment File.
		Added xs114(bond1.20) to Fast Deployment File.
		Added xsi16(bond1.22) to Fast Deployment File.
		Added Zombie_DSRNOAM1 to Fast Deployment File.
		Added Zombie_DSRNOAM2 to Fast Deployment File.
		Added Zombie_DSRDRNOAM1 to Fast Deployment File.
		Added Zombie_DSRDRNOAM2 to Fast Deployment File.
		Added Zombie_SDSNOAM1 to Fast Deployment File.
		Added Zombie SDSDRNOAM1 to Fast Deployment File.
		Added Zombie SDSDRNOAM2 to Fast Deployment File.
		Added Zombie_DSRSOAM1 to Fast Deployment File.
		Added Zombie DSRSOAM2 to Fast Deployment File.
		Added Zomble_SDSSOLM1 to Fast Deployment File.
		Added Zombie DSRDAMP1 to Fast Deployment File.
		Added Zombie_DSRDAMP2 to Fast Deployment File.
		Added Zombie_DSRIPFE1 to Fast Deployment File.
		Added Zombie_DSRIPFE2 to Fast Deployment File.
		Added Zombie_SDSDPSV1 to Fast Deployment File.
		Validating Fast Deployment File
		Validate configuration file: "Zombie DSR Fast Deployment 06-15-16.xml"
		Configuration file validation successful.
		Validation complete
		Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml
		admusr@5010441PMAC_RMS1\$

Procedure 3. Recovery Scenario 3

19. □	PMAC : Execute fast deployment	With the file generated from the config.sh script, execute the following command to start fast deployment:							
		\$ screen							
		<pre>\$ sudo fdconfig configfile=<fd_config.xml></fd_config.xml></pre>							
		<i>Note:</i> Th bei scr	is is a long dura fore executing th reen session in t	tion comm ne fdconfig the event c	and. If the so , perform a s of a terminal t	creen co creen - imeout,	omman dr to re etc.	d was r sume t	un he
20.	PMAC GUI:	1. If not a	Iready done, es	tablish a G	UI session o	n the PN	MAC se	erver.	
	Monitor the configuration	2. Naviga	2. Navigate to Task Monitoring .						
	eegerane	🛓 🧰 Sta	atus and Manage						
		— 🖺 Та	sk Monitoring						
		🧼 He	lp						
		💾 Le	gal Notices						
		🔁 Lo	gout						
		3. Monito	r the configuration	on to comp	oletion:				
		Main Menu: Task	Monitoring						
		Filter* •	Torest	Status	Cinta	Task Output	Queeina Timo	Start Time	Ornersee
		925 Accept	RMS: pc5010441 Guest:	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:35	100%
		924 Accept	Zombie_SDSDRNOAM1 RMS: <u>pc5010441</u> Guest:	Success	COMPLETE	N/A	0:01:04	2016-07-11	100%
		923 Accept	Zombie_SDSNOAM1 RMS: pc5010441 Guest: Zombie_DSRIPFE1	Success	COMPLETE	N/A	0:01:06	2018-07-11	100%
		922 Accept	RMS: pc5010439 Guest: Zembie: DSRDAMP2	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%
		921 Accept	RMS: <u>pc5010441</u> Guest: Zombie_DSRDAMP1	Success	COMPLETE	NA	0:01:05	2016-07-11 11:26:43	100%
		920 Accept	RMS: pc5010439 Guest: Zomble_DSRSOAM2	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:42	100%
		Note: If a /va [admusr@me file=deplo Dump Steps Here are t 	failure occurs w m/TKLC/log/fdc lbourne-pmac-1 y_melbourne_201 in file: "depl he steps that w begin steps: Y INFRA ID SVR1 Fast_Deploymer Fast_Deploymer Fast_Deploymer Fast_Deploymer the fdconfig res	with fdconf config/fdco fdconfig] 170329T202 loy_melbou were gener rYPE CMD E nt 0 21 0 nt 0 1 1 1 nt 0 3 mel nt 1 ter a failure start	ig, logs can b onfig.log file. \$ sudo fdcon 458_701b.fdc rne_20170329 ated LEMENT PRE S Complete 300 Skipped 300 bourne_RMS3 e has occurre	fig dum db T202458 TATE TO 0 Chec 0 Add 1 Skipp d and h	ssed in psteps _701b.f BGTS (k PM&C Cabinet ed 900 as been	 Edcdb" COMMAND is : 0 Add n resolv	TEXT Rms /ed:

Procedure 3.	Recovery	Scenario 3
--------------	----------	------------

21.	PMAC : Repeat for each rack mount server configuration file	Repeat steps 1320. for each rack mount server/configuration file, if required.			
22.	PMAC: Back up	1. Copy the updated fdc file to the fdc backup directory:			
	FDC file	<pre>\$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> /usr/TKLC/smac/etc/fdc/</fdc_file></pre>			
		2. Change permissions:			
		<pre>\$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/<fdc_file></fdc_file></pre>			
23.	Perform CPU pinning	Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only) procedure from reference [8].			
24.	Obtain latest database backup	 Obtain the most recent database backup file from external backup sources (for example, file servers) or tape backup sources. 			
	and network configuration data	2. Obtain most recent RADIUS shared secret encryption key from the DpiKf.bin.encr file on external backup sources (only when the RADIUS key revocation MOP has been executed on the system).			
		3. 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.			
25.	Execute DSR	Verify the networking data for network elements.			
	installation procedure for the first NOAM	 Notes Use the backup copy of network configuration data and site surveys from step 2. 			
		• SDS disaster recovery actions can and should be worked simultaneously to allow faster recovery of the complete solution (that is, stale DB on DP servers do not receive updates until SDS-SOAM servers are recovered). The following steps accommodate both DSR and SDS disaster recovery steps.			
		<i>Important</i> : While creating the first NOAMs in this step, it is important that the server hostname is the same as one of the NOAM hostnames used prior to the disaster.			
		1. Configure the first NOAM server by executing the Configure First NOAM NE and Server procedure from reference [8].			
		 Configure the NOAM server group by executing the Configure the NOAM Server Group procedure from reference [8]. 			
		SDS:			
		3. Configure the first SDS NOAM server by executing Configure First SDS NOAM NE and Server procedure from reference [8].			
		4. Configure the SDS NOAM server group by executing the Configure the SDS NOAM Server Group procedure from reference [8].			
		5. Skip to step 31.			

-	······································		
26.	NOAM GUI : Login	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:
	DSR only. If SDS, skip to step 31.		http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>
	If the failed server is not OAM, then skip to step 37.	2.	Login as the guiadmin user:
	Oracle System Login Mon Ju		Oracle System Login Mon Jul 11 13:59:37 2016 EDT
			Image:

Procedure 3. Recovery Scenario 3

27.	NOAM GUI:	1. Navigate to Status & Manage > Files.			
	Upload the backup database file.	🖹 🚔 Status & Manage			
	DSR only. If SDS,	🦳 🙀 Network Elements			
	skip to step 31.	HA REAL REAL REAL REAL REAL REAL REAL REA			
		₩ Database			
		Processes			
		2. Select the active NOAM server.			
		Main Menu: Status & Manage -> Files			
		Filter* ▼ Tasks ▼			
		ZombieNOAM1			
		File Name			
		TKLCConfigData.ZombieNOAM1.sh			
		ugwrap.log			
		upgrade.log			
		3. Click Upload and select the NO Provisioning and Configuration file backed up after initial installation and provisioning.			
		Delete View Upload Download Deploy ISO Validate ISO			
		40 KB used (0.00%) of 15.7 GB available System utilization: 867.9 MB (5.39%) of 15.7 GB available.			
		4. Click Browse and locate the backup file.			
		Note: If there is no backup file, refer to Appendix L Backup Directory to create the backup directory.			
		5. Click Open .			
		6. Mark the This is a backup file checkbox.			
		7. Click Upload.			
		8			
		File: Browse Backup dsr ZombieNOAM1 Configuration NETWORK OAM			
		This is a backup file			
		Upload			
		oprodu			
		Cancel			
		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.			

28.	NOAM GUI: Disable provisioning. DSR only. If SDS, skip to step 31.	 Navigate to Status & Manage > Database.
		Server HA Database KPIs Processes Tasks Files Click Disceble Provisioning
		Disable Provisioning Report Inhibit/Allow
		 Click OK to disable Provisioning. Disable provisioning. Are you sure?
		OK Cancel

Procedure 3. Recovery Scenario 3

29.	NOAM GUI: Verify the archive	1. Se	lect the	active NO	AM server and click Compare .		
	contents and database	lication	Backup	Compare	Restore		
	compatibility. DSR only. If SDS, skip to step 31.	2. Cli 27 Datab	ck the bu . of this p ase Comp	utton for th procedure. are	e restored database file uploaded as a part of step		
		Select a	rchive to com	ipare on server:	ZombieNOAM1		
		Archive *	e 🔘 backup/	Backup.dsr.Zom	bieNOAM1.Configuratio		
		Ok	Ok Cancel				
		3. Ve	rify the	output win	dow matches the screen below.		
		Note:	A datal possibl warnin otherw assista	base mism y User cor gs are exp ise, stop a nce.	atch regarding the Topology Compatibility and npatibility (due to authentication) display. These ected. If these are the only mismatches, proceed; nd contact My Oracle Support (MOS) to ask for		
		Databas	e Archive C	ompare			
		The sel	ected datab	ase came from	ZombieNOAM1 on 10/10/2016 at 10:36:44 EDT and contains the follow		
		Archive Configu	Contents ration data	L			
		Databas The dat	e Compatibi abases are	<u>lity</u> compatible.			
		Node Typ The node Topology THE TOP	pe Compatik e types are	compatible.			
			y Compatibi OLOGY IS NO	<u>lity</u> T COMPATIBLE.	CONTACT ORACLE CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE.		
		Discre - Serv - Serv - Serv - Serv - Serv	pancies: ver A1860.03 ver A1860.03 ver A0630.23 ver B2934.03 ver C0422.20	2 on network 2 on network 38 on network 11 on network 00 on network	XMI is in the current topology but not the selected backup file. IMI is in the current topology but not the selected backup file. XMI is in the selected backup file but not the current topology. XMI is in the selected backup file but not the current topology. XMI is in the selected backup file but not the current topology.		
		Note:	Archive	e Contents	and Database Compatibilities must be the following:		
			Archiv	e Content	s: Configuration data.		
			Databa	ase Comp	atibility: The databases are compatible.		
		Note:	The fol since v databa	lowing is e ve are rest se with jus	expected output for Topology Compatibility Check oring from an existing backed up database to a st one NOAM:		
			Topolo	ogy Comp	atibility		
			The top	ology sho	uld be compatible minus the NODEID.		
		Note:	We are databa	e trying to r se. This is	estore a backed up database onto an empty NOAM an expected text in Topology Compatibility.		
		4. If t this	he verific s proced	cation is su ure.	accessful, click Back and continue to next step in		

Procedure 3. Recovery	Scenario 3
-----------------------	------------

30.	Active NOAM:	1. From Status & Manage > Database.					
	Restore the database.	2. Select the active NOAM server and click Restore .					
	DSR only. If SDS, skip to step 31.	are Restore Man Ar					
		3. Select the proper backup provisioning and configuration file.					
		Select archive to Restore on server: Zombin					
		Archive *					
		Ok Cancel					
		4. Click OK .					
		5. 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.					
		Database Restore Confirm					
		Incompatible archive selected					
		The selected database came from ZombieNOA					
		Archive Contents Configuration data					
		Database Compatibility The databases are compatible.					
		Confirm archive "backup/Backup.dsr.ZombieNOAM1.Configurat					
		Force Restore? Vertication Force Force restore					
		Ok Cancel					
	Note: After the restore has started, the user is logged out of th GUI since the restored topology is old data.						
		6. Go to step 37.					

Procedure	3.	Recovery	/ Scenario 3
-----------	----	----------	--------------

31.	SDS NOAM: Transfer SDS configuration and provisioning backup database files. SDS only. If DSR, skip to step 37.	<pre>Jsing the IP of the recovered SDS NOAM, transfer the uncompressed ackup database files to the /var/TKLC/db/filemgmt directory. .inux: . From the command line of a Linux machine, copy the configuration backup file to the SDS NOAM guest:</pre>		
32.	SDS NOAM:	Establish an SSH session to the SDS active NOAM XMI IP address and login		
	Login.	as admusr .		
	SDS only. If DSR, skip to step 37.			
33. □	SDS NOAM: Stop running	Issue the following command to stop running applications. Leave database running:		
	applications.	\$ sudo prod.stopignore-cap		
skip to step 37.		<i>Note:</i> This step may take several minutes to complete.		
34.	SDS NOAM:	Restore the configuration DB by executing the following command:		
Restore configuration		<pre>\$ sudo idb.restore -n -t /var/TKLC/db/filemgmt -v <full archive="" configuration="" file="" name="" path="" to=""></full></pre>		
	SDS only. If DSR, skip to step 37.			
35.	SDS NOAM: Restore provisioning database. SDS only. If DSR, skip to step 37.	Refer to Appendix I Restore Provisioning Database to restore the provisioning database.		
36.	SDS NOAM: Start	Start the SDS application by executing the following command:		
	running	\$ sudo prod.start		
	SDS only. If DSR, skip to step 37.			

37. □	NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:		
		http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>		
		2. Login as the guiadmin user:		
		Oracle System Login		
		Mon Jul 11 13:59:37 2016 EDT		
		Log In Enter your username and password to log in Username: Password: Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.		
38.	NOAM VIP GUI:	1. Wait for 5-10 minutes for the system to stabilize with the new topology:		
	Monitor and confirm database restore	2. Monitor the Info tab for Success . This indicates the restore is complete and the system is stabilized.		
		Ignore these alarms for NOAM and MP servers until all the servers are configured:		
		 Alarms with Type Column as REPL, COLL, HA (with mate NOAM), DB (about Provisioning Manually Disabled). 		
		Notes:		
		 Do not pay attention to alarms until all the servers in the system are completely restored. 		
		• The Configuration and Maintenance information is in the same state it was when backed up during initial backup.		

Procedure 3. Recovery Scenario 3

39.	Active NOAM: Set failed servers to OOS	 Navigate to Status Set the Ma Modifying HA 	Status & Manage & Manage work Elements over atabase Pls occesses x Allowed HA Ro	ge > HA.	DS for the failed servers.
		Hostnamo	Max Allowed HA Polo	Description	
		Hostname	Max Allowed HA Role	Description	
		ZombieNOAM1	Active 💌	The maximum des	
		ZombieNOAM2	OOS	The maximum des	
		ZombieDRNOAM1	Standby Spare Observer	The maximum des	
		4. Click OK. Ok Can	cel		
40. 	NOAM VIP GUI: Recover standby NOAM	Install the seco DSR:	nd NOAM server	:	
		Execute the Co from reference SDS:	>nfigure the Sec [8].	ond NOAM Se	<pre>>rver procedure, steps 1, 3-6,</pre>
		Execute the Co 3-6, from refere	onfigure the Sec ence [8].	ond SDS NO	AM Server procedure, steps 1,
41.	Install NetBackup client (optional)	If NetBackup is procedure from	s used, execute the second s	ne Install NetE	ackup Client (Optional)

Procedure 3. Recovery Scenario 3

12		1 Navigate to Status & Manage > HA				
4 ∠ .	Set HA on standby	T. Navigale to Status & Manage > TA.				
	NOAM	🖃 🤤 Status & Manage				
		Network Elements				
		Database				
		KPIs KPIs				
		🔤 🛐 Processes				
		🛨 🧰 Tasks				
		3. Select the standby NOAM server and set it to Active .				
		Modifying HA attributes				
		Hostname Max Allowed HA Role Description				
		ZombieNOAM1 Active The maximum				
		Active				
		Standby Searce The maximum				
		4. Click OK .				
43. NOAM VIP GUI: 1. Navigate to Status & Manage > 3	1. Navigate to Status & Manage > Server.					
	Restart DSR application	Status & Manage				
		Network Elements				
		Server				
		HA				
		Database				
	- 🕅 KPIs					
		Processes				
		🗈 🧰 Tasks				
		En Files				
		2. Select the recovered standby NOAM server and click Restart .				
		op Restart Rebo				

44.	Active NOAM:	1. Establish an SSH session to the active NOAM and login as admusr .
	recognized	2. Execute this command:
	authority table	<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></dsr_noam_a_hostname></dsr_noam_b_hostname></pre>
45.	NOAM VIP GUI: Perform Keyexchange with remote import server. SDS only. If DSR, skip to step 47.	 1. Navigate to SDS > Configuration > Options. SDS Configuration Options Connections NAI Hosts Destinations Destination Map 2. Unmark the Remote Import Enabled checkbox
		Remote Import Enabled Whether or not import files are if DEFAULT = UNCHECKED 3. Click Apply. Note: Navigate to SDS > Configuration > Options again to clear the banner. 4. Enter the Remote Import Password. Remote Import Host IP Address 10.250.53.25 Remote Import User systest
		Remote Import Password
		 5. Click Apply. Remote Import Enabled Note: Navigate to SDS > Configuration > Options again to clear the banner. 6. Mark the Remote Import Enabled checkbox. Remote Import Enabled

Procedure 3. Recovery Scenario 3

46.	NOAM VIP GUI: Repeat for remote export server. SDS only. If DSR, skip to step 47.	Repeat step 45. for the remote export server.
47.	NOAM VIP GUI: Perform Keyexchange with export server	 Navigate to Administration > Remote Servers > Data Export. Administration General Options Access Control Software Management Remote Servers LDAP Authentication SNMP Trapping Data Export DNS Configuration Click SSH Key Exchange. SSH Key Exchange Transfe Type the Password and click OK. SSH Key Exchange GK Cancel
48. □	NOAM VIP GUI: Recover query servers. SDS only. If DSR, skip to step 51.	Execute the Configuring SDS Query Servers procedure, steps 1, 4-7, from reference [8].
Procedure 3. Recovery Scenario 3

40				
49.	GUI: Set HA on	1. Navigate to Status & Manage > HA.		
	query server.	🖻 😋 Status & Manage		
	SDS only. If DSR,	Network Elements		
	skip to step 51.	Server Server		
		HA HA		
		Database		
		KPIs		
		🛨 🧰 Tasks		
		Files		
		2. Click Edit .		
		3. Select the query server and select Observer .		
		ZombieQS1 Observer 💌 The		
		Observer		
		OOS		
		4. Click OK .		
50	SDS NOAM VIP	1 Navigate to Status & Manage > Server		
□	GUI: Restart SDS			
	application.			
	SDS only. If DSR,	Network Elements		
	skip to step 51.	Server 💓		
		- State HA		
		Database		
		KPIS		
		Processes		
		2. Select the recovered query server and click Restart .		
		op Restart Reboo		
51.	NOAM VIP GUI:	DSR:		
	Recover the remaining SOAM	Execute the Configure the SOAM Servers procedure, steps 1-3 and 5-9, from reference [8].		
	servers (standby, spare)	<i>Note:</i> If you are using NetBackup, also execute step 12.		
	. ,	SDS:		
		Execute the Configure the SDS DP SOAM Servers procedure, steps 1-3		
		and 5-8, from reference [8].		

Procedure 3. Recovery Scenario 3



54.	NOAM VIP GUI:	1. Navigate to Status & Manage > Server.	
	Restart DSR application	 Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered SOAM server and click Restart. 	
55.	Activate PCA feature. DSR only. If SDS, skip this step.	If you have PCA installed in the system being recovered, re-activate PCA by executing the PCA Activation on Active NOAM Network procedure on the recovered active NOAM server and the PCA Activation on Stand By SOAM Network procedure on the recovered standby SOAM from reference [7].	
56.	NOAM VIP GUI: Recover the C- level servers (DA- MPs, SBRs, IPFE, SS7-MP, and SDS DPs	 DSR: Execute the Configure the MP Servers procedure, steps 1 and 9-13, from reference [8]. Note: Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. SDS: Execute the Configure the SDS DP Servers procedure, steps 1 and 5-8, from reference [8], Repeat this step for any remaining failed MP servers. 	

Procedure 3. Recovery Scenario 3

57.	NOAM VIP GUI:	1. Navigate to Status & Manage > HA.				
Set HA on all C-						
		Network Elements				
		Server				
		HA				
			abase			
		- Star	cesses			
		2. Click Edit.				
		3. For each server whose Max Allowed HA Role is set to OOS, set it to Active .				
		ZombieDAMP1	Active	The maximum desired HA Role for ZombieDAMI		
		ZombieDAMP2	Standby Spare Observer OOS	The maximum desired HA Role for ZombieDAMI		
		4. Click OK.				
58.	NOAM VIP GUI: Restart DSR application on recovered C-level servers	1. Navigate to	Status & Manage :	> Server.		
		📄 🔄 Status	& Manage			
		Network Elements				
		Se 🔂	rver			
		M HA				
		KPIs				
		📄 🕅 Pro	ocesses			
		2. Select the recovered C-level servers and click Restart .				
		a Destad	Daha			
		p Restart	RedC			
59.	Active NOAM:	1. Establish ar	n SSH session to the	e active NOAM, login as admusr .		
	Perform keyexchange between the active-NOAM and recovered servers	2. Perform a k	eyexchange from th	e active NOAM to each recovered server:		
		\$ keyexchar	nge admusr@ <rec< td=""><td>overed Server Hostname></td></rec<>	overed Server Hostname>		
		Note: If an ex	port server is config	ured, perform this step.		

60.	Active NOAM: Activate optional features. DSR only. If SDS, then skip to next step.	Establish an SSH session to the active NOAM and login as admusr.
		Note for PCA Feature Activation:
		If you have PCA installed in the system being recovered, re-activate the PCA by executing the PCA Activation on Active NOAM Server procedure on recovered active NOAM server and the PCA Activation on Standby SOAM Server procedure on the recovered standby SOAM server from [6].
		Notes:
		 If not all SOAM sites are recovered at this point, then repeat the activation for each "new" SOAM site that comes online.
		 If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature.
		Refer to section 1.5 Optional Features to activate any features that were previously activated.
		<i>Note:</i> While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored:
		iload#31000{S/W Fault}

Procedure	3. Recovery	Scenario 3
-----------	-------------	------------

	1 Novigate to Status & Manage > Database
\Box Fetch and store	1. Navigate to Status & Manage > Database.
the database	📄 😋 Status & Manage
report for the	🟹 Network Elements
newly restored	Server
data and save it	HA 🔂
	Database
	KPIs
	R Processes
	2. Select the active NOAM server and click Report .
	oning Report Inhit
	The following screen displays:
	Main Menu: Status & Manage -> Database [Report]
	der Database Status Report
	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 3. Recovery Scenario 3

62.	Active NOAM: Verify replication between servers	1. Log into the active NOAM as admusr using SSH terminal.			
		2. Execute this command:			
		\$ sudo irepstat -m			
		Example output:			
		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 Oanu-NOAM-I ACTIVE 0 0.25 1%R 0.04%Cpu 61B/S			
		AB 10 Oahu -SOAM-2 ACCIVE 0 0.50 16K 0.05% Cpu /5B/S			
		BB From Oabu-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			

63.	NOAM VIP GUI:	1. Navigate to Status & Manager > Database.				
	Verify the database states	 Status & Manage Network Elements Server HA Database KPIs Processes Verify the OAM Max HA Role is either Active or Standby for NC SOAM; Application Max HA Role for MPs is Active; and status i Normal: 		or NOAM and atus is		
		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	ZombielPFE1		MP	Active
		ZombieSOAM	ZombielPFE2		MP	Active
64.	NOAM VIP GUI: Verify the HA status	 Navigate to Status Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the row for al Verify the HA Role i 	and Manag Il of the serv is either Act	e > HA. ers. ive or Standl	Dy.	
		Hostname		OAM HA Role	Application HA	Max Allowed HA
		7			Role	Role
		ZombieNOAM1		Active	N/A	Active
		ZombieNOAM2		Standby	N/A	Active
		ZombieDRNOAM1		Active	N/A	Active
		ZombieDRNOAM2		Standby	N/A	Active
		ZombieSOAM1		Active	N/A	Active
		ZombieSOAM2		Standby	N/A	Standby

Procedure 3. Recovery Scenario 3

65		1 Navigate to Status & Manage > Database
	Enable	Status & Manage
	provisioning	Network Elements
		Server Server
		🕅 HA
		💽 Database
		KPIs KPIs
		Processes
		Iasks Iasks Iasks
		2 Click Enable Provisioning
		Enable Provisioning Report Inhibit/
		3. Click OK .
66.	SOAM GUI:	1. Navigate to Status & Manage > Database.
	provisioning.	🖻 😋 Status & Manage
	DSR only. If SDS,	Network Elements
	then skip to step	Server
	75.	
		Tasks
		Files
		2. Click Enable Site Provisioning.
		Enable Site Provisioning Report Inhibit/Allo
		3 Click OK
67		1 Navigate to Diameter > Configuration > Peer Node
□	Verify the peer node information.	
	DSR only. If SDS, then skip to step	Capacity Summary
	75.	Connection Capacity E
		CEX Parameters
		Command Codes
		⊡ Configuration Sets ☐
		Local Nodes
		2 Verify all the peer pedec are shown
		2. venity all the peer houses are shown.

	-		
68.	SOAM VIP GUI: Verify the connections information. DSR only. If SDS, then skip to step 75.	 1. Navigate to Diameter > Configuration > Connections. Diameter Configuration Capacity Summary Connection Capacity Dash Application Ids CEX Parameters Command Codes Configuration Sets Configuration Sets Local Nodes Peer Nodes Peer Node Groups Connections 2. Verify all the connections are shown. 	
69. □	MP Servers: Disable SCTP Auth Flag (DSR only). DSR only. If SDS, then skip to step 75.	For SCTP connections without DTLS enabled, refer to the Enable/Disable DTLS (SCTP Diameter Connections Only) section in reference [8]. Execute this procedure on all failed MP servers.	
70.	SOAM VIP GUI: Enable connections, if needed. DSR only. If SDS, then skip to step 75.	 Navigate to Diameter > Maintenance > Connections. Maintenance Route Lists Route Groups Peer Nodes Connections Connections Select each connection and click Enable. Alternatively, enable all the connections by clicking EnableAll. EnableAll Disable I 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 	

	,	
71.	SOAM VIP GUI: Enable optional features. DSR only. If SDS, then skip to step 75.	 Navigate to Diameter > Maintenance > Applications. Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups Applications Select the optional feature application configured in step 60. Click Enable.
72.	SOAM VIP GUI: Re-enable transports, if needed. DSR only. If SDS, then skip to step 75.	 Navigate to Transport Manager > Maintenance > Transport. Transport Manager Configuration Maintenance Transport Select each transport and click Enable. Enable Disable Block Verify the Operational Status for each transport is Up.
73.	SOAM VIP GUI: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 75.	 Navigate to SS7/Sigtran > Maintenance > Local SCCP Users. SS7/Sigtran Configuration Maintenance Local SCCP Users Remote Signaling Points Remote MTP3 Users Linksets Links Click the Enable button corresponding to MAPIWF Application Name. Enable Disable Verify the SSN Status is Enabled.

74.	SOAM VIP GUI: Re-enable links, if needed. DSR only. If SDS, then skip to step 75.	 Navigate to SS7/Sigtran > Maintenance > Links. SS7/Sigtran Configuration Maintenance Local SCCP Users Remote Signaling Points Remote MTP3 Users Linksets Links 2. Click Enable for each link. Enable Disable 3. Verify the Operational Status for each link is Up.
75.	NOAM VIP: Verify all servers in topology are accessible (RADIUS only)	<pre>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. Establish an SSH session to the NOAM VIP and login as admusr. 2. Check if all the servers in the topology are accessible:</pre>

76.	SOAM 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. 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>
		Note: If output of above command shows that existing key file is not valid, contact My Oracle Support (MOS).
		4. Establish an SSH session to the active NOAM, login as admusr .
		5. Copy the key file to active NOAM:
		<pre>\$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -copyKey -destServer <active name="" noam="" server=""></active></pre>

77.	NOAM VIP : Copy key file to all the servers in	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:
	topology (RADIUS	\$ cd /usr/TKLC/dpi/bin/
	oniy)	<pre>\$./sharedKrevo -synchronize</pre>
		Example output:
		<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] 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. FIPS integrity verification test failed.</pre>
		1450203506: [INFO] Key file on Active NOAM and SOAM-2 are same. 1450203506: [INFO] NO NEED to sync key file to SOAM-2. FIDS integrity worification test failed
		\$./sharedKrevo -updateData
		Example output:
		<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>
78.	SOAM VIP GUI:	1. Navigate to Alarms & Events > View Active.
	Examine all alarms	 Alarms & Events View Active View History View Trap Log 2. Examine all active alarms and refer to the on-line help on how to address them. If needed, contact My Oracle Support (MOS).

Procedure 3. Recovery Scenario 3

	-	
79.		1. Navigate to Alarms & Events > View Active.
	alarms	😑 😋 Alarms & Events
		View Active
		View History
		View Trap Log
		2. Examine all active alarms and refer to the on-line help on how to address them.
		If needed, contact My Oracle Support (MOS).
80.	Back up and archive all the databases from the recovered system	Execute the DSR Database Backup procedure to back up the configuration databases.
81. □	Recover IDIH, if configured	If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.
82.	SNMP workaround	Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases:
		1. If SNMP is not configured in DSR/SDS.
		 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
- Recover Query Server (if needed) by recovering base hardware and software.
 - Recover the base hardware.
 - Recover the software.
- Recover Standby SOAM server by recovering base hardware and software.
 - Recover the base hardware.
 - Recover the software.
- Recover MP/DP C-level servers by recovering base hardware and software.
 - Recover the base hardware.
 - Recover the software.

• Recover IDIH if necessary

	This procedure perfo server is intact and a	rms recovery if at least one NOAM server is intact and available and 1 SOAM vailable.				
S T	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.					
 P If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for # 						
1.	Workarounds	 Refer to Appendix L Backup Directory to look for a backup directory and sreate a directory if one does not exist. Refer to Appendix K SNMP Configuration to configure SNMP as a vorkaround in these cases: If SNMP is not configured in DSR. If SNMP is already configured and SNMPv3 is selected as enabled version. 				
2.	Gather required materials	Sather the documents and required materials listed in Required Materials.				
3.	Replace failed equipment	Work with the hardware vendor to replace the failed equipment.				
4.	NOAM VIP GUI: Login	 Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: http://<primary_noam_vip_ip_address></primary_noam_vip_ip_address> Login as the guiadmin user: CORCACLEC° Oracle System Login 				
		Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.				

Procedure 4. Recovery Scenario 4

5.	Active NOAM: Set failed servers to OOS	 Navigate to Status & Manage > HA. Status & Manage Network Elements Server HA Database KPIs 				
			cesses			
		2. Click Edit.		option to OOS f	or the folled convers	
		Modifying HA	attributes			
		Hostname	Max Allowed HA Role	Description		
		ZombieNOAM1	Active 💌	The maximum des		
		ZombieNOAM2	OOS	The maximum des		
		ZombieDRNOAM1	Standby Spare Observer	The maximum des		
		4. Click OK .				
		Ok Cance	ł			
6.	Recover PMAC and PMAC TVOE Host: Configure	 Configure and verify the BIOS/NEB settings by executing the following procedures from reference [8]: 				
	BIOS settings and	HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings				
	upuale infliware	 Oracle X5-2/Netra X5-2/X6-2/X7-2: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings 				
		• HP DL38	30 Gen9: Configu	ure HP Gen9 Sei	rver BIOS Settings	
		2. Verify and/or Mount Serve	[.] upgrade server fi er Firmware proc	irmware by exec edure from refer	uting the Upgrade Rack rence [8].	

-					
7. Recover PMAC, TVOE Hosts, and		If the PMAC is located on the failed rack mount server, execute this step; otherwise skip to step 10.			
	Switch : Backups available	This step assumes TVOE and PMAC backups are available. If backups are NOT available, skip this step .			
		 Restore the TVOE backup by executing Appendix G Restore TVOE Configuration from Backup Media on ALL failed rack mount servers. 			
		 Restore the PMAC backup by executing Appendix H Restore PMAC from Backup. 			
		3. Proceed to step 9.			
8.	Recover PMAC, TVOE Hosts, and	If the PMAC is located on the failed rack mount server, execute this step; otherwise skip to step 10.			
	Switch: Backups NOT available	This step assumes TVOE and PMAC backups are NOT available. If the TVOE and PMAC have already been restored, skip this step .			
		Execute these procedures from reference [8]:			
		Install and Configure TVOE on First RMS (PMAC Host)			
		Install PMAC			
		Initialize the PMAC Application			
9.	Configure PMAC (no backup)	If PMAC backup was NOT restored in step 7. , execute this step; otherwise, skip this step.			
		Execute these procedures from reference [8]:			
		Configure PMAC Server (NetBackup Only)			
		Add RMS to the PMAC Inventory			
10. □	Install/Configure additional rack mount servers	<i>Note:</i> If TVOE backups are available, refer Appendix G Restore TVOE Configuration from Backup Media; otherwise, execute this step.			
		If TVOE backups were NOT performed on any additional rack mount servers or are not available, execute this step; otherwise, skip this step.			
		1. Execute these procedures from reference [8]:			
		Install TVOE on Additional Rack Mount Servers			
		Configure TVOE on Additional Rack Mount Servers			
		 Configure and verify the BIOS/NEB settings by executing these procedures from reference [8]: 			
		HP DL380 Gen8: Configure HP Gen 8 Server BIOS Settings			
		 Oracle X5-2/Netra X5-2/X6-2/X7-2: Configure Oracle X5-2/Netra X5-2/X6-2/ X7-2 Server BIOS Settings 			
		HP DL380 Gen9: Configure HP Gen9 Server BIOS Settings			
		3. Verify and/or upgrade server firmware by executing the Upgrade Rack Mount Server Firmware procedure from reference [8].			

11.	Determine VM placement and socket pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 only)	HP DL380 GEN 8, skip this step . Determine VM placement and pinning by following section 3.1, item 14.			
12. □	Deploy redundant PMAC, if required	Refer to the Deploy Redundant PMAC (Optional) procedure to re-deploy and configure any redundant PMACs previously configured.			
13.	PMAC : Determine if the fdconfig file exists from the initial deployment	 Type: <pre>[admusr@melbourne-pmac-1 ~]\$ l1 /usr/TKLC/smac/etc/fdc/</pre> Examine the results and verify if the rms config file <hostname>.cfg exists. </hostname> Note: There may be multiple fdconfig backup files for each RMS. Select the respective one according to the RMS. <pre>3. Skip to step 15.</pre> 			
14.	Create fdconfig backup file, if it does not already exist	Execute this step ONLY If the fdconfig backup file does NOT exist. Create the needed file(s) by executing the Virtual Machine/Network Fast Deployment section from reference [8]. WARNING It is very important to ensure the file(s) created only affects the TVOE server(s) and the guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service			
15. 	PMAC : Load ISOs into PMAC, if not done already	If DSR, SDS, and TPD ISOs are NOT loaded into PMAC, execute procedure 14 in the Virtual Machine/Network Fast Deployment section from reference [8].			
16.	PMAC: Edit/Update configuration file	 Edit the fdconfig file to include only the required/failed servers. Notes: Comment out configuration items that are not needed. Create a separate configuration file for EACH rack mount server being deployed. The Cabinet ID in the config file needs to match the cabinet already defined in PMAC. The following items are mandatory: siteName tpdlso dsrlso (if DSR VMs are being configured) sdslso (if SDS VMs are being configured) NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured) 			

		XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured)
		• XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured)
		DSRNOAM1XMIIPADDRESS (if DSRNOAM1 is being configured)
		DSRNOAM2XMIIPADDRESS (if DSRNOAM2 is being configured)
		DSRDRNOAM1XMIIPADDRESS (if DSRDRNOAM1 is being configured)
		DSRDRNOAM2XMIIPADDRESS (if DSRDRNOAM2 is being configured)
		SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured)
		SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured)
		SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured)
		SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured)
		Notes:
		 Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].
		 Comment out SDS and DSR profile items if corresponding products are not used.
		• For Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6- 2/X7-2/HP DL380 Gen 9, refer to Appendix Q.3 Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file from reference [8].
		 VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName.
		• VM locations should not be changed from their RMSx format. Each RMS should correspond to a separate rack mount server.
		WARNING
		Ensure the file(s) created only affect the TVOE server(s) and guests being recovered. Failure to ensure working servers are not included in the file could result in those servers/guests being taken out of service.
17.	PMAC: Copy the	Copy the fdconfig backup file to the RMS directory.
	backed up fdc file to the RMS directory	<pre>\$ sudo cp /usr/TKLC/smac/etc/fdc/<backup_fdc_file> /usr/TKLC/smac/etc/RMS/</backup_fdc_file></pre>
1		

18.	PMAC: Execute	Execute config.sh against the modified backup config file.								
	the config.sh script	<pre>xecute config.sh against the modified backup config file. /ote: If the below command is executed on multiple cfg files, it overwrites the existing xml file. Rename the xml file before running the command again. \$ sudo ./config.sh <config file=""> xample output: atmusz@SolO441PMAC RMS]\$ sudo ./config.sh rms.cfg Validating cfg file Successful validation of cfg file. Added Zombie_TVC21 to Fast Deployment File. Added Zombie_TVC21 to Fast Deployment File. Added Zombie_TVC21 to Fast Deployment File. Added imi (bond0.4) to Fast Deployment File. Added imi (bond0.4) to Fast Deployment File. Added imi (bond0.4) to Fast Deployment File. Added xsi1 (bond1.6) to Fast Deployment File. Added xsi2 (bond1.7) to Fast Deployment File. Added xsi3 (bond1.6) to Fast Deployment File. Added xsi3 (bond1.1) to Fast Deployment File. Added xsi4 (bond1.1) to Fast Deployment File. Added xsi12 (bond1.1) to Fast Deployment File. Added xsi14 (bond1.2) to Fast Deployment File. Added zsi16 (bond1.2) to Fast Deployment File. Added zsi16 (bond1.2) to Fast Deployment File. Added zsi16 (bond1.2) to Fast Deployment File. Added zombie_DSRNOAM2 to Fast Deployment File. Added Zo</config></pre>								
		<pre>\$ sudo ./config.sh <config file=""></config></pre>								
		Example output:								
		[admusr@5010441PMAC RMS]\$ sudo ./config.sh rms.cfg								
		Validating cfg file								
		Successful validation of cfg file.								
		Added Cabinet for to fast Deployment file.								
		Added Zombie_TVOE2 to Fast Deployment File.								
		Added xmi(bond0.4) to Fast Deployment File.								
		Added imi(bond0.3) to Fast Deployment File.								
		Added rep(bond1.10) to Fast Deployment File.								
		Added xsi2 (bond1.7) to Fast Deployment File.								
		Added xsi3(bond1.8) to Fast Deployment File.								
		Added xsi4(bond1.9) to Fast Deployment File.								
		Added xsi5(bond1.11) to Fast Deployment File.								
		Added xsi7(bond1.13) to Fast Deployment File.								
		Added xsi8(bond1.14) to Fast Deployment File.								
		Added xsi9(bond1.15) to Fast Deployment File.								
		Added xsill(bond1.16) to fast Deployment File.								
		Added xsill(bond1.17) to Fast Deployment File.								
		Added xsi13(bond1.19) to Fast Deployment File.								
		Added xsi10(bond1.16) to Fast Deployment File. Added xsi11(bond1.17) to Fast Deployment File. Added xsi12(bond1.18) to Fast Deployment File. Added xsi13(bond1.19) to Fast Deployment File. Added xsi14(bond1.20) to Fast Deployment File. Added xsi15(bond1.21) to Fast Deployment File.								
		Added Zombie_TVOE1 to Fast Deployment File. Added Zombie_TVOE2 to Fast Deployment File. Added xmi(bond0.4) to Fast Deployment File. Added imi(bond0.3) to Fast Deployment File. Added rep(bond1.10) to Fast Deployment File. Added xsi2(bond1.7) to Fast Deployment File. Added xsi2(bond1.7) to Fast Deployment File. Added xsi3(bond1.8) to Fast Deployment File. Added xsi4(bond1.9) to Fast Deployment File. Added xsi5(bond1.11) to Fast Deployment File. Added xsi6(bond1.12) to Fast Deployment File. Added xsi6(bond1.12) to Fast Deployment File. Added xsi6(bond1.13) to Fast Deployment File. Added xsi6(bond1.14) to Fast Deployment File. Added xsi9(bond1.15) to Fast Deployment File. Added xsi9(bond1.16) to Fast Deployment File. Added xsi10(bond1.16) to Fast Deployment File. Added xsi10(bond1.17) to Fast Deployment File. Added xsi11(bond1.16) to Fast Deployment File. Added xsi11(bond1.17) to Fast Deployment File. Added xsi11(bond1.12) to Fast Deployment File. Added xsi11(bond1.20) to Fast Deployment File. Added xsi15(bond1.21) to Fast Deployment File. Added xsi15(bond1.21) to Fast Deployment File. Added zsi16(bond1.22) to Fast Deployment File. Added zsi16(bond1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombi								
		Added imi (bond0.3) to Fast Deployment File. Added rep(bond1.10) to Fast Deployment File. Added xsi1(bond1.6) to Fast Deployment File. Added xsi2(bond1.7) to Fast Deployment File. Added xsi3(bond1.8) to Fast Deployment File. Added xsi5(bond1.11) to Fast Deployment File. Added xsi6(bond1.12) to Fast Deployment File. Added xsi7(bond1.13) to Fast Deployment File. Added xsi7(bond1.14) to Fast Deployment File. Added xsi10(bond1.15) to Fast Deployment File. Added xsi10(bond1.16) to Fast Deployment File. Added xsi10(bond1.16) to Fast Deployment File. Added xsi11(bond1.17) to Fast Deployment File. Added xsi12(bond1.19) to Fast Deployment File. Added xsi13(bond1.19) to Fast Deployment File. Added xsi13(bond1.19) to Fast Deployment File. Added xsi13(bond1.20) to Fast Deployment File. Added xsi16(bond1.21) to Fast Deployment File. Added xsi16(bond1.22) to Fast Deployment File. Added xsi16(bond1.22) to Fast Deployment File. Added zsi16(bond1.22) to Fast Deployment File. Added zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRDNOAM1 to Fast Deployment File. Added Zombie_DSRDNOAM2 to Fast Deployment File. Added Zombie_DSRDNOAM2 to Fast Deployment File. Added Zombie_SDSDNOAM1 to Fast Deployment File. Added Zombie_SDSDNOAM2 to Fast Deployment File. Added Zombie_SDSDNOAM2 to Fast Deployment File. Added Zombie_SDSDNOAM2 to Fast Deployment File. Added Zombie_SDSDNOAM1 to Fast Deployment File. Added Zombie_SDSDNOAM1 to Fast Deployment File. Added Zombie_SDSDNOAM2 t								
		Added Zombie DSRNOAM2 to Fast Deployment File.								
		Added Zombie_DSRDRNOAM1 to Fast Deployment File.								
		Added Zombie_DSRDRNOAM2 to Fast Deployment File.								
		Added Zomble_SDSNOAM1 to fast Deployment file.								
		Added Zombie SDSDROAM1 to Fast Deployment File.								
		Added Zombie_SDSDRNOAM2 to Fast Deployment File.								
		Added Zombie DSRSOAM1 to Fast Deployment File.								
		Added Zombie_DSRSOAM2 to Fast Deployment File.								
		Added Zombie SDSSOAM1 to Fast Deployment File.								
		Added Zombie_DSRDAMP1 to Fast Deployment File.								
		Added Zombie DSRDAMP2 to Fast Deployment File.								
		Added Zombie DSRIPFE1 to Fast Deployment File.								
		Added Zomble_DSRIPTE2 to rast Deployment file. Added Zomble SDSDPSV1 to Fast Deployment File.								
		Added Zombie SDSDPSV2 to Fast Deployment File.								
		Validating Fast Deployment File								
		Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml"								
		configuration file validation successful.								
		Successful Validation of Zombie DSR Fast Deployment 06-15-16.xml								
		SUCCESS: OPERATION SUCCESS !!								
		[admusr@5010441PMAC RMS]\$								

19. []	PMAC : Execute fast deployment	With the file generated from the config.sh script, execute the following command to start fast deployment: \$ screen \$ sudo fdconfig configfile= <fd_config.xml></fd_config.xml>							
	Note: This is a long duration command. If the screen command was before executing the fdconfig, perform a screen -dr to resume screen session in the event of a terminal timeout, etc.							sume t	:he
20.	PMAC GUI:	1. If not alre	ady done, es	tablish a Gl	JI session or	n the Pl	MAC se	erver.	
	Monitor the configuration	2. Navigate	to Task Mon	itoring.					
		💽 📄 Statu	s and Manage Monitoring						
			wonitoning						
			Notices						
			ut						
			ui.						
		3. Monitor th	ne configurati	on to compl	etion:				
		Main Menu: Task Mo	nitoring						
		Filter* -							
		D Task	Target RMS: pc5010441 Guest:	Status	State	Task Output	Running Time	Start Time 2016-07-11	Progress
			Zombie_SDSDRNOAM1 RMS: pc5010441		COMPLETE			2016-07-11	
		924 Accept	Guest: Zombie_SDSNOAM1 BMS: pc:5010441	Success	COMPLETE	NIA	0:01:04	11:27:04	100%
		923 Accept	Guest: Zombie_DSRIPFE1 RMS: pc5010439	Success	COMPLETE	NA	0:01:06	11:26:43	100%
		922 Accept	Guest: Zombie_DSRDAMP2 RMS: pc:5010441	Success	COMPLETE	N/A	0:01:05	11:26:43	100%
		921 Accept	Guest: Zombie DSRDAMP1	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%
		920 Accept	RMS: pc5010439 Guest: Zombie_DSRSOAM2	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:42	100%
		Note: If a fa /var/ [admusr@melbd file=deploy_r Dump Steps in Here are the Dump of DB st NUM PHS DLY : 1 1 0 pmac Fa available 2 1 0 pmac Fa 3 1 0 pmac Fa	Allure occurs with a second state of the secon	with fdconfig config/fdcor fdconfig]\$ 170329T2024 Loy_melbour were genera TYPE CMD EL TYPE CMD EL to 21 0 C nt 0 1 1 1 nt 0 3 melb	g, logs can b nfig.log file. sudo fdcon: 58_701b.fdcd ne_201703297 ted EMENT PRE ST omplete 300 Skipped 300 ourne_RMS3 3	e acces fig dum db r202458 TATE TC 0 Chec 0 Add 1 Skipp	sed in psteps _701b.f BGTS (Edcdb" COMMANE is is 0 Add) TEXT
		4 2 0 pmac Fa	ast_Deploymer	nt 1	_		_		
		4. Restart th	ne fdconfig af	ter a failure	has occurre	d and h	as beer	n resolv	ved:
		<pre>\$ sudo fd file=depl</pre>	config res oy_melbour	start rne_20170	329T20245	8_701]	b.fdcc	lb	

21. □	PMAC : Repeat for each rack mount server configuration file	Repeat steps 1320. for each rack mount server/configuration file, if required.			
22.	PMAC: Back up FDC file	 Copy the updated fdc file to the fdc backup directory: \$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> /usr/TKLC/smac/etc/fdc/</fdc_file> Change permissions: \$ sudo chmod 777 /usr/TKLC/smac/etc/fdc/<fdc_file></fdc_file> Configure VM CPLL socket pipping on each TVOE bact to optimize 			
23.	Perform CPU pinning	Configure VM CPU socket pinning on each TVOE host to optimize performance by executing the CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen9 Only) procedure from reference [8].			
24.	NOAM GUI: Login If the failed server is not OAM, then skip to step 47.	 Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: http://<primary_noam_vip_ip_address></primary_noam_vip_ip_address> Login as the guiadmin user: Coracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Username: Password: Change password Log in Welcome to the Oracle System Login. Welcome to the Oracle System Login. Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookles. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. 			
		Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Copyright © 2010, 2016, <u>Oracle</u> and/or its affiliates. All rights reserved.			

25.	NOAM VIP GUI: Recover standby NOAM, if needed	Install the second NOAM server: DSR : Execute the Configure the Second NOAM Server procedure, steps 1 and 3- 6, from reference [8]. SDS : Execute the Configure the Second SDS NOAM Server procedure, steps 1 and 3-6, from reference [8].			
26. □	Install NetBackup client (optional)	If NetBackup is u procedure from r	used, execute the I reference [8].	nstall NetBa	ckup Client (Optional)
27.	NOAM VIP GUI: Set HA on standby NOAM	procedure from reference [8]. 1. Navigate to Status & Manage Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Click Edit. 3. Select the standby NOAM server Modifying HA attributes Hostname Max Allowed HA Role C ZombieNOAM1 Active T Active T Active T Active T Active T Active T		> HA. er and set it t Description The maximum The maximum The maximum	o Active .

Procedure 4.	Recovery	Scenario 4
--------------	----------	------------

28.	NOAM VIP GUI: Restart DSR application	 1. Navigate to Status & Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Select the recovered standby NOAM server and click Restart.
29.	Active NOAM: Correct the recognized authority table	 Establish an SSH session to the active NOAM and login as admusr. Execute this command: \$ sudo top.setPrimary Using my cluster: A1789 New Primary Timestamp: 11/09/15 20:21:43.418 Updating A1789.022: <dsr_noam_b_hostname></dsr_noam_b_hostname> Updating A1789.144: <dsr_noam_a_hostname></dsr_noam_a_hostname>
30 .	NOAM VIP GUI: Recover query servers. SDS only. If DSR, skip to step 33.	Execute the Configuring SDS Query Servers procedure, steps 1 and 4-7, from reference [8].

Procedure 4. Recovery Scenario 4

31.	SDS NOAM VIP GUI: Set HA on query server. SDS only. If DSR, skip to step 33.	 Navigate to ortation of manage > mA. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click Edit. Select the query server and select Observer. 			
		ZombieQS1 Observer The Observer Oos 4. Click OK.			
32.	SDS NOAM VIP GUI: Restart SDS application. SDS only. If DSR, skip to step 33.	 1. Navigate to Status & Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the recovered query server and click Restart. 			
33.	NOAM VIP GUI: Recover the SOAM servers (Standby, Spare — Oracle X5-2/Netra X5- 2/X6-2/X7-2/HP DL380 Gen 9 Only)	DSR: Execute the Configure the SOAM Servers procedure, steps 1-3 and 5-9, from reference [8]. Note: If you are using NetBackup, also execute step 12. SDS: Execute the Configure the SDS DP SOAM Servers procedure, steps 1-3 and 5-8, from reference [8].			

Procedure 4. Recovery Scenario 4

34.	NOAM VIP GUI:	1. Navigate to Status & Manage > HA.			
	NOAM	 Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click Edit. Select the standby NOAM server and set it to Active. Modifying HA attributes 			
		Hostname Max Allowed HA Role Description			
		ZombieNOAM1 Active The maximum			
		ZombieNOAM2 Active The maximum			
		ZombieDRNOAM1 Standby 4. Click OK. The maximum			
35.	NOAM VIP GUI: Restart DSR application	 1. Navigate to Status & Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Select the recovered standby NOAM server and click Restart. 			
36. □	Activate PCA feature. DSR only. If SDS, skip this step.	If you have PCA installed in the system being recovered, re-activate PCA by executing the PCA Activation on Active NOAM Network procedure on the recovered standby NOAM server and the PCA Activation on Stand By SOAM Network procedure on the recovered standby SOAM from reference [7].			

37.	NOAM VIP GUI: Recover the C-level servers (DA-MPs, SBRs, IPFE, SS7- MP, and SDS DPs	 DSR: Execute the Configure the MP Servers procedure, steps 1 and 9-13, from reference [8]. Note: Also execute steps 14-16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. 			
		SDS — Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 Only: Execute the Configure the SDS DP Servers procedure, steps 1 and 5-8, from reference [8],			
		Repeat this ste	p for any remaining f	ailed MP servers.	
38.	NOAM VIP GUI: Set HA on all C- level servers	 Navigate to Status Status Net Ser HA To Click Edit. For each se Active. 	Status & Manage & Manage work Elements ver abase s cesses erver whose Max Allo	• HA.	
		ZombieDAMP1	Active	The maximum desired HA Role for ZombieDAMI	
		ZombieDAMP2	Spare Observer OOS	The maximum desired HA Role for ZombieDAMI	
		4. Click OK .			

39.	NOAM VIP GUI: Restart DSR application on recovered C-level servers	 1. Navigate to Status & Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the recovered C-level servers and click Restart. P Restart Rebx
40.	Active NOAM: Perform keyexchange between the active- NOAM and recovered servers	 Establish an SSH session to the active NOAM, login as admusr. Perform a keyexchange from the active NOAM to each recovered server: \$ keyexchange admusr@<recovered hostname="" server=""></recovered> Note: If an export server is configured, perform this step.
41.	Active NOAM: Activate optional features. DSR only. If SDS, then skip step 43.	 Establish an SSH session to the active NOAM and login as admusr. Note for PCA Feature Activation: If you have PCA installed in the system being recovered, re-activate the PCA by executing the PCA Activation on Active NOAM Server procedure on recovered active NOAM server and the PCA Activation on Standby SOAM Server procedure on the recovered standby SOAM server from [6]. Notes: If not all SOAM sites are recovered at this point, then repeat the activation for each "new" SOAM site that comes online. If any of the MPs have failed and recovered, then restart these MP servers after activation of the feature. Refer to section 1.5 Optional Features to activate any features that were previously activated. Note: While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored: iload#31000{S/W Fault}
42.	MP Servers: Disable SCTP Auth Flag (DSR only). DSR only. If SDS, then skip step 43.	For SCTP connections without DTLS enabled, refer to the Enable/Disable DTLS (SCTP Diameter Connections Only) section in reference [8]. Execute this procedure on all failed MP servers.

Procedure 4. Recovery Scenario 4

r						
43.	NOAM VIP GUI: Fetch and store the database report for the newly restored data and save it	1. Navigate to Status & Manage > Database.				
		😑 😋 Status & Manage				
		Network Elements				
		Server Server				
		THA INTERNATIONAL INTERNATIA INTERNATIANA INTERNATIANA INTERNATIANA INTERNATIA INTERNATIANA INTERNAT				
		Database				
		KPIs				
		2. Calent the active NOAM commence and alight Bernart				
		2. Select the active NOAM server and click Report .				
		oning Report Inhit				
		The following screen displays:				
		Main Menu: Status & Manage -> Database [Report]				
		dsr Database Status Report				
		Report Generated: Tue Oct 11 13:24:26 2016 EDT				
		From: Active Network OAM&P on host ZombieNOAM1 Report Version: 8.0.0.0.0-80.9.0				
		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.				

44 .	Active NOAM: Verify replication between servers	1. Log into the active NOAM as admusr using SSH terminal.					
		2. Execute this command:					
		\$ sudo irepstat -m					
		Example output:					
	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					
		Vanu-SOAM-2 Active					
		AB From Oanu-NOAM-2 Active 0 0.50 0.03%cpu 24B/s					
		BE TO UARU-SUAM-I ACCIVE 0 0.50 1%R 0.04% CPU 32B/S					
		BC TO Oahu-SS7MD-2 Lative 0 0.50 1% 0.04% cpu $21B/S$					
		irepstat (40 lines) (h)elp (m)erged					

45. □	NOAM VIP GUI : Verify the database	1.	Navigate to Status	& Manager > Database.			
	states	Status & Manage					
			Database				
			KPIs				
			Processes				
		2. Verify the OAM Max HA Role as shown.					
			Role	Server Type	Expected	d HA Role(s)	
			Network OAM&P	NO	Active/St	andby	
			SYSTEM OAM	SOAM	Active/St	andby/Spare	
			MP	DA MP(s)	Active		
		IPFE(s)					
		SS7MP(s)					
			MP	SBR(s)	Active/St	andby/Spare	
		 Verify the Status and OAM Repl Status is Normal and Repl Status=Allowed. 				pl	
46.	NOAM VIP GUI:	1.	Navigate to Status a	and Manage > HA.			
	Verify the HA status	🖃 😋 Status & Manage					
	010100	Network Elements					
			Database				
			Control Processes				
			🕕 🧰 Tasks				
			Files				
		2.	Select the row for al	l of the servers.			
		3.	Verify the HA Kole is	s either Active or Standi	уу.		
		Hostname OAM HA Role Application HA Role Max Allowed HA Role ZombieNOAM1 Active N/A Active					
		ZombieNOAM2 Standby N/A Active					
		Zom		Active	N/A	Active	
		2011		Standby	N/A	Active	
		Zom	DIESUAMIT	Active	N/A	Active	

47.	SOAM VIP GUI: Verify the local node information. DSR only. If SDS, then skip to step 56.	 Navigate to Diameter > Configuration > Local Node. Diameter Configuration Capacity Summary Connection Capacity Dashb Application Ids CEX Parameters Command Codes Configuration Sets Configuration Sets Local Nodes Local Nodes
		2. Verify all the local nodes are shown.
48.	SOAM VIP GUI: Verify the peer node information. DSR only. If SDS, then skip to step 56.	 1. Navigate to Diameter > Configuration > Peer Node. Diameter Configuration Capacity Summary Connection Capacity E Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes 2. Verify all the peer nodes are shown.
49.	SOAM VIP GUI: Verify the connections information. DSR only. If SDS, then skip to step 56.	 3. Navigate to Diameter > Configuration > Connections. Diameter Configuration Capacity Summary Connection Capacity Dash Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes Peer Node Groups Connections 4. Verify all the connections are shown.

50.	SOAM VIP GUI:	1. Navigate to Diameter > Maintenance > Connections .
	Enable connections, if needed. DSR only. If SDS, then skip to step 56.	 Maintenance Route Lists Route Groups Peer Nodes Connections Select each connection and click Enable. Alternatively, enable all the connections by clicking EnableAll. EnableAll Disable.
		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
51.	SOAM VIP GUI: Enable optional features. DSR only. If SDS, then skip to step 56.	 Navigate to Diameter > Maintenance > Applications. Maintenance Route Lists Route Groups Peer Nodes Connections Egress Throttle Groups Egress Throttle Groups Applications Select the optional feature application configured in step 72. Click Enable. Disable Pause updates
52.	SOAM VIP GUI: Re-enable transports, if needed. DSR only. If SDS, then skip to step 56.	 Navigate to Transport Manager > Maintenance > Transport. Transport Manager Configuration Maintenance Transport Select each transport and click Enable. Enable Disable Block Verify the Operational Status for each transport is Up.

53.	SOAM VIP GUI: Re-enable MAPIWF application, if needed. DSR only. If SDS, then skip to step 56.	 Navigate to SS7/Sigtran > Maintenance > Local SCCP Users. SS7/Sigtran Configuration Maintenance Local SCCP Users Remote Signaling Points Remote MTP3 Users Linksets Links 2. Click the Enable button corresponding to MAPIWF Application Name.
		3. Verify the SSN Status is Enabled .
54.	SOAM VIP GUI: Re-enable links, if needed. DSR only. If SDS, then skip to step 56.	 1. Navigate to SS7/Sigtran > Maintenance > Links. SS7/Sigtran Configuration Maintenance Local SCCP Users Remote Signaling Points Remote MTP3 Users Linksets Links 2. Click Enable for each link. Enable Disable 3. Verify the Operational Status for each link is Up.

55.	SOAM VIP GUI:	1. Navigate to SS7/Sigtran > Maintenance > Remote MTP3 Users.
	MTP3 users, if needed. DSR only. If SDS, then skip to step 56.	 SS7/Sigtran Configuration Maintenance Local SCCP Users Remote Signaling Poin Remote MTP3 Users Linksets Links 2. Click Reset for each record, if needed. Reset
56.	NOAM VIP: Verify all servers in topology are accessible (RADIUS only)	<pre>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. Establish an SSH session to the NOAM VIP and login as admusr. 2. Check if all the servers in the topology are accessible:</pre>
57.	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 (the NOAM, which is intact and was not recovered) server is valid:
Procedure 4. Recovery Scenario 4

	\$ cd /usr/TKLC/dpi/bin/
	\$./sharedKrevo -validate
	Example output:
	[admusr@NOAM-2 bin]\$./sharedKrevo -validate
	FIPS integrity verification test failed.
	1450723458: [INFO] Key file for 'NOAM-1' is valid
	1450723458: [INFO] Key file for 'NOAM-2' is valid
	FIPS integrity verification test failed.
	1450723460: [INFO] Key file for 'SOAM-2' is valid
	FIPS integrity verification test failed.
	1450723461: [INFO] Key file for 'MP-2' is valid
	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. 1450722733: [INFO] Synched key to IPFE FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722734: NON-2 and MP-2 key files differ. Sync NON-2 key file to MP-2.
	FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722735: [INFO] Synched key to MP-2 FIPS integrity verification test failed. FIPS integrity verification test failed.
	1450722736: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. FIPS integrity verification test failed. 1450722738: [INFO] Synched key to MP-1 [admusr@NOAM-2 bin]\$
	\$./sharedKrevo -updateData
	Example output:

		<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. FIPS integrity verification test failed. 1450203522: [INFO] 1 rows updated on 'SOAM-2' 1450203522: [INFO] Data updated to 'SOAM-2'</pre> Note: If any errors display, stop and contact My Oracle Support (MOS).				
58.	SOAM VIP GUI: Examine all alarms	 Navigate to Alarms & Events > View Active. Alarms & Events View Active View History View Trap Log Examine all active alarms and refer to the on-line help on how to address them. If needed, contact My Oracle Support (MOS). 				
59.	NOAM VIP GUI: Examine all alarms	 Navigate to Alarms & Events > View Active. Alarms & Events View Active View History View Trap Log Examine all active alarms and refer to the on-line help on how to address them. If needed, contact My Oracle Support (MOS). 				
60.	Restart oampAgent, if needed	 Note: If 10012: The responder for a monitored table failed to respond to a table change alarm displays, the oampAgent needs to be restarted. 1. Establish an SSH session to each server that has the alarm. 2. Login admusr 3. Execute the following commands: \$ sudo pm.set off oampAgent \$ sudo pm.set on oampAgent 				
61. 	Back up and archive all the databases from the recovered system	Execute the DSR Database Backup procedure to back up the configuration databases.				
62.	Recover IDIH	If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.				

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

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

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

S T 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.	Workarounds	 Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist. Refer to Appendix K SNMP Configuration to configure SNMP as a workaround in these cases: 1. If SNMP is not configured in DSR. 2. If SNMP is already configured and SNMPv3 is selected as enabled version. 			
2. □	Gather required materials	Gather the documents and required materials listed in Required Materials.			
3. □	Switch DR NOAM to primary	Refer to [13] DSR/SDS NOAM Failover User's Guide.			

Procedure 5. Recovery Scenario 5

4.	Recover failed	If ALL SOAM servers have failed, execute Procedure 2.						
	SOAMS	If ALL NOAM servers have failed, execute:						
		1. Procedure 4, steps 4. through 14.						
		2. Perform keyexchange between the newly active NOAM and the recovered NOAM PMAC.						
			From a terminal window connection on the active NOAM as the admusr use exchange SSH keys for admusr between the active NOAM and the recovered NOAM's PMAC server using the keyexchange utility, using the management IP address for the PMAC server.					
			When asked for the password, enter the password for the admusr user of the PMAC server.					
			<pre>\$ keyexchange admusr@<recovered_servers_pmac_ip address=""></recovered_servers_pmac_ip></pre>					
		te: If keyexchange fails, edit /home/admusr/.ssh/known_hosts and remove blank lines. Retry the keyexchange commands.						
		3.	Use the PMAC GUI to determine the control network IP address of the recovered VMs.					
		4. Navigate to Software Inventory .						
		5.	Perform a keyexchange between the recovered PMAC and the recovered guests:					
			From a terminal window connection on the recovered PMAC as the admusr user, exchange SSH keys for admusr between the PMAC and the recovered VM guests using the keyexchange utility, using the control network IP addresses for the VM guests.					
			When asked for the password, enter the password for the admusr user of the VM guest.					
		<pre>\$ keyexchange admusr@<recovered_vm_control_ip add<="" pre=""></recovered_vm_control_ip></pre>						
		<i>Note:</i> If keyexchange fails, edit /home/admusr/.ssh/known_hosts blank lines. Retry the keyexchange commands.						
		6.	Procedure 4, steps 15. through 19. for each NOAM.					
5.	Perform keyexchange	Per NO	form a keyexchange between the newly active NOAM and the recovered AM servers:					
	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.							
		9.	. When prompted for the password, enter the password for the admusr user of the recovered NOAM servers.					
		<pre>\$ keyexchange admusr@<recovered_noam hostname=""></recovered_noam></pre>						
-								

6. □	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.		
7.	Recovered NOAM Servers: Activate optional features	 Map-Diameter Interworking (MAP-IWF) and/or Policy and Charging Application (PCA) Only Activate the features Map-Diameter Interworking (MAP-IWF) and Policy and Charging Application (PCA) as follows: For PCA: Establish SSH sessions to the all the recovered NOAM servers and login as admusr. Refer [7] and execute PCA Activation on Standby NOAM Server on all recovered NOAM servers to re-activate PCA. For MAP-IWF: Establish SSH session to the recovered active NOAM, login as admusr. Refer to [5] to activate Map-Diameter Interworking (MAP-IWF). 		
		 Note: While running the activation script, the following error message (and corresponding messages) output may display. This can safely be ignored: iload#31000{S/W Fault} Note: If any of the MPs are failed and recovered, then restart these MP servers after activation of the feature. 		
8.	NOAM VIP: Copy key file to all the servers in topology (RADIUS only)	<pre>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 (the NOAM, which is intact and was not recovered) server is valid: \$ cd /usr/TKLC/dpi/bin/ \$./sharedKrevo -validate Note: If output of above command shows that existing key file is not valid, contact My Oracle Support (MOS). 2. Copy the key file from active DR NOAM to recovered NOAMs. \$./sharedKrevo -copyKey -destServer <first noam="" server=""> \$./sharedKrevo -copyKey -destServer <second noam="" server=""></second></first></pre>		

9. □	Primary NOAM: Modify DSR OAM process	1. 2.	Establish an SSH session to the primary NOAM, login as admusr . Retrieve the cluster ID of the recovered NOAM:			
			<pre>\$ sudo iqt -fClusterID TopologyMapping where "NodeID='<dr_noam_host_name>'" Server_ID NodeID ClusterID 1 Oabu DSB_NOAM 2</dr_noam_host_name></pre>			
		3.	Execute this command to start the DSR OAM process on the recovered NOAM:			
			<pre>\$ echo "<clusterid> DSROAM_Proc Yes" iload -ha -xun -fcluster -fresource -foptional HaClusterResourceCfg</clusterid></pre>			
10.	Switch DR NOAM back to secondary	On Use	ce the system has been recovered, refer to [13] DSR/SDS NOAM Failover er's Guide.			

 	· · · · · · · · · · · · · · · · · · ·
NOAM VIP: Verify all servers in topology are accessible (RADIUS only). DSR only. If SDS, then skip to the next step.	<pre>/ fthe RADUS key has never been revoked, skip this step. If RADUS was never configured on any site in the network, the RADUS key would have most likely never been revoked. Check with your system administrator. 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>
	Note: If any errors display, stop and contact My Oracle Support (MOS).

12.	Recovered Servers: Verify alarms	 Navigate to Alarms & Events > View Active. Alarms & Events View Active View History View Trap Log Verify the recovered servers are not contributing to any active alarms (Replication, Topology misconfiguration, database impairments, NTP, etc.)
13. □	Recover IDIH	If IDIH was affected, refer to section 6 IDIH Disaster Recovery to perform disaster recovery on IDIH.

4.6 Recovery Scenario 6 (Database Recovery)

4.6.1 Recovery Scenario 6: Case 1

For a partial outage with

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

Notes:

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

Procedure 6. Recovery Scenario 6 (Case 1)

STEP#	This procedure perform a site have failed. T Check off ($$) each s step number. If this procedure fails assistance.	orms recovery if at least one NOAM server is available, but all SOAM servers in this includes any SOAM server that is in another location. tep as it is completed. Boxes have been provided for this purpose under each s, it is recommended to contact My Oracle Support (MOS) and ask for				
1.	WorkaroundsRefer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.					

2. □	NOAM VIP GUI : Login	 Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: 					
		http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>					
		2. Login as the guiadmin user:					
		ORACLE					
		Oracle System Login Tue Jun 7 13:49:06 2016 EDT					
		Log In Enter your username and password to log in					
		Username:					
		Password:					
		Change password					
		Log In					
		Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.					
		Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.					
		Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.					

Procedure 6. Recovery Scenario 6 (Case 1)

Procedure 6. Recovery Scenario 6 (Case 1)

3.	NOAM VIP GUI:	1. Navigate to Status & Manage > HA.						
	Set failed servers	🖃 😋 Status & Manage						
		Server						
		HA HA						
		🔤 🛐 Database						
		KPIs						
		2. Select Edit.						
		Modifying HA attributes						
		Hostname Max Allowed HA Role Description						
		ZombieNOAM1 Active The maximum des						
		ZombieNOAM2 OOS The maximum des Active						
		ZombieDRNOAM1 Spare The maximum des Observer						
		3. Set the Max Allowed HA Role option to OOS for the failed servers.						
		4. Click OK .						
		Ok Cancel						
4.	Server in Question: Login	Establish an SSH session to the server in question. Login as admusr .						
5.	Server in	Bring the system to runlevel 3.						
	Question: Change runlevel	\$ sudo init 3						
	to 3							
6.	Server in Question:	Execute this command and follow the instructions appearing in the console prompt.						
	Recover system	<pre>\$ sudo /usr/TKLC/appworks/sbin/backout_restore</pre>						
7.	Server in	Bring the system back to runlevel 4.						
	Question: Change runlevel to 4	\$ sudo init 6						

8 Server in Verify if the processes are up and rupping							
0.	Question: Verify	\$ sudo pm.getprocs					
		A 5139 cmha	Ū	p 12/	21 13:16:25 1	cmha	
		A 5140 cmplata	larm U	p 12/	/21 13:16:25 1	cmplatalarm	
		A 5143 cmsnmps	a U	p 12/	21 13:16:25 1	cmsnmpsa -R 1.3.6.1.4.1.3	
		A 5145 cmsoapa	U	p 12/	21 13:16:25 1	ствоара	
		A 9969 eclipse	Help U	p 12/	/21 13:16:39 1	eclipseHelp	
		A 5149 idbsvc	U	p 12/	21 13:16:25 1	. idbsvc -M10 -ME204 -D40 -	
		A 6149 idbunlo	ck U	p 12/	/21 13:16:36 1	idbunlock -f	
		A 5151 inetmer	ge U	p 12/	21 13:16:25 1	inetmerge	
		A 5155 inetrep	D. D.	p 12/	21 13:16:25 1	. inetrep	
		A 5160 CampAge	hdog U	p 12/ p 12/	21 13:16:25 1 21 13:16:25 1	pm.watchdog	
		A 5167 raclerk	U	p 12/	21 13:16:25 1	raclerk -r 6000	
		A 5171 re.port	map U	p 12/	21 13:16:25 1	re.portmap -c100	
		A 5174 Stattle	rk U	p 12/ p 12/	21 13:16:25 1 21 13:16:25 1	vipmgr	
		A -1 AstateI	nit D	one 12/	/21 13:16:36 1	AstateInit	
		A -1 auditPT	ask D	one 12/	21 13:16:36 1	auditPeriodicTask	
		A -1 auditia A -1 guiRegM	apLoad D	one 12/	21 13:16:36 1	guiRegMapLoad	
		A -1 mkdbhoo	ks D	one 12/	/21 13:16:25 1	mkdbhooks	
		[root@MP-1 admu	sr]#				
9.	NOAM VIP GUI:	1. Navigate to	o Status & Mana	age > I	HA.		
	Set failed servers						
	to active	🖃 🔄 Status	& Manage				
		🔤 🕅 Net	work Elements				
		💽 Ser	ver				
		🚮 HA					
		Database					
		Database					
			5				
		🔤 🏹 Pro	cesses				
		🕞 🧰 Tas	Tasks				
		🔤 📳 File	S				
		2 Click Edit					
		3. Select the failed server and set it to Active.					
		Modifying HA	attributes				
		Hostname	Max Allowed HA Role	Descript	ion		
		ZombieNOAM1	Active 💌	The maxi	mum		
		ZombieNOAM2	Active 💌	The maxi	mum		
			Active				
		ZombioDDNOAMA	Standby	The meri	201122		
		4. Click OK					

Procedure 6. Recovery Scenario 6 (Case 1)

Procedure 6. Recovery Scenario 6 (Case 1)

10.	NOAM VIP: Verify all servers in topology are accessible (RADIUS only)	<pre>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. Establish an SSH session to the NOAM VIP and login as admusr. 2. Check if all the servers in the Topology are accessible: \$ 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-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-2' is accessible. FIPS integrity verification test failed. 1450723798: [INFO] 'MP-1' is accessible.</pre>
11.	NOAM VIP: Copy key file to all the servers in topology (RADIUS only)	<pre>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 (The NOAM which is intact and was not recovered) server is valid: \$./sharedKrevo -validate [admusr@NOAM-2 bin]\$./sharedKrevo -validate FIPS integrity verification test failed. I450723843: [INFO] Key file for 'NOAM-1' is valid I450723843: [INFO] Key file for 'NOAM-1' is valid FIPS integrity verification test failed. FIPS integrity verification</pre>





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)

e have failed. Th	his ir	recovery if at least one NOAM server is available, but all SOAM servers in includes any SOAM server that is in another location.		
$\begin{bmatrix} S \\ T \\ E \end{bmatrix}$ Check off ($$) each step as it is completed. Boxes have been provided for this purpose u step number.				
s procedure fails stance.	s, it is	recommended to contact My Oracle Support (MOS) and ask for		
karounds	Ref crea	Refer to Appendix L Backup Directory to look for a backup directory and create a directory if one does not exist.		
M VIP GUI: n	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:		
		http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>		
	2.	Login as the guiadmin user:		
	Ο Γ.	Added and a series of the set of		
	Ave failed. Ti k off (√) each si number. s procedure fails tance. (arounds M VIP GUI: ∩	a have failed. This in k off (√) each step a number. s procedure fails, it is stance. (arounds Refe creation of the step a M VIP GUI: 1. 1. 2. Ora U U U		

Procedure 7. Recovery Scenario 6 (Case 2)

3.	NOAM VIP GUI: Set failed servers to OOS	 Navigate to Status & Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes 				
		Modifying HA	attributes			
		Hostname	Max Allowed HA Role	Description		
		ZombieNOAM1	Active -	The maximum des		
		ZombieNOAM2	OOS	The maximum des		
		ZombieDRNOAM1	Standby Spare Observer	The maximum des		
		3. Set the Ma	x Allowed HA Ro	le option to OC	DS for the failed serv	/ers.
		4. Click OK.				
		Ok Can	cel			
4.	Server in Question: Login	Establish an SS	SH session to the	server in ques	stion. Login as adm	usr.
5.	Server in	Stop the httpd :	service.			
	httpd service	\$ sudo bas	h -1			
		Stop the HTTP service after the	D service before e database has s	the database i tarted.	s down and start the	HTTPD
		\$ service	httpd stop			
6.	Server in	Take the serve	r out of service.			
	service	\$ prod.clo	bber			
7.	Server in	Take the serve	r to Dbup and sta	irt the DSR ap	plication.	
	uestion: Take server to DbUp	\$ prod.sta	rt			
	state and start the application					

8.	Server in	1. S	start the ht	ttpd service.		
	httpd service		\$ servi	ce httpd sta	art	
		2. E	xit out of	root.		
			\$ exit			
9.	NOAM VIP GUI:	1. N	lavigate to	Status & Man	age > HA.	
	Set failed servers to active	2. C 3. S Moc Zomb Zomb 4. C	Status & Neth Neth Sen HA Data Chick Edit a Select the difying HA bieNOAM1 bieNOAM1 bieNOAM1 bieNOAM1	& Manage work Elements ver abase s cesses ks s at the bottom of failed server and attributes Max Allowed HA Role Active Active Active Standby Spare	the screen. d set it to Active . Description The maximum The maximum	
10.	NOAM VIP GUI:	1. N	lavigate to	Status & Man	age > Server.	
	Restart DSR application	2. S	Statu:	s & Manage etwork Elements erver A atabase PIs rocesses h recovered serv Rebo	ver and click Restart .	

Procedure 7. Recovery Scenario 6 (Case 2)

11.	Server in	1. Verify the processes are up and running:						
	the server state	\$ sudo pm.getprocs						
		Example output:						
		A 5139 cmha Up 12/21 13:16:25 1 cmha						
		A 5140 cmplatalarm Up 12/21 13:16:25 1 cmplatalarm						
		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 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 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 auditPTask Done 12/21 13:16:36 1 auditPeriodicTask						
		A -1 auditTasks Done 12/21 13:16:36 1 auditDefunctTasks						
		A -1 gulRegMapLoad Done 12/21 13:16:25 1 gulRegMapLoad A -1 mkdbhooks Done 12/21 13:16:25 1 mkdbhooks						
		[root@MP-1 admusr]#						
		2. Verify if replication channels are up and running:						
		\$ sudo irepstat						
		Example output:						
		- Policy 0 ActSth [DbDeplication]						
		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						
		3. Verify if merging channels are up and running:						
		\$ sudo inetmstat						
		Example output:						
		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						
12. 🗌	NOAM VIP : Verify all servers in topology are	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.						
	accessible	1. Establish an SSH session to the NOAM VIP and login as admusr.						
	(RADIUS Only).	2. Check if all the servers in the Topology are accessible:						
	skip to step 14.							
		<pre>\$ cd /usr/TKLC/dpi/bin/ \$ (abaradWrawa abacklasses)</pre>						
		<pre>> ./snareakrevo -cneckaccess</pre>						

Procedure 7. Recovery Scenario 6 (Case 2)

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

r		
13. □	NOAM VIP : Copy key file to all the servers in topology (RADIUS	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.
	Only)	was not recovered) server is valid:
		<pre>\$ cd /usr/TKLC/dpi/bin/</pre>
		\$./sharedKrevo -validate
		If output 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
		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.
		FIPS integrity verification test failed.
		FIPS integrity verification test failed. 1450722736: NOAM-2 and MP-1 key files differ. Sync NOAM-2 key file to MP-1.
		FIPS integrity verification test failed.
		FIPS integrity verification test failed.
		FIPS integrity verification test failed. FIPS integrity verification test failed.
		1450722738: [INFO] Synched key to MP-1 [admusr@NOAM-2 bin]\$
		\$./sharedKrevo -updateData
		[admusr@NOAM-1 bin]\$./sharedKrevo -updateData
		1450203518: [INFO] Updating data on server 'NOAM-1'
		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] Data updated to 'SOAM-2'
		<i>Note:</i> If any errors are present, stop and contact My Oracle Support (MOS).
14.	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	Perform this procedure to keep users restored by system restoration.					
E	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each					
P	step number.	step number.				
#	If this procedure fa	ails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.				
1.	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. □	After Restoration:	 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: 				
	NOAM VIP	http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>				
		2. Login as the guiadmin user:				
		URACLE				
		Oracle System Login Tue Jun 7 13:49:06 2016 EDT				
		Log In				
		Enter your username and password to log in				
		Username:				
		Password:				
		Change password				
		Log In				

-	•	
3.	After Restoration: Reset user passwords	 Navigate to Administration > Access Control > Users. Main Menu Administration General Options Access Control Access Control Groups Sessions Certificate Management
		Authorized IPs SFTP Users
		2. Select the user.
		3. Click Change Password.
		Insert Edit Delete Report Change Password
		 Type a new password. Enter the old password once, new password
		twice for guiadmin
		Old Password:
		New Password:
		Retype New Password:
		Force password change on next login
		Continue
		NOTE: The password must be between 8 and 16 characters.
		The password must also contain 3 of these 4 types of characters:
		numeric, lowercase alpha, uppercase alpha, special character (!@#\$%^&*?~).
1	1	

Procedure 8. Keep Restored User

5. Click Continue.

5.3 Remove a Restored User

Procedure 9. Remove the Restored User

S T E P #	Perform this procedure to remove users restored by system restoration Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1.	After Restoration: Log into the NOAM VIP	 Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: http://<primary_noam_vip_ip_address> </primary_noam_vip_ip_address> Login as the guiadmin user: ORACLE® 	
		Oracle System Login Tue Jun 7 13:49:06 2016 EDT Log In Enter your username and password to log in Username: Password: Password: Change password Log In Change password 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.	

2.	After Restoration: Reset user passwords	 Navigate to Administration > Access Control > Users. Main Menu Administration General Options Access Control Access Control Users Groups Sessions Certificate Management Authorized IPs SFTP Users
		2. Select the user.
	3. dit	3. Click Delete. dit Delete Repo Delete selected users? OK Cancel
		4. Click OK to confirm.

Procedure 9. Remove the Restored User

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.

S	Perform this procedure to remove users restored by system restoration.			
ь Е Р	Check off ($$) each ste step number.	as it is completed. Boxes have been provided for this purpose under each		
#	If this procedure fails,	, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1.	Before Restoration: Notify affected users before restoration	Contact each user that is affected before the restoration and notify them that you will reset their password during this maintenance operation.		
2.	Before Restoration: Log	 Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: 		
		http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>		
		2. Login as the guiadmin user:		
		Oracle System Login The Junt 13:49:06 2016 ECC State 13:49:06 2016 ECC State 20:40 Control of C		
		Copyright © 2010, 2016, <u>Oracle</u> and/or its affiliates. All rights reserved.		

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

3.	Before	1. Navigate to Administration > Access Control > Users.
	Record user settings	🖃 💻 Main Menu
		😑 😋 Administration
		📓 General Options
		🖃 🔄 Access Control
		- 🔓 Users
		👘 🚰 Groups
		Sessions
		🔛 🔛 Certificate Management
		Authorized IPs
		SFTP Users
		2. Under each affected user, record the following:
		Username
		Account status
		Remote Auth
		Local Auth
		Concurrent Logins Allowed
		Inactivity Limit
		Comment
		Groups

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

4.	After Restoration: Login	 Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: http://<primary_noam_vip_ip_address></primary_noam_vip_ip_address> Login as the guiadmin user: ORACLE®
		Oracle System Login Tue Jun 7 13:49:06 2016 EDT
		Log In Enter your username and password to log in Username: Password: Change password Log In
		Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.
		Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Copyright © 2010, 2016, <u>Oracle</u> and/or its affiliates. All rights reserved.

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



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

6. □	After Restoration: Repeat for additional users	Repeat step 5 to recreate additional users.
7.	After Restoration: Reset the passwords	See Procedure 8 for resetting passwords for a user.

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

6. IDIH Disaster Recovery

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

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

```
</infrastructure>
 </infrastructures>
<servers>
<tvoeguest id="ORA">
     <infrastructure>localPMAC</infrastructure>
        </postdeploy>
     </scripts>
  </tvoeguest
<tvoequest id="MED">
     <infrastructure>localPMAC</infrastructure>
         <!--Specify which Rack Mount Server TVOE Host the Mediation
server will be placed -->
     <tvoehost>mgmtsrvrtvoe2</tvoehost>
     <name>MED</name>
```

Disaster Recovery Scenarios

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

Procedure 11. IDIH Disaster Recovery Preparation

S	This procedure performs disaster recovery preparation steps for the IDIH.					
E	Check off (√) each step number.	off ($$) each step as it is completed. Boxes have been provided for this purpose under each mber.				
#	If this procedure fa	a fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.				
1. PMAC GUI : 1. Open web browser and enter:		1. Open web browser and enter:				
	Login	http:// <pmac_mgmt_network_ip></pmac_mgmt_network_ip>				
		2. Login as pmacadmin user:				
		ORACLE				
		Uracie System Login Tue Jun 7 13:49:06 2016 EDT				
		Log In				
		Enter your username and password to log in				
		Username:				
		Password:				
		Change password				
		Log In				
		Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.				
		Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.				
		Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.				

2.	PMAC GUI: Verify necessary	1 Navigate to Software > Manage Software Images
	available	Software Inventory
		Manage Software Images
		 Verify the current IDIH TVOE, TPD, Oracle, Application and Mediation images are listed.
		 Verify these values match the name in the <software> </software> section in the hostname-upgrade_xx-xx.xml file.
		<i>Note:</i> 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. □	Oracle Guest : Login	Establish an SSH session to the Oracle guest, login as admusr .
4.	Oracle Guest:	Perform a database health check:
	Perform database health	<pre>\$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i</pre>
	check	Example output:
		admusr@thunderbolt-ora:
		[admusr@thunderbolt-ora ~]\$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i 10:10:52: STARTING HEALTHCHECK PROCEDURE
		10:10:52: date: 05-12-15, hostname: thunderbolt-ora
		10:10:52:
		10:10:52: Checking disk free space 10:10:52: No disk space issues found
		10:10:52: Checking syscheck - this can take a while 10:10:58: No errors in syscheck modules
		10:10:58: Checking Alarm Manager alarmStatus
		10:11:00: No alarms found 10:11:00: Checking statefiles
		10:11:00: Statefiles do not exist
		10:11:00: Checking runlevel 10:11:00: Runlevel is OK (N 4)
		10:11:00: Checking upgrade log
		10:11:00: Analyzing date
		10:11:00: NTF deamon is running 10:11:00: Server is synchronized with ntp server
		10:11:00: Checking NTP status
		10:11:00: Ntp settings is OK
		10:11:00: Checking server entries in host file.
		10:11:00: mediation is present in /etc/hosts
		10:11:00: appserver is present in /etc/hosts 10:11:00: Ping server entries in host file.
		10:11:00: Ping server oracle
		10:11:00: Ping server mediation 10:11:00: Ping server appserver
		10:11:00: Check oracle Server 10:11:01: Oracle Server and resources online
		10:11:01: All tests passed!
		[admusr@thunderbolt-ora ~]\$

Procedure 11. IDIH Disaster Recovery Preparation

	This procedure performs disaster recovery for the IDIH by re-installing the mediation and application			
S	servers.			
E	Check off $()$ each s	heck off ($$) each step as it is completed. Boxes have been provided for this purpose under each		
P #	If this procedure fails	P number. this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance		
# 1	PMAC GUI: Login	1 Open web browser and enter:		
		http:// <pmac_mgmt_network_ip></pmac_mgmt_network_ip>		
		2. Login as pmacadmin user:		
		Oracle System Login		
		Tue Jun 7 13:49:06 2016 EDT		
		Log In Enter your username and password to log in		
		Desmand		
		Password:		
		Change password		
		Log In		
		Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.		
		Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.		
		Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.		
2.	Remove existing	1. Navigate to Main Menu > VM Management.		
	application server	😑 😋 Software		
		Software Inventory		
		Manage Software Images		
		2. Select the application guest.		
		3. CIICK Delete.		
		Edit Delete Clone		
		Upgrade		
		Patch		

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

3.	Remove existing mediation server	 1. Navigate to Main Menu > VM Management. Software Software Inventory Manage Software Images VM Management 2. Select the Mediation guest. 3. Click Delete. Edit Delete Clone Upgrade Patch
4 .	PMAC : Establish SSH session and login	Establish an SSH session to the PMAC, login as admusr .
5.	PMAC : Re-install the mediation and application servers	Execute this command (Enter your upgrade file): \$ cd /var/TKLC/smac/guest-dropin \$ screen \$ sudo fdconfig configfile= <hostname-upgrade_xx-xx- xx>.xml Warning If you run the fdconfig without upgrade in the XML filename, the database is destroyed and you lose all of the existing data. Note: 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.</hostname-upgrade_xx-xx-

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

PMAC GUI: Monitor the configuration	1. If not already done, establish a GUI session on the PMAC server.
	2. Navigate to Task Monitoring.
	🗉 🧰 Status and Manage
	Task Monitoring
	🖉 Help
	Egal Notices
	🔁 Logout
	3. Monitor the IDIH configuration to completion.
	Alternatively, you can monitor the fdconfig status through the command line after executing the fdconfig command:
	Example:
	admusr@bertie:/var/TKLC/smac/guest-dropin
	[admusr@bertie guest-dropin]\$ sudo fdconfig configfile=d-ray_04-21-15.xml run Config Request to start a new configuration Running d-ray_04-21-15.xml configuration Configuration file processing complete
	Created a deployment database file: deploy_d-ray_20150511T093944_630c.fdcdb Preparing to run the configuration steps PM&C has no in progress tasks Cabinet is already provisioned, skipping: 1 RMS is already provisioned, skipping: 10.250.36.27 Server discovery complete: [RMS ip: 10.250.36.27] Hostname for [RMS ip: 10.250.36.27] already set to d-ray skipping
	PMAC GUI: Monitor the configuration

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

Appendix A. DSR Database Backup

Procedure 13. DSR Database Backup

	This procedure backs up the provision and configuration information from an NOAM or SOAM server after the disaster recovery is complete.			
S T Check off (\checkmark) each step as it is completed. Boxes have been provided step number.			ep as it is completed. Boxes have been provided for this purpose under each	
С Р #	If this procedure assistance.	e fails, it is recommended to contact My Oracle Support (MOS) and ask for		
1.	NOAM/SOAM VIP: Login	1.	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:	
			http:// <primary_noam soam_vip_ip_address=""></primary_noam>	
		2.	Login as the guiadmin user:	
			ORACLE	
		0	raela Svetem Login	
			Tue Jun 7 13:49:06 2016 EDT	
			Log In Enter your username and password to log in	
			Password	
			Change password	
			Log In	
			Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.	
			Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.	
			Copyright © 2010, 2016, <u>Oracle</u> and/or its affiliates. All rights reserved.	

2.	NOAM/SOAM	1. Navigate to Status & Manage > Database.
	VIP : Backup configuration	😑 😋 Status & Manage
	data for the	💽 Network Elements
	system	Server Server
		HA HA
		M Database
		KPIS
		– Processes
		2. Select the active NOAM server and click Backup .
		eplication Backup Compa
		3. Make sure that the Configuration checkbox is marked.
		Database Backup
		Field Value
		Server: ZombieNOAM1
		Select data for backup
		© gzip
		Compression * i bzip2
		none
		Archive Name * Backup.dsr.ZombieNOAM1.Configuration.NETV
		Comment
		Ok Cancel
		4. Enter a filename for the backup and click OK .

Procedure 13. DSR Database Backup

3.	NOAM/SOAM	1. Navigate to Status & Manage > Files.
	VIP: Verify the	📮 🚗 Status & Manage
	existence	Network Elements
		Server
		Main Manue Status & Managa > Files
		Gillert - Tasks -
		ZombieNOAM1 ZombieNOAM2 ZombieDRNOAM1 ZombieDRNOAM2 ZombieSOAM1 ZombieSOA
		File Name
		backup/Backup.dsr.ZombieNOAM1.Configuration.NETWORK_OAMP.20161010_103628.MAN.tar.bz2
		metadata/cm_metadata.bt
		metadata/metadata.xml
		TKLCConfigData.ZombieNOAM1.sh
		TKLCConfigData.zombieNOAM2.sh
		TKLCConfigData.zombieSOAW1.sh
		Incucconligibilita.zomblesGAMZ.sn
		ugrade log
		apgrade.log
		2. Select the active NOAM or SOAM tab.
		3. The files on this server display. Verify the existence of the backup file.
4.	NOAM/SOAM VIP: Download	1. From the previous step, select the backup file.
		2 Click Download
	the file to a	
		bload Download
		GB available System ut
		3. Click OK to confirm the download.
5. □	Upload the	Transfer the backed up image saved in the previous step to a secure location
	secure location	
6.	Backup active SOAM	Repeat steps 2 through 5 to back up the active SOAM.

Procedure 13. DSR Database Backup

7.	Take Secured backup of key file (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. Log into ssn shell of active NOAM server using user admusr .
		 Take 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:
		\$./sharedKrevo -encr
		4. Copy the encrypted key file to secure customer setup:
		<pre>\$ sudo scp /var/TKLC/db/filemgmt/DpiKf.bin.encr user@<customer ip="">:<path customer="" of="" setup=""></path></customer></pre>
		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.
Appendix B. Recover/Replace Failed Cisco 4948 Aggregation Switches (HP DL380 Gen 9 Only)

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

	This procedure reco	overs a failed aggregation (4948E/4948E-F) switch.							
	Prerequisites:	Prerequisites:							
	A copy of the ne	etworking xml configuration files							
	• A copy of HP m	cellaneous firmware DVD or ISO							
	IP address and	ostname of the failed switch							
s	Rack mount pos	sition of the failed switch							
T E P	Check off (√) each s step number.	step as it is completed. Boxes have been provided for this purpose under each							
#	If this procedure fail	s, it is recommended to contact My Oracle Support (MOS) and ask for assistance.							
1.	Recover failed	1. Log into the PMAC using SSH as admusr .							
	Aggregation Switches: Cisco 4948E/4948E-F	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>							
		 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. 							
		<i>Note:</i> 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.							
		<i>Note:</i> Copy the switch appropriate init file and use it for respective switch:							
		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.							
		4. The templates can be found using the following method:							
		From the PMAC CLI:							
		df grep -I DSR							
		Sample output:							
		<pre>/var/TKLC/smac/image/repository/DSR- 8.4.0.0.0_84.9.0- x86_64.iso</pre>							
		1118514 1118514 0 100% /usr/TKLC/smac/html/TPD/DSR-							
		8.4.0.0.0_84.9.0-x86_64							
		/var/TKLC/smac/image/repository/DSR-8.4.0.0.0_84.9.0- x86 64.iso							
		<pre>/var/TKLC/smac/image/repository/DSR- 8.4.0.0.0_84.9.0- x86_64.iso</pre>							

	1117976 1117976 0 100% /usr/TKLC/smac/html/TPD/DSR-
5	5. Determine the applicable directory of the DSR release being recovered.
	cd usr/TKLC/smac/html/TPD/ <dsr release<br="">dir>/upgrade/overlay/</dsr>
	Example: cd /usr/TKLC/smac/html/TPD/DSR-8.4.0.0.0_84.9.0-x86_64 /upgrade/overlay/
6	Locate the DSR_NetConfig_Templates.zip file.
E s	Example: 5 11
	-rr 1 root root 611 Feb 21 19:18 change ilo admin passwd.xml
	-rr 1 root root 107086 Feb 21 19:18 DSR_NetConfig_Templates.zip
-	rr 1 root root 11642 Feb 21 19:18 DSR_NOAM_FD_Blade.xml
-	rr1 root root 13346 Feb 21 19:18 DSR_NOAM_FD_RMS.xml
d	dr-xr-xr-x 2 root root 2048 Feb 21 19:18 RMS
-	rr 1 root root 812 Feb 21 19:18 SAMPLE-NetworkElement.xml
-	rr 1 root root 2309 Feb 21 19:20 TRANS.TBL
-	r-xr-xr-x 1 root root 2186 Feb 21 19:18 TVOEcfg.sh
-	r-xr-xr-x 1 root root 598 Feb 21 19:18 TVOEclean.sh
-	rr 1 root root 128/03 Feb 21 19:18 UpgradeHCplug1n.pnp-ov1
7	 Unzip the DSR_NetConfig_Templates.zip file and retrieve the required switch init file.
	Example:
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.
9	Copy the new init file to the /usr/TKLC/smac/etc/switch/xml dir.
	Example:
	<pre>\$ cp <switch_xml_file> /usr/TKLC/smac/etc/switch/xml/</switch_xml_file></pre>

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

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

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

S T E P	This procedure inhibits A and B level replication on all C-level servers of this site. Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.						
# 1.	Active NOAM: Login	Log into the activ	e NOAM serve	r using SSH as	admusr.		
2.	Active NOAM:	Execute this com	xecute this command:				
	Inhibit replication on all C-level servers	<pre>\$ for i in \$(iqt -p -z -h -fhostName NodeInfo where "nodeId like 'C*' and siteId='<soam name="" of="" site_ne="" the<br="">site>'"); do iset -finhibitRepPlans='A B' NodeInfo where "nodeName='\$i'"; done</soam></pre>					
Note: SOAM Site_NE name of the sit active NOAM GUI and navigatin The following figure shows more details the site being recovered, then siteID is				f the site can be havigating to Co e details, for exa iteID is SO_HP	e found out by lo onfiguration > S ample, if ServerS C03.	gging into the Gerver Groups . SO1 belongs to	
		Filter* • Into* •	1-> Servers				
		Rostname	Role	System ID	Server Group	Network Element	
		ZombieNOAM1	Network CAMSP		ZombieteOAM	ZombieNeDAM	
		ZombieNOAM2	Network CAMSP		ZombielvOAM	ZomoleNOAM	
		ZombieDRteOAtt1	Network CAMSP		ZombieDRNOAM	ZombieDRNOAM	
		ZombieORMOAM2	Network OAM&P		ZombleDRNOAM	ZombieORINOAM	
		ZombieSOAM1	System OAM		ZombieSOAM	ZombieSDAM	
		Zombw5O4M2	System CAM		ZombieSOAM	ZombieSOAM	
		ZomoleDAMP1	Mb.		ZombieDAMP	ZombieSO4M	
		ZombieDAIIP2	MP		ZombieDAMP	ZombieSCAM	
3.	Active NOAM: Verify replication has been Inhibited	After executing a would be raised Verify replication InhibitRepPlans SO_HPC03 is se	bove steps to i informing that r inhibition on M field for all the I at as A B .	nhibit replication eplication on M Ps by analyzing MP servers for t	n on MP(s), no a P is disabled. g NodeInfo outpu the selected site,	larms on GUI ut. , for example, Site	
		\$ iqt NodeIn	nfo				
		Example output:					
		nodeId nodeName excludeTables	e hostName noo	deCapability	inhibitRepPlans	siteId	
		A1386.099 NO	D1 NO1	Active		NO_HPC03	
		B1754.109 SC	D1 S01	Active		SO_HPC03	
		C2254.131 MI	22 MP2	Active	АВ	SO_HPC03	
		C2234.233 MI	TI MPI	ACLIVE	АБ	PO_ULCO2	

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

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

S T E P	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	Log into the active NOAM server using SSH as admusr .					
2.	Active NOAM:	Execute this command:						
	Un-Inhibit replication on all C-level servers	<pre>\$ 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</soam_site_ne_name></pre>						
		Note: SC act Please see belongs to Main Menu: Con	OAM Site N tive NOAM the snaps the site be figuration -> Ser	IE name of I GUI and i shot below ing recove	f the site can be for navigating to Con for more details, pred, then siteID is	ound out by logg figuration > Ser for example, if So s SO_HPC03.	ing into the • ver Groups . erverSO1	
		Filter* • Indo* •	0					
		Hostname		Role	System ID	Server Group	Network Element	
		ZombieNOAM1		Network OAMAP		ZombieNOAM	ZombieNOAM	
		ZombieNO482		Network OAMSP		ZombieNOAM	ZombieNOAM	
		ZombieDRIxOAM1		Network CAMSP		ZombieDRNOAM	ZombieDRNOAM	
		ZombieDRNOAM2		Network CAM&P		ZombieDRNOAM	ZombieDRNDAM	
		ZombieSOAM1		System QAM		ZombieSOAM	ZombieSOAM	
		ZombieSO4M2		System QAM		ZombieSOAM	ZombieSOAM	
		ZombieDAMP1		мр		ZombieDAMP	ZombieSO4M	
		ZombieDAMP2		w		ZombieDAMP	ZombieSO4M	
3.	Active NOAM: Verify replication has been Inhibited	After exect would be ra Verify replie InhibitRepF Site SO_H \$ sudo Example of nodeId excludeTab A1386.099 B1754.109 C2254.131	uting above aised inforr cation inhit Plans field PC03 is se iqt Node utput: nodeName les NO1 SO1 MP2 MP1	e steps to u ming that r bition on W for all the l et as A B . EInfo hostName NO1 SO1 MP2 MP1	un-inhibit replication eplication on MP IPs by analyzing I MP servers for the NODECapability Active Active Active Active	on on MP(s), no is disabled. NodeInfo output. e selected site, fo inhibitRepPlan.	alarms on GUI The or example, s siteId NO_HPC03 SO_HPC03 SO_HPC03	

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

s	This procedure inhibits A and B level replication on all C-level servers of this site when active, standby, and spare SOAMs are lost.									
E	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.									
Р #	If this procedure fails	s, it is recomr	nendeo	d to contac	t My Oracle	Support	(MOS) a	and ask for	assistance.	
1.	Active NOAM: Login	Log into the	Log into the active NOAM server using SSH as admusr .							
2.	Active NOAM:	Execute the script from /usr/TKLC/dsr/tools/InhibitReplication.sh, if available.								
	Inhibit replication on all C-level	If the /usr/T script, then	KLC/d use thi	s r/tools/ p s manual c	ath does no ommand.	ot have th	e Inhibi	tReplicatio	on.sh	
	servers	/usr/TKL0	C/dsr/	/tools/Ir	nhibitRep	licatio	on.sh -	-		
		replicati	on=ir	nhibit	-SO_SG_Na	me= <so< td=""><td>AM serv</td><td>ver group</td><td>> name></td></so<>	AM serv	ver group	> name>	
		Alternatively	/ to the	above scr	ipt, if the sc	ript is not	t in the s	pecific path	1:	
		\$ for i in	n \$(sud	lo Imysql.c	lient -B -I	N-e "				
		FROM app	works.	Server CS,	appworks.	Server P	S, appwo	rks.Server	2SG C2SG,	
		appworks.	appworks.Server2SG P2SG, appworks.ServerGroup CSG, appworks.ServerGroup							
		comcol.Clu	usterGr	coupInfo	.1, CONCOL.	crustern	IIIO PCI,			
		WHERE CS	Sh_Se	erver_ID =	C2SGh_Se	rver_ID				
		AND C2	2SGh_ SG_alus	_SG_ID = CS	Gh_SG_ID	4				
		AND CO	CI.grou	ips = comcc	l.ClusterG	roupInfo	.groupId	l		
		AND comcol.ClusterGroupInfo.parentGroup = PCI.groups								
		AND PCI.clusterId = PSG.clusterId								
		AND PSG.ServerGroupName='< <u>SOAM_SG_NAME></u> '								
		done	su -111	штотскеррт	alis- A b I	Noderiiro	where	IIOGENallie-	γı /	
		Note: SO. into Gro	AM_SC the ac	G_NAME is ative NOAM	the name of GUI and na	of the ser avigating	ver grou to Conf	ip found by figuration >	logging > Server	
		For example group is SC	e, if SC _SG.	AM1 belor	igs to the si	te being	recovere	ed, then the	server	
		DRNO_SG	A	NONE	DSR (active/standby pair)	1	Network Elemen Server DRNOAM1 DRNOAM2	t DSR_DR_NO_NE Node HA Pref	VIPs	
							Network Elemen	t DSR_NO_NE	1/10-	
		NO_SG	A	NONE	pair)	1	NOAM1 NOAM2	NOUE HA PIET	VIPS	
		Network Element: DSR					t DSR_SO_NE			
		SO_SG	В	NO_SG	DSR (active/standby pair)	1	Server SOAM1 SOAM2	Node HA Pref	VIPs	

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

3.	Active NOAM: Verify replication has been inhibited	After exect would be ra Verify replie InhibitRepF example, s Execute th	uting above aised inforr cation inhit Plans field f erver grou is comman	e steps to in ning that re pition on M for all the N p SO_SG i d:	nhibit replication e eplication on MP Ps by analyzing I MP servers for the is set as A B .	on MP(s), no alarm is disabled. NodeInfo output. e selected server g	ns on GUI proup, for
		\$ iqt N	odeInfo				
		Example o	utput:				
		nodeId excludeTab	nodeName les	hostName	nodeCapability	inhibitRepPlans	siteId
		A1386.099	NO1	NO1	Active		NO_HPC03
		B1754.109	S01	S01	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)

s	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.					
T E	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.					
P #	If this procedure fails	s, 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	<pre>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=allowSO_SG_Name=<soam group="" name="" server=""> 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 CSh_Server_ID = C2SGh_Server_ID AND C2SGh_SG_ID = CSGh_SG_ID AND CSG.clusterId = CCI.clusterId AND CCI groups = comcol ClusterGroupInfo groupId</soam></pre>				
		<pre>AND Contect.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.</soam_sg_name></pre>				
		DRNO_SG A NONE DSR (adtwe/standby pair) 1 Network Element DSR_DR_NO_NE DRNO_SG A NONE DSR (adtwe/standby pair) 1 Node HA Pref VIPs DRNOAM1 DRNOAM2 Network Element DSR_NO_NE Server Node HA Pref VIPs				
		NO_SIG A NONE pair/ 1 NOAI1 NOAI1 NO_SIG B NO_SIG DSR (active/standby pair) 1 Network Element DSR_SO_NE SO_SIG B NO_SIG DSR (active/standby pair) 1 SOAI1 SOAI2 Image: Noois and pair Image: Noois and pair Image: Noois and pair Image: Noois and pair				

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

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

3.	Active NOAM: Verify replication has been Inhibited	After exect would be ra Verify replie InhibitRepF example, s Execute thi	ating above aised inforr cation inhit Plans field erver grou s comman	e steps to u ning that re pition on M for all the N p SO_SG i d:	In-inhibit replicati eplication on MP Ps by analyzing I MP servers for the is set as A B .	on on MP(s), no al is disabled. NodeInfo output. e selected server g	arms on GUI proup, for
		\$ sudo	iqt Node	Info			
		Example of	utput:				
		nodeId excludeTab	nodeName les	hostName	nodeCapability	inhibitRepPlans	siteId
		A1386.099	NO1	NO1	Active		NO_HPC03
		B1754.109	S01	S01	Active		SO_HPC03
		C2254.131	MP2	MP2	Active	A B	SO_HPC03
1		C2254.233	MP1	MP1	Active	A B	SO_HPC03

Appendix G. Restore TVOE Configuration from Backup Media

Procedure 19. Restore TVOE Configuration from Backup Media

	This procedure provides steps to restore the TVOE application configuration from backup media.			
S T F	Check off $()$ each step number.	step as it is completed. Boxes have been provided for this purpose under each		
Р #	If this procedure fa assistance.	ils, it is recommended to contact My Oracle Support (MOS) and ask for		
1.	Install TVOE application	 If the PMAC is NOT hosted on the failed rack mount server, execute IPM Servers Using PMAC Application from reference [8]. 		
		 If the PMAC is hosted on the failed rack mount server, execute Installing TVOE on the Management Server from reference [8]. 		
2.	Establish network	• If the PMAC is NOT hosted on the failed rack mount server, skip this step .		
	connectivity	 If the PMAC is hosted on the failed rack mount server, execute TVOE Network Configuration, steps 1-11, from reference [8]. 		
		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.		
3.	Restore TVOE backup ISO	If using NetBackup to restore the TVOE backup ISO image, then execute this step; otherwise, skip this step.		
	image to the TVOE host (NetBackup)	 Execute Application NetBackup Client Installation Procedures from reference [8]. 		
	(Netbackup)	 Interface with the NetBackup master server and initiate a restore of the TVOE backup ISO image. 		
		<i>Note:</i> Once restored, the ISO image is in <i>/var/TKLC/bkp/</i> on the TVOE server.		

Procedure 19. Restore TVOE Configuration from Backup Media

4.	Transfer TVOE	Restore TVOE backup ISO using SCP.				
	backup ISO image to the TVOE host	Using the IP of the TVOE host, transfer the backup ISO image to the TVOE.				
		Linux:				
		From the command line of a Linux machine use this command to copy the backup ISO image to the TVOE host:				
		<pre># scp <path_to_image> tvoexfer@<tvoe_ip>:backup/</tvoe_ip></path_to_image></pre>				
		where <path_to_image> is the path to the backup ISO image on the local system and <tvoe_ip> is the TVOE IP address.</tvoe_ip></path_to_image>				
		Notes:				
		• If the IP is an IPv4 address, then <tvoe_ip> is a normal dot-decimal notation (for example, 10.240.6.170).</tvoe_ip>				
		• 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.</tvoe_ip>				
		• 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.				
		IPv4 Example:				
		<pre># scp /path/to/image.iso tvoexfer@10.240.6.170:backup/</pre>				
		IPv6 Example:				
		<pre># scp /path/to/image.iso</pre>				
		<pre>tvoexfer@[fe80::21e:bff:fe76:5e1c%control]:backup/</pre>				
		Windows:				
		Use WinSCP to copy the Backup ISO image into the /var/TKLC/bkp directory. Refer to [8], theUsing WinSCP procedure, to copy the backup image to the customer system.				
5.	TVOE Server: Login	Establish an SSH session to the TVOE server and login as admusr .				



Procedure 19. Restore TVOE Configuration from Backup Media

7.	Monitor TVOE	1. Wait for the restore to complete.
	buokup proceed	System Busy
		Restoring This may take a while.
		Please wait
		Note: This typically takes loss than 5 minutes
		nessage
		Restore completed successfully!
		Press any key to continue
		Press any key to continue
		2. Exit platcfg.
8.	TVOE Server:	Exit the Restore Backup Menu.
	Exit restore	lqqu Restore Backup Menu tqqk
	раскир тепи	X X X
		x View Table of Contents a x
		x Change Restore Dir a x
		x Restore Backup Archive x
		wddadadadadadadadadad
		lu Backup and Restore Menu tqk
		x Backup Platform(CD/DVD) x
		x Backup Platform(USB) a x
		x Restore Platform a x
		x Restore USB Archive x
		x x
		madaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Procedure 19. Restore TVOE Configuration from Backup Media



Procedure 19. Restore TVOE Configuration from Backup Media

Pro	cedure 19. Restore	TVOE Configuration from Backup Media
10. 	TVOE Server: Wait for restart to successfully	1401715649: Upstart Job TKLChpacucli: started
	complete	1401/15649: Upstart Job alarmMgr: started ####################################
		1401715649: Upstart Job tpdProvd: started ####################################
		Oracle Linux Server release 6.5 Kernel 2.6.32-431.11.2.el6prerel7.0.0.0.0_86.3.0.x86_64 on an x86_64
		1401715649: Upstart Job syscheck: started ####################################
		1401715650: Upstart Job TKLCsnmp-subagent: started ####################################
		1401715651: Upstart Job ntdMgr: started ####################################
		Oracle Linux Server release 6.5 Kernel 2.6.32-431.11.2.el6prerel7.0.0.0.0_86.3.0.x86_64 on an x86_64
	TV05 0	hostname71e968a495e6 login:
11. □	Verify storage	1. Login as admusr .
	pools are active	2. Verify all storage pools are listed and are in the active state:
		<pre>\$ sudo virsh -c "qemu:///system" pool-list [admusr@5010441-TVOE ~]\$ sudo virsh -c "qemu:///system" pool-li Name State Autostart</pre>
		 vgguests active yes

[admusr@5010441-TVOE ~]\$

Note: If any storage pools are missing or inactive, contact My Oracle Support (MOS).

Procedure 19. Restore I VOE Configuration from Backup Media

12. □	TVOE Server: Enable HIDS (Optional)	Note: Enabling HIDS is optional. This step is skipped if HIDS is not required to be enabled.
		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:
		<pre>\$ /usr/TKLC/plat/bin/hidsMgr -initialize</pre>
		LOG: HIDS monitoring has been Initialized
		HIDS baseline has been initialized
		<pre>\$ /usr/TKLC/plat/bin/hidsMgrenable</pre>
		HIDS monitoring has successfully been enabled
		New State: ENABLED
		<pre>\$ /usr/TKLC/plat/bin/hidsMgrupdateall</pre>
		HIDS baseline has successfully been updated



Procedure 19. Restore TVOE Configuration from Backup Media

Appendix H. Restore PMAC from Backup

Procedure 20. Restore PMAC from Backup Media

	This procedure p	rovides steps to restore the PMAC application configuration from backup media.	
S T	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.		
P #	If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1.	Deploy the PMAC guest	Execute Install PMAC from reference [8].	
2.	PMAC: Login	Establish an SSH session to the PMAC server and login as admusr .	
3.	Restore PMAC Backup image to the PMAC host	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, admusr@[<ipv6addr>]:/<file> Note: Execute the scp command from the recovered PMAC and the backup file is pulled/retried from the backup location. \$ sudo /usr/bin/scp -p \ admsur@<remoteserver>:/var/TKLC/smac/backup/*.pef \ /var/TKLC/smac/backup 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.</remoteserver></file></ipv6addr>	
4.	PMAC : Verify no Alarms are	Verify no alarms are present. \$ sudo /usr/TKLC/plat/bin/alarmMgralarmStatus	
5.	Restore the	1. Restore the PMAC data from backup.	
	FMAC Data from Backup	<pre>\$ sudo /usr/TKLC/smac/bin/pmacadm restore PM&C Restore been successfully initiated as task ID 1</pre>	
		2. Check the status of the background task.	
		<pre>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</pre>	
		Note: The result eventually displays PMAC Restore successful.	

-		-	
6.	PMAC GUI:	1. Op	en web browser and navigate to the PMAC GUI.
	Login	2. Lo	gin as PMACadmin user:
		http	s:// <pmac_network_ip></pmac_network_ip>
			ORACLE
		Oracle	e System Login Tue Jun 7 13:49:06 2016 EDT
			Log In Enter your username and password to log in
			Lisername:
			Descued
			Password:
			Change password
			Log In
		Unau	thorized 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.
7.	PMAC GUI:	1. Na	vigate to Task Monitoring.
	Verify restore task completed	2. Ve	rify the restore background task completed successfully.
		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.
		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.

Procedure 20. Restore PMAC from Backup Media

8.	PMAC GUI: Verify system inventory	 Navigate to Hardware > System Inventory. Main Menu Hardware System Inventory Cabinet 1 Cabinet 2 Cabinet 101 Cabinet 101 FRU Info Verify previously provisioned enclosures are present.
9.	PMAC: Verify PMAC	Perform a system health check on the PMAC. \$ sudo /usr/TKLC/plat/bin/alarmMgralarmStatus This command should return no output on a healthy system. \$ sudo /usr/TKLC/smac/bin/sentry status All processes should be running, displaying output similar to the following: PM&C Sentry Status
10.	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 20. Restore PMAC from Backup Media

Procedure 21. Restore PMAC from Backup Server

S T P #	This procedure pro Prerequisite : TV Check off ($$) each step number. If this procedure fa assistance.	vides steps to restore the PMAC application configuration from backup server. (OE management server has been restored. step as it is completed. Boxes have been provided for this purpose under each ils, it is recommended to contact My Oracle Support (MOS) and ask for
1.	Deploy the PMAC quest	Execute Install PMAC from reference [8].
	5	Note: This procedure is for restoring from a NetBackup server, so specify the appropriate options when deploying PMAC for use with NetBackup.
2.	PMAC TVOE Host: Login	Establish an SSH session to the PMAC TVOE Host, login as admusr .
3.	PMAC TVOE	1. On the TVOE host, execute this command:
	PMAC guest console	\$sudo virsh list
		This produces a listing of currently running virtual machines.
		Id Name State
		1 Oahu-PMAC running
		 Find the VM name for your PMAC and note its ID number in the first column.
4.	Connect to	On the TVOE host, execute this command:
	console of the VM using the VM number obtained in step 3	<pre>\$sudo virsh console <pmac-vmid></pmac-vmid></pre>
		Where PMAC-VMID is the VM ID you obtained in step 3:
		[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.el6prerel7.0.3.0.0_86.37.0.x86_64 on an x86_64
		Oahu-PMAC login:
		You are now connected to the PMAC guest console.
		If you wish to return to the TVOE host, you can exit the session by pressing CTRL +].

5. PMAC : F	PMAC: Prepare	Execute these commands on the PMAC.
transfer ti appropria backup fr backup so Disable ip and enab TPD plato backup configura menus	the the ate rom server. ptables, ole the cfg ation	<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: NBInit 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: NBVerifyEnv to visible=1 Modified menu NBVerify show Set the following menus: NBVerifyEnv to visible=1 Modified menu NBVerify show Set the following menus: NBVerify to visible=1=</pre>

_		
6.	PMAC: Verify the TPD platcfg backup menus are visible, then exit the TPD platcfg Utlility	Verify the TPD platcing backup menus are visible.
		\$ sudo /bin/su - platcfg
		Main Menu Maintenance Diagnostics Server Configuration Network Configuration Remote Consoles NetBackup Configuration Exit
		<i>Note:</i> In the example image above of the TPD platcfg utility Main Menu the backup menu is identified as NetBackup Configuration .
7.	PMAC: Verify	Verify the iptables rules are disabled on the PMAC guest.
	the iptables rules are disabled on the PMAC quest	\$ sudo /sbin/iptables -nL
		INPUT (policy ACCEPT)
	<u>j</u>	target prot opt source destination
		Chain FORWARD (policy ACCEPT)
		target prot opt source destination
		Chain OUTPUT (policy ACCEPT)
		target prot opt source destination
8.	PMAC : Install backup utility	Execute PMAC NetBackup Client Installation and Configuration from reference [8] starting at step 4.
	client software on the PMAC guest	<i>Note:</i> The Initialize PMAC Application and Configure PMAC Application prerequisites can be ignored.
9.	Backup server:	This step is likely executed by customer IT personnel.
	verify appropriate PMAC backup exists	 Log into the backup server as the appropriate user using the user password.
		 Execute the appropriate commands to verify the PMAC backup exists for the desired date.
		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.
		<i>Note:</i> 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.

Procedure 21. Restore PMAC from Backup Server

10	Backup Server	This step is likely executed by customer IT personnel
	Verify appropriate PMAC backup exists	
		 Log into the backup server as the appropriate user using the user password.
		 Execute the appropriate commands to verify the PMAC backup exists for the desired date.
		 Execute the appropriate commands to restore the PMAC management server backup for the desired date.
		<i>Note:</i> 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.
11.	PMAC: Verify no	Verify no alarms are present.
	alarms are present	<pre>\$ sudo /usr/TKLC/plat/bin/alarmMgralarmStatus</pre>
12.	Restore the PMAC data from backup	1. Restore the PMAC data from backup.
		\$ sudo /usr/TKLC/smac/bin/pmacadm restore
		DM&C Restore been successfully initiated as task ID 1
		That Restore been successfully interaced as cask if i
		Check the status of the background task:
		<pre>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</pre>
		<i>Note:</i> The result eventually displays PMAC Restore successful.

Procedure 21. Restore PMAC from Backup Server

13.	PMAC GUI:	1. Open web browser and navigate to the PMAC GUI.
	Login	
		2. Login as PMACadmin user:
		ORACLE
		Oracle System Login
		Tue Jun 7 13:49:06 2016 EDT
		Log In Enter your username and password to log in
		Username:
		Password:
		Change password
		Log In
		Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.
		Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
		Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.
14.	PMAC GUI:	1. Navigate to Task Monitoring.
	Verify restore	2. Verify the restore background task completed successfully.
		<i>Note:</i> 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.
		<i>Note:</i> 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.

Procedure 21. Restore PMAC from Backup Server

15.	PMAC GUI: Verify system inventory	 1. Navigate to Hardware > System Inventory. Main Menu Hardware System Inventory Cabinet 1 Cabinet 2 Cabinet 101 Cabinet 101 Cabinet Undesignated FRU Info 2. Verify previously provisioned enclosures are present
16.	PMAC: Verify PMAC	<pre>Perform a system health check on the PMAC. \$ sudo /usr/TKLC/plat/bin/alarmMgralarmStatus This command should return no output on a healthy system. \$ sudo /usr/TKLC/smac/bin/sentry status All processes should be running, displaying output similar to the following: PM&C Sentry Status</pre>
17. □	PMAC : Add ISO images to the PMAC	Re-add any needed ISO images to the PMAC by executing procedure Load Application and TPD ISO onto PMAC Server from reference [8].

Procedure 21. Restore PMAC from Backup Server

Appendix I. Restore Provisioning Database

S T E	This procedure restores the SDS provisioning database. Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.												
P #	If this procedure assistance.	rocedure fails, it is recommended to contact My Oracle Support (MOS) and ask for nce.											
1.	Primary SDS NOAM GUI: Log into the primary SDS NOAM GUI	Log into prir	Log into primary SDS NOAM GUI using its static IP (not the VIP).										
2.	Primary SDS NOAM GUI: Place the newly recovered standby NOAM into forced standby	 Navigat Click Ec Click Ec Move the Main Menu: Modifying HA Hostname rlghnc-sds-NO-a rlghnc-sds-NO-b 	e to Status dit. he newly reco Status & Mana A attributes Max Allowed HA Ro Active	& Manag overed sta age -> HA [Description The maximum The maximum	e > H, andby Edit] h desired H	A. Serve	er to fo r righnc-so r righnc-so	brced is-NO-a is-NO-b is-QS	Stand	dby.			
3.	Primary SDS NOAM GUI: Restore provisioning data	 Navigat Select t Main Menu: Statu Filter Infor Network Element 	e to Status he active NC s & Manage -> Dat Tasks ~	& Manag DAM and abase	e > Da click F	ataba Resto	Se. re.	DB Level	OAM Repi	SIG Repl Status	1on Mar 20 : Repl Status	L6:38:03 2017 Repl Audit Status	utc
		NO_RLGHNC	rlghnc-sds-NO-b	Network OAM&P	Active	N/A	Normal	7261273	Normal	NotApplica	Allowed	NotApplica	-
		NO_MRSVNC	mrsvnc-sds-NO-b	Network OAM&P	Active	N/A	Normal	7261273	Normal	ble	Allowed	ble Noveppilca	4
		SDS_SO_Nassau	nassau-dp-2	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplica	
		SDS_SO_Turks	turks-dp-2	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplica	
		SDS_S0_Turks	turks-sds-so-b	System OAM	Standby	N/A	Normal	7261273	Normal	NotApplica	Allowed	NotApplica	
		SDS_SO_Nassau	nassau-sds-so-b	System OAM	Active	N/A	Normal	7261273	Normal	NotApplica	Allowed	NotApplica	
		NO_RLGHNC	righnc-sds-NO-a	Network OAM&P	Standby	N/A	Normal	7261273	Normal	NotApplica	Allowed	NotApplica	
		SDS SO Freenart	freenort-rin-?	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplica	T
		Disable Provisioning	Report Inhibit/Allow Rep	lication Backup	Compare.	. Restore	Man A	udit Resu	me Auto Audit				
						· · · · ·	И.	- Copyright ©	2010, 2017, 0	Dracle and/or	ts affiliates.	All rights reser	ved.

-		5
		3. Select the Provisioning backup file from the list (which was previously placed in the /var/TKLC/db/filemgmt/backup directory in step 5 of section 2.6.2) and click OK .
		<i>Note:</i> You must use a provisioning only backup file. Combined backup files contain configuration and provisioning data and cause
		catastrophic issues, which could lead to a complete re-installation.
		Main Menu: Status & Manage -> Database [Restore]
		Database Restore
		Select archive to Restore on server: mrsvnc-sds-NO-a
		 backup/Backup.sds.rlghnc-sds-NO-b.Configuration.NETWORK_OAMP.20170316_021512.AUTO.tar.gz backup/Backup.sds.rlghnc-sds-NO-b.Provisioning.NETWORK_OAMP.20170316_031512.AUTO.tar.gz backup/Backup.sds.rlghnc-sds-NO-b.Configuration.NETWORK_OAMP.20170317_021512.AUTO.tar.gz backup/Backup.sds.rlghnc-sds-NO-b.Provisioning.NETWORK_OAMP.20170317_021512.AUTO.tar.gz
		Archive * O backup/Backup.sds.rlghnc-sds-NO-b.Configuration.NETWORK_OAMP.20170318_021512.AUTO.tar.gz O backup/Backup.sds.rlghnc-sds-NO-b.Provisioning.NETWORK_OAMP.20170318_031511.AUTO.tar.gz O backup/Backup.sds.rlghnc-sds-NO-b.Configuration.NETWORK_OAMP.20170319_021512.AUTO.tar.gz O backup/Backup.sds.rlghnc-sds-NO-b.Provisioning.NETWORK_OAMP.20170319_031511.AUTO.tar.gz O backup/Backup.sds.rlghnc-sds-NO-b.Provisioning.NETWORK_OAMP.20170319_031511.AUTO.tar.gz
		C backup/Backup.sds.righnc-sds-NO-b.Provisioning.NETWORK_OAMP.20170320_021512.A010.tar.gz
		4. Verify compatibility and click OK to restore.
		Main Menu: Status & Manage -> Database [Restoreconfirm]
		Database Restore Confirm
		Compatible archive.
		The selected database came from righnc-sds-NO-b on 03/17/2017 at 02:15:12 EDT and contains the following comment: Nightly Archive Contents Configuration data Database Compatibility
		Confirm archive "backup.Backup.sds.rlghnc-sds-NO-b.Configuration.NETWORK_OAMIP20170317_021512.AUTO.tar.gz" to Restore on server: rlghnc-sds-NO-b
		Force Restore? Force restore on righnc-sds-NO-b, despite compare errors.
		OK Cancel
4.	Primary SDS	1. Wait 60 seconds for the restore to begin.
	NOAM GUI: Wait for the restore to	 Monitor the Info tab under the Status & Manage > Database screen and look for the following message:
	begin and track progress until	Restore on <active_no_hostname> status MAINT_IN_PROGRESS.</active_no_hostname>3. Wait for the restore to complete by looking for the following message:
	complete	Success: - Restore on rlghnc-sds-NO-b status MAINT_CMD_SUCCESS. Success
		<i>Note:</i> Refresh the Info tab manually to see updated status by navigating to Status & Manage > Database again and selecting the Info tab.

5.	Primary SDS NOAM GUI: Uninhibit servers	Uninhibit all servers in the following staggered arrangement: 1. Uninhibit active NOAM.											
		Refresh Level d 2. Uninhib	/monitor the isplays for the it standby f	e Status & he active N NOAM/Que	Mana IOAM ery ser	i ge > l .ver.	Datab	ase s	creen	until a	a valio	DB	
		Refresh/monitor the Status & Manage > Database screen until a valid DB Level displays for the standby NOAM/Query server. 3. Uninhibit active SOAMs.											
		 Refresh/monitor the Status & Manage > Database screen until a valid DB Level displays for the active SOAMs. 4. Uninhibit standby SOAMs/DPs. 											
		Refresh Level d	/monitor the isplays for t	e Status & he standby	Mana / SOA	ige > I Ms/DF	Datab °s.	ase s	creen	until a	a valio	DB	
6. □	Recover Pdbrelay (if needed)	Verify whether PDB Relay is Enabled by following the instructions in Appendix J Recover PDB Relay.											
7.	Primary SDS NOAM GUI:	Navigate to Main Menu: State	Status & M us & Manage -> Da	anage > [ntabase	Databa	ase an	d clic	k Ena	ble Pr	ovisio	oning		-c
	Enable	Filter* 👻 Info* 👻	Tasks 💌										
	provisioning	Network Element	Server	Role	OAM Max HA Role	Application Max HA Role	Status	DB Level	OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status	
		SDS_SO_Turks	turks-sds-so-a	System OAM	Active	N/A	Normal	7261273	Normal	NotApplica ble	Allowed	NotApplica	
		NO_RLGHNC	righnc-sds-NO-b	Network OAM&P	Active	N/A	Normal	7261273	Normal	NotApplica ble	Allowed	NotApplica ble	
		NO_MRSVNC	mrsvnc-sds-NO-b	Network OAM&P	Active	N/A	Normal	7261273	Normal	NotApplica ble	Allowed	NotApplica	
		SDS_SO_Nassau	nassau-dp-2	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplica	1
		SDS_SO_Turks	turks-dp-2	MP	Active	N/A	Normal	7261273	Normal	Normal	Allowed	NotApplica ble	
		SDS_SO_Turks	turks-sds-so-b	System OAM	Standby	N/A	Normal	7261273	Normal	NotApplica ble	Allowed	NotApplica ble	
		SDS_SO_Nassau	nassau-sds-so-b	System OAM	Active	N/A	Normal	7261273	Normal	NotApplica ble	Allowed	NotApplica ble	
		NO RIGHNO	rlohnc-sids-NO-a	Network OAM&P	Standby	N/A	Normal	7261273	Normal	NotApplica	Allowed	NotApplica 💂	·
		Enable Provisioning	Report Inhibit/Allow B	Dealum Dealum									

8.	 Primary SDS NOAM GUI: Remove NO from forced standby 	 Navigate Select the HA Role Main Menu: 3 	to Status & Ma e server, which to Active, and Status & Manag	anage > HA and click Edit. was moved to forced standby in ste click OK. je -> HA [Edit]	ep 2, change Max
		Modifying HA	attributes Max Allowed HA Role	Description	
		rlghnc-sds-NO-a	Active	The maximum desired HA Role for righnc-sds-NO-a	
		rlghnc-sds-NO-b	Active	The maximum desired HA Role for righnc-sds-NO-b	
		rlghnc-sds-QS	Observer 💌	The maximum desired HA Role for righnc-sds-QS	

Appendix J. Recover PDB Relay

Procedure 23. Recover PDB Relay

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

Appendix K. SNMP Configuration

Procedure 24. Configure SNMP

s	This workaround traps configurati	workaround configures SNMP with SNMPv2c and SNMPv3 as the enabled versions for SNMP configuration since PMAC does not support SNMPv3.				
T E	Check off $()$ eastep number.	ch step as it is completed. Boxes have been provided for this purpose under each				
Р #	If this procedure	e fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.				
1.	(Workaround)	<i>Note:</i> This workaround step should be performed only in the following cases:				
	GUI: Login	1. If SNMP is not configured.				
		 If SNMP is already configured and SNMPv3 is selected as enabled version. 				
		<i>Note:</i> 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.				
		 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:				
		http:// <primary_noam_vip_ip_address></primary_noam_vip_ip_address>				
		3. Log into the NOAM GUI as the guiadmin user:				
		ORACLE				
		Oracle System Login Tue Jun 7 13:49:06 2016 EDT				
		Log In Enter your username and password to log in				
		Username:				
		Password:				
		Change password				
		Log In				
		Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.				
		Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.				
		Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.				

Procedure 24	I. Configure	SNMP
--------------	--------------	------

2.		1. Navigate to Administration > Remote Servers > SNMP Trapping.				
	GUI.	E 🚇 Main Menu				
	Configure	🖻 😋 Administration				
	system-wide	📲 General Options				
	SNMP trap					
	receiver(s)	Software Management				
	10001/01(0)					
		SMP Transing				
		Data Export				
		DNS Configuration				
		2. Select the Server Group tab for SNMP trap configuration:				
		Main Menu: Administration -> Remote Servers				
		ZombieDRNOAM ZombieSOAM ZombieSOAM				
		Name				
		3. Type the IP address or hostname of the Network Management Station (NMS)				
		where you want to forward trans. This IP should be reachable from the				
		NOAMP's XMI network. If already configured SNMP with SNMPy3 as enabled				
		vorsion 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				
		ue Clobal				
		Configuration Mode "				
		Hanager 1				
		Manager 2				
		5. Set the Enabled Versions as SNMPv2c and SNMPv3 .				
		Enabled Versions SNMPv2c and SNMPv3				
		6. Check I raps Enabled checkboxes for the Manager servers being configured.				
		Manager 1 Manager 2				
		Traps Enabled Manager 3				
		Manager 4				
		Manager 5				
		7. Type the SNMP Community Name.				
		SNMDv2c Read Only Community Name				
		SNMPv2c Read-Write Community Name				
		8 Leave all other fields at their default values				
		9. Ulick UK .				

Procedure 24. Configure SNMP

3.	NOAMP VIP: Enable traps from individual servers (optional)	 Note: By default SNMP traps from MPs are aggregated and displayed at the active NOAMP. If, instead, you want every server to send its own traps directly to the NMS, then execute this procedure. This procedure requires all servers, including MPs, to have an XMI interface on which the customer SNMP target server (NMS) is reachable. Navigate to Administration > Remote Servers > SNMP Trapping.
		 Main Menu Administration General Options Access Control Software Management Software Management Enabled checkbox is marked. Traps from Individual Servers Click Apply and verify the data is committed.
4.	PMAC GUI: Update the TVOE host SNMP community string	 Establish an SSH session to the PMAC. Login as admusr user: Update the TVOE hos community string with this command: \$ sudo pmaccli setCommStraccessType=rwcommStr=<site specific="" value=""></site> Note: When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest on the PMAC control network are updated. All those servers that match the existing Site Specific Community String are not updated again until the string name is changed.

Appendix L. Backup Directory

Procedure 25. Backup Directory

S	This procedure checks and creates the backup directory.					
Т	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each					
Ε	step number.					
Ρ	If this procedure	fails	s, it is recommended to contact My Oracle Support (MOS) and ask for assistance.			
#						
1. □	NOAM/SOAM VIP Console:	1.	Execute this command an active NOAM/SOAM server console (accessed using the VIP) and compare the output.			
	backup		<pre>\$ cd /var/TKLC/db/filemgmt/</pre>			
	directory		\$ ls -ltr			
	exists	2.	Look for the backup directory in the output.			
		3.	Make sure the directory is already created with correct permission. The directory looks like this:			
			drwxrwx 2 awadmin awadm 4096 Dec 19 02:15 backup			
		4.	If the directory is already there with correct permissions, then skip steps 2 and 3.			
		5.	If directory does not have the correct permissions, then go to step 3.			
2.	NOAM/SOAM	1.	Go to the backup directory location.			
	Create		cd /var/TKLC/db/filemgmt/			
	backup directory	2.	Create backup directory.			
			\$ mkdir backup			
		3.	Verify directory has been created.			
			<pre>\$ ls -ltr /var/TKLC/db/filemgmt/backup</pre>			
			<i>Note:</i> A No such file or directory error message should not display. The directory should show as empty with the total as 0 for content.			

Procedure 25. Backup Directory

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

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

Beginning with TPD 7.7.0.0.0-88.68.0, the cipher list is restricted to allow only a limited number of ciphers for ssh access to the servers. As a result, netConfig backup and restore operations are not functional with Cisco switches (3020, 4948s), as these switches use other ciphers. Executing these commands with the restricted ciphers would fail as shown below:

[admusr@p5-pmac ~]\$ /usr/bin/sudo /usr/TKLC/plat/bin/netConfig -device=3020_ip backupConfiguration service=ssh_ip filename=backup Command failed: backupConfiguration Error saving to SSH service [admusr@p5-pmac ~]\$

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

Procedure 26. Turn off cipher list before

backupConfiguation/restoreConfiguration/upgradeFirmware command

STEP #	Procedure	Description				
This proc before the <i>Check of</i> number. If this pro	This procedure prepares the PM&C to avoid the cipher mismatch issue with Cisco switches. This is performed before the netConfig backup, restore or upgrade operations. <i>Check off (v) each step as it is completed.</i> Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.					
	Turn off cipher list	<pre>From the PMAC shell enter the following: /usr/bin/sudo /bin/vi /etc/ssh/sshd_config Add # in the beginning of the following three lines to comment them out, the result is: #Ciphers aes256-ctr,aes192-ctr,aes128-ctr #MaxAuthTries 4 #LoginGraceTime 1m</pre>				
2	Restart sshd	/usr/bin/sudo service sshd restart				
STEP #	Procedure	Description				
--------	--	--				
3	Run the netConfig backupConfigu ation/restoreCo nfiguration/upg radeFirmware command	<pre>For a backup operation: [admusr@pmac ~]\$ /usr/bin/sudo /usr/TKLC/plat/bin/netConfig backupConfigurationdevice=<switch_name> service=<ssh_service> filename=<switch_name>-backup For a restore operation: [admusr@pmac ~]\$ /usr/bin/sudo /usr/TKLC/plat/bin/netConfig restoreConfigurationdevice=<switch_name> service=<ssh_service> filename=<switch_name>-backup For a upgrade operation: [admusr@pmac ~]\$ /usr/bin/sudo /usr/TKLC/plat/bin/netConfig</switch_name></ssh_service></switch_name></switch_name></ssh_service></switch_name></pre>				
		<pre>[admusr@pmac ~]\$ /usr/bin/sudo /usr/TKLC/plat/bin/netConfig upgradeFirmwaredevice=<switch_name> service=<ssh_service> filename=<cisco ios=""></cisco></ssh_service></switch_name></pre>				

Procedure 27. Resume cipher list after backupConfiguation/restoreConfiguration/upgradeFirmware command

STEP #	Task	Description	
This procedure restores the PM&C restricted cipher list after perform the netConfig backup, restore or upgrade operations.			
Check off ($\sqrt{2}$) 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	Resume the cipher list	<pre>From the PMAC shell enter the following: /usr/bin/sudo /bin/vi /etc/ssh/sshd_config Uncomment the three lines: Ciphers aes256-ctr,aes192-ctr,aes128-ctr MaxAuthTries 4 LoginGraceTime lm</pre>	
2	Restart sshd	/usr/bin/sudo service sshd restart	

Appendix N. My Oracle Support (MOS)

My Oracle Support

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

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

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

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

Emergency Response

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

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

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

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

Locate Product Documentation on the Oracle Help Center

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

- 1. Access the Oracle Help Center site at http://docs.oracle.com.
- 2. Click Industries.
- 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.