Oracle[®] Communications Diameter Signaling Router

C-Class Disaster Recovery Guide Release 8.5.1 F51111-01

December 2021



Oracle Communications DSR C-Class 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			6
	1.1	Purpo	se and Scope	6
	1.2	Refere	ences	6
	1.3	Acron	yms	6
	1.4	Termi	nology	7
	1.5	Optior	nal Features	8
2.	Gen	eral D	escription	8
	2.1	Comp	lete Server Outage (All Servers)	9
	2.2	Partia	I Server Outage with One NOAM Server Intact and Both SOAMs Failed	. 10
	2.3	Partia	I Server Outage with Both NOAM Servers Failed and One SOAM Server Intact	. 10
	2.4	Partia	I Server Outage with NOAM and One SOAM Server Intact	. 10
	2.5	Partia	I Service Outage with Corrupt Database	. 10
3.	Pro	cedure	Overview	. 10
	3.1	Requi	red Materials	. 10
	3.2	Disast	ter Recovery Strategy	. 11
4.	Disa	aster R	ecovery Procedure	. 13
	4.1	Recov	very Scenario 1 (Complete Server Outage)	. 13
	4.2	Recov Failed	very Scenario 2 (Partial Server Outage with One NOAM Server Intact and ALL SOAMs	
	4.3	Recov Serve	very Scenario 3 (Partial Server Outage with All NOAM Servers Failed and One SOAM r Intact)	. 68
	4.4	Recov Intact)	very Scenario 4 (Partial Server Outage with One NOAM Server and One SOAM Server) 89	
	4.5	Recov	very Scenario 5 (Both NOAM Servers Failed with DR-NOAM Available)	105
	4.6	Recov	very Scenario 6 (Database Recovery)	112
		4.6.1	Recovery Scenario 6: Case 1	112
		4.6.2	Recovery Scenario 6: Case 2	116
5.	Res	olving	User Credential Issues after Database Restore	120
	5.1	Resto	re a Deleted User	120
	5.2	Keep	a Restored User	120
	5.3	Remo	ve a Restored User	122
	5.4	Resto	re a Modified User	123
	5.5	Resto	re an Archive that does not contain a Current User	123
6.	IDIH	l Disas	ter Recovery	128
Ар	pend	lix A.	DSR Database Backup	133
Ар	ppendix B. Recover/Replace Failed 3 rd Party Components (Switches, OAs)			
Ар	pend	lix C.	Inhibit A and B Level Replication on C-level Servers	141

Appendix D.	Un-Inhibit A and B Level Replication on C-level Servers	142
Appendix E. and Spare	Inhibit A and B Level Replication on C-level Servers (When Active, Standby, SOAMs are Lost)	144
Appendix F. and Spare	Un-Inhibit A and B Level Replication on C-Level Servers (When Active, Standby SOAMs are Lost)	146
Appendix G.	Restore TVOE Configuration from Backup Media	149
Appendix H.	Restore PMAC from Backup	157
Appendix I.	Configure TVOE Hosts	166
Appendix J.	Create NOAM/SOAM Virtual Machines	177
Appendix K.	SNMP Configuration	185
Appendix L.	Backup Directory	189
Appendix M. TPD Ciphe	netConfig backupConfiguration/restoreConfiguration/upgradeFirmware with r Change	191
Appendix N.	DSR Database Restore	193
Appendix O.	My Oracle Support (MOS)	195

List of Tables

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

List of Figures

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

List of Procedures

Procedure 1.	Recovery Scenario 1	14
Procedure 2.	Recovery Scenario 2	44
Procedure 3.	Recovery Scenario 3	69
Procedure 4.	Recovery Scenario 4	89
Procedure 5.	Recovery Scenario 5	105
Procedure 6.	Recovery Scenario 6 (Case 1)	113
Procedure 7.	Recovery Scenario 6 (Case 2)	116
Procedure 8.	Keep Restored User	120
Procedure 9.	Remove the Restored User	122
Procedure 10.	Restore an Archive That Does Not Contain a Current User	124

Procedure 11.	IDIH Disaster Recovery Preparation	28
Procedure 12.	IDIH Disaster Recovery (Re-Install Mediation and Application Servers)	30
Procedure 13.	DSR Database Backup13	3
Procedure 14.	Recover a Failed Aggregation Switch (Cisco 4948E/4948E-F)13	6
Procedure 15.	Recover a Failed Enclosure Switch (Cisco 3020)13	8
Procedure 16.	Recover a Failed Enclosure Switch (HP 6120XG , HP 6125XLG, HP 6125G)13	8
Procedure 17.	Recover a Failed Enclosure OA	1
Procedure 18.	Inhibit A and B Level Replication on C-level Servers	1
Procedure 19.	Un-Inhibit A and B Level Replication on C-level Servers	2
Procedure 20.	Inhibit A and B Level Replication on C-level Servers	4
Procedure 21.	Un-Inhibit A and B Level Replication on C-Level Servers	6
Procedure 22.	Restore TVOE Configuration from Backup Media14	9
Procedure 23.	Restore PMAC from Backup Media15	57
Procedure 24.	Restore PMAC from Backup Server15	;9
Procedure 25.	Configure TVOE	6
Procedure 26.	Create NOAM Guest VMs17	7
Procedure 27.	Create SOAM Guest VMs	31
Procedure 28.	Configure SNMP	5
Procedure 29.	Backup Directory	9
Procedure 30.	Turn Off Cipher List Before backupConfiguation/restoreConfiguration/upgradeFirmware Command)1
Procedure 31.	Resume Cipher List After backupConfiguation/restoreConfiguration/upgradeFirmware Command	92
Procedure 32.	DSR Database Restore	13

1. Introduction

1.1 Purpose and Scope

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

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

1.2 References

- [1] TPD Initial Product Manufacture
- [2] Platform Configuration Procedure Reference
- [3] CPA Feature Activation Procedure
- [4] DSR Mediation Feature Activation Procedure
- [5] DSR FABR Feature Activation Procedure
- [6] DSR RBAR Feature Activation Procedure
- [7] DSR MAP-Diameter IWF Feature Activation Procedure
- [8] DSR C-Class Software Installation and Configuration Procedure Part 2/2
- [9] DSR GLA Feature Activation Procedure
- [10] DSR C-Class Hardware and Software Installation Procedure 1/2
- [11] PMAC Disaster Recovery Guide
- [12] SDS C-Class Disaster Recovery Guide
- [13] DSR PCA Activation Guide
- [14] DSR DTLS Feature Activation Procedure
- [15] DSR Security Guide
- [16] DCA Framework and Application Activation and Deactivation Guide
- [17] DSR/SDS 8.x NOAM Failover User's Guide

1.3 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

Acronym	Definition	
BIOS	BIOS Basic Input Output System	
CD	Compact Disk	
DVD	Digital Versatile Disc	
EBIPA	Enclosure Bay IP Addressing	

Acronym	Definition	
FRU	Field Replaceable Unit	
HP c-Class HP blade server offering		
iLO	Integrated Lights Out manager	
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform	
MSA	Modular Smart Array	
NB	NetBackup	
OA	HP Onboard Administrator	
OS	Operating System (for example, TPD)	
RMS	Rack Mounted Server	
PMAC	Platform Management & Configuration	
SAN	Storage Area Network	
SFTP	Secure File Transfer Protocol	
SNMP	Simple Network Management Protocol	
TPD	Tekelec Platform Distribution	
TVOE	Tekelec Virtual Operating Environment	
VM	Virtual Machine	
VSP	Virtual Serial Port	
IPFE	IP Front End	
PCA	Policy and Charging Application	
IDIH	Integrated Diameter Intelligence Hub	
SDS	Subscriber Database Server	

1.4 Terminology

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).
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.

Term	Definition
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.

1.5 **Optional Features**

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

Feature	Document
Diameter Mediation	DSR Meta Administration Feature Activation Procedure
Full Address Based Resolution (FABR)	DSR FABR Feature Activation Procedure
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation Procedure
Policy and Charging Application (PCA)	DSR PCA Activation Guide
Gateway Location Application (GLA)	DSR GLA Feature Activation Procedure
Host Intrusion Detection System (HIDS)	DSR Security Guide (Section 3.2)
Diameter Custom Applications (DCA)	DCA Framework and Application Activation and Deactivation Guide

2. General Description

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

Table 4.	Recovery	Scenarios
----------	----------	-----------

Procedure	State of NOAM and/or SOAM server(s)
Recovery of the entire network from a total outage	All NOAM servers failed.
Recovery Scenario 1 (Complete Server Outage)	All SOAM servers failed.
	• MP servers may or may not be failed.
Recovery of one or more servers with at least one NOAM server intact	 At least 1 NOAM server is intact and available.
Recovery Scenario 2 (Partial Server Outage with	All SOAM servers failed.
One NOAM Server Intact and ALL SOAMS Failed)	• MP servers may or may not be failed.
Recovery of the NOAM pair with one or more	All NOAM servers failed.
SOAM servers intact	• At least 1 SOAM server out of active, standby,
Recovery Scenario 3 (Partial Server Outage with	spare is intact and available.
Intact)	• MP servers may or may not be failed.

Procedure	State of NOAM and/or SOAM server(s)
Recovery of one or more server with at least one NOAM and one SOAM server intact	 At least 1 NOAM server is intact and available.
Recovery Scenario 4 (Partial Server Outage with One NOAM Server and One SOAM Server Intact)	• At least 1 SOAM server out of active, standby, spare is intact and available.
	• 1 or more MP servers have failed.
Recovery Scenario 5 (Both NOAM Servers Failed	Both NOAM servers 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)
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: Aggregation switches, OA, or 6120/6125/3020 switches refer to Recover/Replace Failed 3rd Party Components (Switches, OAs).

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

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

2.1 Complete Server Outage (All Servers)

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

Database backups are taken from customer offsite backup storage locations (assuming these were performed and stored offsite before the outage). If no backup files are available, the only option is to

rebuild the entire network from scratch. The network data must be reconstructed from whatever sources are available, including entering all data manually.

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

This case assumes at least one NOAM server is intact. All SOAM servers have failed and are recovered using base recovery of hardware and software. Database is restored on the SOAM server and replication recovers the database of the remaining servers.

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

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

2.4 Partial Server Outage with NOAM and One SOAM Server Intact

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

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

2.5 Partial Service Outage with Corrupt Database

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

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

3. Procedure Overview

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

3.1 Required Materials

The following items are needed for disaster recovery:

- 1. A hardcopy of this document and hardcopies of all documents in the reference list
- Hardcopy of all NAPD performed at the initial installation and network configuration of this customer's site. If the NAPD cannot be found, escalate this issue within My Oracle Support (MOS) until the NAPD documents can be located.
- 3. DSR recent backup files: electronic backup file (preferred) or hardcopy of all DSR configuration and provisioning data.
- 4. Latest Network Element report: Electronic file or hardcopy of Network Element report.
- 5. Oracle Tekelec Platform Distribution (TPD) Media (64 bits).
- 6. Platform Management and Configuration (PMAC) ISO or SW.
- 7. DSR CD-ROM (or ISO image file on USB Flash) of the target release.
- 8. TVOE Platform Media (64 bits)
- 9. The xml configuration files used to configure the switches, available on the PMAC server (or PMAC backup)

- 10. The switch backup files taken after the switch is configured, available on the PMAC server (or PMAC backup)
- 11. The network element XML file used for the blades initial configuration.
- 12. The HP firmware upgrade pack (or customer-provided firmware)
- 13. NetBackup Files if they exist. This may require the assistance of the customer's NetBackup administrator.
- 14. PMAC and TVOE backups (If available)
- 15. List of activated and enabled features
- 16. IDIH CD-ROM (or ISO image file on USB Flash) of the target release (If IDIH is being recovered)
- *Note*: For all Disaster Recovery scenarios, we assume that the NOAM Database backup and the SOAM database backup were performed around the same time, and that no synchronization issues exist among them.
- *Note*: NOAMs are deployed using the fast deployment tool from the PMAC. In scenarios where both NOAMs are failed, this fast deployment file is used. In scenarios where only one NOAM is failed, the fast deployment file is NOT used.

SUDO

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

3.2 Disaster Recovery Strategy

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

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



Figure 1. Determining Recovery Scenario

4. Disaster Recovery Procedure

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

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

!!WARNING!!

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 there in the system since the system is DRed. In this case, please refer to Appendix L: Backup Directory for steps to check and create the backup directory.

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

Backup.DSR.HPC02-NO2.FullDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2

4.1 Recovery Scenario 1 (Complete Server Outage)

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

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

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

- Recover the SOAM servers by recovering base hardware/software and/or VM image
 - Recover the SOAM database
 - Reconfigure the DSR Application
- Recover all **MP servers** by recovering base hardware and software
 - Reconfigure the signaling interface and routes on the MPs. The DSR software automatically reconfigures the signaling interface from the recovered database
 - Reference [8] for the applicable DSR software installation/configuration guide if any existing routes need to be altered
- Restart process and re-enable provisioning replication
- *Note*: Any other applications DR recovery actions (SDS and IDIH) may occur in parallel. These actions can/should be worked simultaneously; doing so would allow faster recovery of the complete solution, that is, stale DB on DP servers do not receive updates until SDS-SOAM servers are recovered.

Procedure 1. Recovery Scenario 1

This procedure performs recovery if both NOAM servers are failed and all SOAM servers are failed. This procedure also covers the C-level server failure.

Check off ($\sqrt{}$) 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.	Gather required materials	Gather the documents and required materials listed in Section Required Materials.			
2.	Replace failed equipment	HW vendor to replace the failed equipment.			
3.	Recover PMAC and PMAC TVOE Host: Configure BIOS settings and update firmware	 Configure and verify the BIOS settings by executing procedure Configure the RMS and Blade Server BIOS Settings from reference [10]. Verify and/or upgrade server firmware by executing procedure Upgrade Management Server Firmware from reference [10]. Note: As indicated in [10], repeat for additional rack mount servers if equipped. 			

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

4.	PMAC, TVOE Hosts, and Switch Recovery: Backups available	 This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step. 1. Restore the PMAC TVOE host backup by executing Restore TVOE Configuration from Backup Media. 2. Restore the PMAC backup by executing Restore PMAC from Backup. 3. Recover failed OAs, aggregation, and enclosure switches by referring to Recover/Replace Failed 3rd Party Components (Switches, OAs). 4. Verify/Update blade server firmware by executing Server Blades Installation Preparation from reference [10]. 5. Install TVOE on ALL failed TVOE servers as needed by executing Install TVOE on Blade Servers from reference [10].
		 Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on ALL failed TVOE host blade servers.
		7. Proceed to Step 7.
5.	PMAC, TVOE Hosts, and Switch Recovery: Backups NOT	 This step assumes TVOE and PMAC backups are NOT available. If the TVOE and PMAC have already been restored, skip this step. 1. Execute section Configure and IPM Management Server from reference [10]. 2. Execute Install PMAC from reference [10].
	avaliable	 Execute Configure Aggregation Switches from reference [10] to recover Cisco 4948 aggregation switches, if needed.
		4. Execute Configure PMAC Application from reference [10].
		 Execute HP C-7000 Enclosure Configuration from reference [10] to recover and configure any failed OAs, if needed.
		6. Execute Enclosure and Blades Setup from reference [10].
		7. Execute Configure Enclosure Switches from reference [10] to recover enclosure switches, if needed.
		 Verify/Update Blade server firmware by executing Server Blades Installation Preparation from reference [10].
		 Install and configure TVOE on failed rack mount servers by executing Installing TVOE on Rack Mount Server(s) from reference [10].
		 Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10].

|--|

6.	Execute Fast Deployment File	The backup fdconfig file used during the initial DSR installation is available on the PMAC, if a database backup was restored on the PMAC.				
	for NOAMs	If a backup fast deployment xml is NOT available, execute Configure NOAM Servers from reference [8].				
		If a backup fast deployment xml is already present on the PMAC, execute this procedure:				
		 . Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade has been performed since initial installation). 				
		2. Execute these commands:				
		<pre>\$ cd /usr/TKLC/smac/etc \$ screen \$ screen</pre>				
7		<pre>\$ sudo idconing coninginte=<created_fd_file>.xmi</created_fd_file></pre>				
<i>1</i> .	installation	NE and Server section from reference [8].				
	the first NOAM	 Configure the NOAM server group by executing the Configure the NOAM Server Group section from reference [8]. 				
		<i>Note</i> : Use the backup copy of network configuration data and site surveys (Step 2).				
8.	NOAM GUI:	Log into the NOAM GUI as the guiadmin user:				
	Login					
		UIZALLE				
		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				
		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, 2010, <u>Oracle</u> and/or its amiliates. All rights reserved.				

Procedure 1. Recovery Scenario 1



Procedure 1. Recovery Scenario 1

10.	NOAM GUI: Disable provisioning	 Navigate to Status and Manage > Database. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click Disable Provisioning.
		Disable Provisioning Report Inhibit/Allow 3. A confirmation window displays. Click OK to disable Provisioning. Disable provisioning. Disable provisioning. Are you sure?
		OK Cancel

		-				
11. □	NOAM GUI: Verify the	1. Se	elect the	Active NC	DAM serv	ver and click Compare .
	archive contents and database	lication	Backup	Compare	Restore	
	compatibility	2. Cli of Datab	ick the bi this proc ase Comp	utton for th edure. a re	ne restore	ed database file uploaded as a part of step 9.
		Select a	rchive to com	npare on server	: ZombieNOAI	M1
		Archive	* 🔘 backup/	Backup.dsr.Zom	nbieNOAM1.Co	onfiguratio
		Ok	Cancel			
		3. Ve	erify the	output win	dow mat	ches the screen below.
		Note:	A datal possibl warnin otherw assista	base mism y User col gs are exp ise, stop a ince.	natch reg mpatibilit pected. I and conta	arding the Topology Compatibility and y (due to authentication) display. These f these are the only mismatches, proceed; act My Oracle Support (MOS) to ask for
		Databas	e Archive C	ompare		
		The sel	ected datab	ase came from	n ZombieNOAM	M1 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 Ty The nod	pe Compatik le types are	compatible.		
		Topolog THE TOP Discret - Serv - Serv - Serv	V Compatibi OLOGY IS NO pancies: ver A1860.05 ver A1860.05 ver A0630.23	lity T COMPATIBLE 2 on network 2 on network 38 on network	XMI is in the XM	DRACLE CUSTOMER SERVICES BEFORE RESTORING THIS DATABASE. the current topology but not the selected backup file. the current topology but not the selected backup file. the selected backup file but not the current topology.
		- Serv	ver B2934.01 ver C0422.20	11 on network 00 on network	XMI is in a XMI is in a	the selected backup file but not the current topology. The selected backup file but not the current topology.
		Note:	Archive	e Contents	and Dat	tabase Compatibilities must be the following:
		Archive Contents: Configuration	iguration data.			
			Databa	ase Comp	atibility:	I he databases are compatible.
		Note:	The fol since v databa	lowing is e ve are rest se with jus	expected toring fro st one NC	output for Topology Compatibility Check m an existing backed up database to a DAM:
			Topolo THE T	o gy Comp OPOLOG`	atibility Y SHOUI	LD BE COMPATIBLE MINUS THE NODEID.
		Note:	We are databa	e trying to se. This is	restore a s an exp	backed up database onto an empty NOAM ected text in Topology Compatibility.
		4. If t thi	he verific s proced	cation is si ure.	uccessfu	I, click Back and continue to next step in

Procedure 1. Recovery Scenario 1

Procedure 1. Recovery Scenario 1

12.	Active NOAM:	1. From Status and Manage > Database.
	database	2. Select the Active NOAM server and click Restore .
		are Restore Man A
		3. Select the proper backup provisioning and configuration file.
		Select archive to Restore on server: Zombio
		Archive *
		Ok Cancel
		4. Click OK . The following confirmation screen displays.
		5. If you get errors related to the warnings highlighted in the previous step, that is expected. If no other errors are displayed, mark the Force
		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? V Force Force restore
		Ok Cancel
		Note: After the restore has started, the user is logged out of XMI NO GUI since the restored Topology is old data.

13. □	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				
		Oracle System Login Tue Jun 7 13:49:06 2016				
		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 u 10.0, or 11.0 with support for JavaScript and		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.	NOAM VIP GUI: 1. Wait for 5-10 minutes for the system to stabilize with the new topolo Monitor and					
	confirm database restoral	 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). 				
		<i>Note</i> : Do not pay attention to alarms until all the servers in the system are completely restored.				
		<i>Note</i> : The Configuration and Maintenance information is in the same state it was when backed up during initial backup.				

Procedure 1. Recovery Scenario 1

Procedure 1. Recovery Scenario 1

15.	Active NOAM: Set failed servers to standby	 Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Click Edit. Set the Max Allowed HA Role drop down box to OOS for the failed servers. 					
		Modifying HA at Hostname Ma ZombieNOAM1 A	tributes ax Allowed HA Role	Description			
		ZombieNOAM2 O	IOS	The maximum des			
		ZombieDRNOAM1 Spare The maximum des Observer 00S					
		4. Click OK. Ok Cancel					
16. □	Active NOAM: Login	Log into the recovered active NOAM using SSH terminal as admusr user.					
17.	NOAM VIP GUI: Recover standby NOAM	 VIP GUI: er y NOAM 1. Install the second NOAM server by executing procedure Configure th Second NOAM Server, steps 3-5 and 7, from reference [8]. Note: Execute step 6 if NetBackup is used. 2. If NetBackup is used, then execute Install NetBackup Client from reference [8]. 					

Procedure 1. Recovery Scenario 1

18.	NOAM VIP GUI:	 Navigate to Status and Manage > HA. 							
	Set HA on standby NOAM	😑 🚖 Status & Manage							
	Standby NO7 IV	Network Elements							
		- 💽 Sei	Server						
		🕅 HA							
		🔊 🕅 Dai	Database						
		RP RP	Repages						
		🗐 Tay							
		E Eile							
		2. Click Edit	at the bottom of	the screen.					
		2 Soloot the		convor and	ant it to Antivo				
		5. Select the	Stanuby NOAW	server and	set it to Active .				
		Modifying HA	attributes						
		Hostname	Max Allowed HA Role	Description					
		nootilaine		Description					
		ZombieNOAM1	Active 💌	The maximum					
		ZombieNOAM2	Active -	The maximum					
			Active						
		ZombieDBNOAM1	Standby	The maximum					
		4. Click OK.							
19		1 Navigate t	Status and M:	anage > Se	rvor				
□	Restart DSR			anage > 0e	1461.				
	application	🖃 🔄 Status &	Manage						
		Network Elements							
		Serve Serve	er						
		HA	hone						
		Data	base						
			20220						
		🔲 🦳 Task	(S						
		E Eiles							
		2 Select the	recovered stand		conver and click Postart				
					Server and Click Restart.				
		op Restart	Rebo						
		op Rootart							
	1	1							

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

20.	NOAM VIP GUI: Perform key exchange 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 at the bottom of the screen. SSH Key Exchange Transfei Type the Password and click OK. SSH Key Exchange OK Cancel
21.	NOAM VIP GUI:	IIWarningII
	to the C-level servers of this site	Before continuing this procedure, replication to C-level servers at the SOAM site being recovered MUST be inhibited. 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.
22.	to the C-level servers of this site	Before continuing this procedure, replication to C-level servers at the SOAM site being recovered MUST be inhibited. 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.
22.	Stop replication to the C-level servers of this site	Before continuing this procedure, replication to C-level servers at the SOAM site being recovered MUST be inhibited. 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. 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. If the TVOE restore has already been executed (step 5), skip this step. If a TVOE backup of the SOAM server blades is not available, execute Configure SOAM TVOE Server Blades from reference [8].
22. 23.	Configure SOAM TVOE server blades Create and IPM SOAM VMs	 Before continuing this procedure, replication to C-level servers at the SOAM site being recovered MUST be inhibited. 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. If the TVOE restore has already been executed (step 5), skip this step. If a TVOE backup of the SOAM server blades is not available, execute Configure SOAM TVOE Server Blades from reference [8]. 1. Execute Create SOAM Guest VMs for the failed SOAM VMs and MP blades from reference [8].
□ 22. □ 23. □	Configure SOAM TVOE server blades Create and IPM SOAM VMs	 Before continuing this procedure, replication to C-level servers at the SOAM site being recovered MUST be inhibited. 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. 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. If the TVOE restore has already been executed (step 5), skip this step. If a TVOE backup of the SOAM server blades is not available, execute Configure SOAM TVOE Server Blades from reference [8]. 1. Execute Create SOAM Guest VMs for the failed SOAM VMs and MP blades from reference [8]. 2. Execute IPM Blades and VMs for the failed SOAM VMs and MP blades from reference [8].

24. □	Recover active SOAM server	 Execute Configure the SOAM Servers, steps 1-3 and 5-8, from reference [8]. 				
		Note: If you are using NetBackup, also execute step 10.				
		 If you are using NetBackup, execute Install NetBackup Client from reference [8]. 				
25.	NOAM VIP GUI:	1. Navigate to Status and Manage > HA.				
	Set HA on SOAM server	Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Click Edit. 3. Select the SOAM server and set it to Active. Zombie SOAM1 Active The m				
		Zombie SOAM2 Spare The m Observer OOS				
		4. Click OK .				
26.	NOAM VIP GUI: Restart DSR application	 Navigate to Status and Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the recovered SOAM server and click Restart. 				

Procedure 1. Recovery Scenario 1

27.	NOAM VIP GUI:	1. Navigate to Status and Manage > Files.		
	Upload the	📄 😋 Status & Manage		
	backed up	Network Elements		
file		Server		
		The second secon		
		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.		
		W Uplead Des		
		W Opload Dol		
		3. Click Browse and locate the backup file.		
		4. Check This is a backup file checkbox.		
		5. Click Upload .		
		8		
		File:		
		Browse No file selected.		
		This is a backup file		
	Unload			
		opour		
		Cancel		
		I he file takes a few seconds to upload depending on the size of the backup data.		

Procedure 1. Recovery Scenario 1

110						
28. □	 Recovered SOAM GUI: Login 1. Establish a GUI session on the recovered SOAM server. 2. Open the web browser and enter a URL of: 					
	Login	http://cRogoward SOIM ID Addroggs				
		IICtp:// <recovered_soam_ip_address></recovered_soam_ip_address>				
		3. Login as the guiadmin user:				
		ORACLE [®]				
		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 1. Recovery Scenario 1

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

29.	Recovered SOAM GUI: Verify the archive contents and database compatibility	1. Na	vigate to Status and Manage > Database.
		2. Se	lect the Active SOAM server and click Compare.
		n Com	
		ip Con	pare Kesto
		3. Cli 27	ck the button for the restored database file uploaded as a part of Step . of this procedure.
		Datab	ase Compare
		Select a	rchive to compare on server: 2
		Archive	backup/Backup.DSR.Zom
		Ok	Cancel
		4. Ve	rify the output window matches the screen below.
		Datab	ase Archive Compare
			•
		The s	selected database came from ZombieSOAM1 on 10
		Archi	ive Contents
		Confi	guration data
		Datak The c	base Compatibility Matabases are compatible.
		Note:	Archive Contents and Database Compatibilities must be the following:
			Archive Contents: Configuration data.
		Nata	The following is consected output for Tapelogu Compatibility Check
		Note:	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 t this	he verification is successful, click Back and continue to next step in s procedure.

Procedure 1. Recovery Scenario 1

30.	Recovered SOAM GUI: Restore the database	 Select the Active SOAM server and click Restore. Select the proper back up provisioning and configuration file. 		
		Database Compare		
		Select archive to compare on sen		
		Archive * backup/Backup.dsr.2		
		3. Click OK . The following confirmation screen displays.		
		Database Restore Confirm		
		Compatible archive.		
		The selected database came from Zombi		
		Archive Contents Configuration data		
		Database Compatibility The databases are compatible.		
		 If you get an error for Node Type Compatibility, that is expected. If no other errors are displayed, mark the Force checkbox and click OK to proceed with the DB restore. 		
		Note: After the restore has started, the user is logged out of XMI SOAM GUI since the restored Topology is old data. The provisioning is disabled after this step.		
31.	Recovered	Wait for 5-10 minutes for the system to stabilize with the new topology:		
	SOAM GUI: Monitor and	Monitor the Info tab for Success . This indicates the restore is complete and the system is stabilized.		
	contirm database restoral	<i>Note</i> : Do not pay attention to alarms until all the servers in the system are completely restored.		
		<i>Note</i> : The Configuration and Maintenance information is in the same state it was when backed up during initial backup.		

32.	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				
		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.				
33.	NOAM VIP GUI: Recover the	Recover the remaining SOAM servers (standby , spare) by repeating these steps for each SOAM server:				
	remaining SOAM servers	 Execute Configure the SOAM Servers, steps 1-3 and 5-8, from reference [8]. 				
		<i>Note</i> : If you are using NetBackup, also execute step 10.				
		2. If you are using NetBackup, execute Install NetBackup Client from reference [8].				

Procedure 1. Recovery Scenario 1

Procedure 1. Recovery Scenario 1

34.		 Navigate to Status and Manage > HA. 					
	Set HA on	🖃 🚖 Statu	s & Manage				
	SOAMs	Network Elements					
		🔂 S	erver				
			HA HA				
		Database					
		KPIs					
		B Pi	rocesses				
		🔊 🔊 🖓 🖓	asks				
			iles				
		2. Click Edit a	at the bottom of th	e screen.			
		3. Select the	recovered SOAM	server and set it to Active .			
		Zombie SOAM1	Active 🔻	The maximum desired HA			
		Zombie SOAM2	005 -	The maximum desired HA			
			Active				
			Standby				
		ZombieDAMP1	Spare	The maximum desired HA			
			oos				
		4. Click OK .					
35.	NOAM VIP GUI:	1. Navigate to	Status and Man	age > Server.			
	Restart DSR	🚊 🚗 Status	& Manage				
	application	- In Ne	twork Elements				
		Ser	rver				
		HA					
		🔤 Da	tabase				
		KP	ls				
		Pro	cesses				
		2. Select the	recovered standby	/ SOAM server and click Restart .			
		p Restart	Rebo				
1	1						

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

36.	NOAM VIP GUI:	Un-Inhibit (Start) Replication to the recovered Standby SOAM.	
	on the	1. Navigate to Status and Manage > Database.	
	recovered	🖻 😋 Status & Manage	
	standby SOAM	🔤 🕅 Network Elements	
		🔯 Server	
		🔯 HA	
		🔯 Database	
		🔯 KPIs	
		Processes	
		2. Click Allow Replication on the recovered standby SOAM server.	
		 Verify the replication on all servers is allowed. This can be done by checking Repl status column of respective server 	
37.	SOAM VIP GUI:	1. Navigate to Diameter > Configuration > Local Node .	
	Verify the local	📄 😋 Diameter	
		😑 😋 Configuration	
		Capacity Summary	
		Connection Capacity Dashb	
		Application Ids	
		Configuration Sets	
		Local Nodes	
		2. Verify all the local nodes are shown.	
38		1 Navigate to Diameter > Configuration > Peer Node	
□	Verify the peer node info		
		Capacity Summary	
		Connection Capacity E	
		Application Ids	
		CEX Parameters	
		Command Codes	
		Local Nodes	
		Peer Nodes	
		2. Verify all the peer nodes are shown.	

39.	SOAM VIP GUI:	1. Navigate to Diameter > Configuration > Connections.	
	Verify the	🖻 😋 Diameter	
	connections into	🖻 😋 Configuration	
		Capacity Summary	
		Connection Capacity Dash	
		Application Ids	
		Cex Parameters	
		Command Codes	
		Local Nodes	
		Peer Nodes	
		Peer Node Groups	
		Connections	
		2. Verify all the connections are shown.	
40.	SOAM VIP GUI:	1. Navigate to Diameter > Maintenance > Connections .	
	connections. if	🖻 🥽 Maintenance	
	needed	ស Route Lists	
		ស Route Groups	
		Peer Nodes	
		 Select each connection and click Enable. Alternatively, you can enable all the connections by clicking EnableAll. 	
		ble 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	
41.	Active NOAM:	Establish an SSH session to the active NOAM, login as admusr.	
	Activate optional features	Note for PCA Activation:	
		If you have PCA installed in the system being recovered, re-activate PCA by executing PCA Activation on Entire Server on Recovered NOAM Server from [13].	
		Note: If not all SOAM sites are recovered at this point, then you should repeat activation for each *new* SOAM site that comes online.	
		Note: If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.	
		Refer to 1.5 Optional Features to activate any features previously activated.	

Procedure 1. Recovery Scenario 1

		.,			
42 . □	NOAM VIP GUI: Start replication	Un-Inhibit (Start) Rother the same site as of	eplication to the wo the failed SOAM se	rking C-level Serve ervers.	ers which belongs to
on working C- level serversIf the spare SOAM is a Un-Inhibit A and B Leve Standby and Spare SO.			I is also present in Level Replication or SOAMs are Lost).	the site and lost, on C-Level Servers (execute Appendix F When Active,
		If the spare SOAM is NOT deployed in the site, execute Appendix D Un-			
		 Navigate to Status and Manage > Database. 			
		🚊 😋 Status & M	lanage		
		Netwo	rk Elements		
		The server			
		Databa	ase		
		KPIs			
		Proces	ses		
		2. If the Repl Stat order; otherwis continue with th	tus is set to Inhibite e, if none of the serv ne next step:	ed, click Allow Rep vers are inhibited, s	lication using this kip this step and
		Active NOA	AM Server		
		Standby No	OAM Server		
		Active SOA	M Server		
		Standby S	OAM Server		
		Spare SOA	M Server (if applic	able)	
		Active DR	NOAM Server		
		Standby DI	R NOAM Server		
		MP/IPFE set the Active I	ervers (if MPs are c MP; otherwise, the c	onfigured as active/ order of the MPs do	/standby, start with es not matter)
		 SBRS (if SBR servers are configured, start with the active SBR, standby, then spare) 		e active SBR, then	
		3. Verify the replic done by examined by the second	cation on all the wor ning the Repl Status	king servers is allow table as shown he	ved. This can be re:
		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
--------------	---------------------

43.	SOAM VIP GUI: Perform key exchange with export server	 Navigate to Administration > Remote Servers > Data Export. Remote Servers LDAP Authentication SNMP Trapping Data Export DNS Configuration Click SSH Key Exchange. Type the Password and click OK. 	
		Password: OK Cancel	
44.	NOAM VIP GUI: Recover the C- level server (DA- MP, SBRs, IPFE)	 Execute Configure MP Blade Servers, steps 1, 7, 11-14, and 17, from reference [8]. Note: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. Repeat this step for any remaining failed MP servers. 	
45.	NOAM VIP GUI: Set HA on all C- level servers	 Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Click Edit. For each recovered C-level whose Max Allowed HA Role is set to Standby, set it to Active. ZombieDAMP1 Active Active The maximum desired HA Role for ZombieDAMI Active Standby Spare Observer 	
		4. Click OK .	

Procedure 1. Recovery Scenario 1

46.	NOAM VIP GUI:	1. Navigate to Status and Manage > Server.
Restart DSI application recovered C level server	Restart DSR application on recovered C- level servers	 Status & Manage Network Elements Server HA
		🔛 🔯 Database
	 Control Control C	🔣 KPIs
		Processes
		2. Select the recovered C-level servers and click Restart .
		p Restart Rebo
Procedure 1. Recovery Scenario 1

47.	NOAM VIP GUI: Start replication	Un-inhibit (start) re 1. Navigate to Sta	plication to the ALL atus and Manage >	C-level servers. Database.	
	servers	E Calus & M Server Calus & M Server Calus	lanage rk Elements ase sses		
		2. If the Repl Stat order:	tus is set to Inhibite	ed, click Allow Rep	lication using this
		Active NOA	AM Server		
		Standby N	OAM Server		
		Active SOA	M Server		
		Standby S	OAM Server		
		Spare SOA	M Server (if applic	able)	
		Active DR	NOAM Server		
		Standby Di MP/IPFE s the Active I	ervers (if MPs are c MP; otherwise, the c	onfigured as active/ order of the MPs do	standby, start with es not matter)
		 SBRS (if S standby, th 	BR servers are cont en spare)	figured, start with the	e active SBR, then
		3. Verify the replic done by examine	cation on all the wor ning the Repl Status	king servers is allov s table as shown he	ved. This can be re:
		OAM Repl Status	SIG Repl Status	Repl Status	Repl Audit Status
		NotApplicable	NotApplicable	Allowed	NotApplicable
		Normal	NotApplicable	Allowed	NotApplicable
		Normal	NotApplicable	Allowed	NotApplicable
		Normal	NotApplicable	Allowed	NotApplicable
48. □	8. Active NOAM: Perform key exchange	 Establish an SS Perform a keye 	SH session to the ac exchange from the a	ctive NOAM, login a ctive NOAM to each	s admusr . n recovered server:
	between the active-NOAM	\$ keyexchange	admusr@ <recove< th=""><th>ered Server Hos</th><th>tname></th></recove<>	ered Server Hos	tname>
	and recovered servers	<i>Note</i> : If an export	t server is configure	d, perform this step	

Procedure 1. Recovery Scenario 1



Trocedure I. Recovery Scenario I	Procedure	1.	Recovery	Scenario	1
----------------------------------	-----------	----	----------	----------	---

50.	Active NOAM: Verify replication between servers	1. Log into the active NOAM using SSH terminal as admusr .		
		2. Execute this command:		
		\$ sudo irepstat -m		
		Output:		
		Policy 0 ActStb [DbReplication]		
		Oahu-DAMP-1 - Act/Act		
		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 - Act/Stb		
		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		
		Define the second seco		
		Defrom Canu-SOAM-2 Accive 0 0.50 0.03%cpu 24B/S A=C3042.212		
		BC From Oabu-SOAM-2 Active 0 0.50 ^0.03%cpu 28B/s A=C3642.212		
		Oahu-NOAM-1 Stby		
		AA From Oahu-NOAM-2 Active 0 0.25 ^0.03%cpu 23B/s		
		Oahu-NOAM-2 Active		
		AA To Oahu-NOAM-1 Active 0 0.25 1%R 0.04%cpu 61B/s		
		AB To Oahu-SOAM-2 Active 0 0.50 1%R 0.05%cpu 75B/s		
		Oahu-SOAM-1 Stby		
		BB From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 27B/s		
		Oahu-SOAM-2 Active		
		AB From Oahu-NOAM-2 Active 0 0.50 ^0.03%cpu 24B/s		
		BB To Oahu-SOAM-1 Active 0 0.50 1%R 0.04%cpu 32B/s		
		BC To Oahu-IPFE-1 Active 0 0.50 1%R 0.04%cpu 21B/s		
		irepstat (40 lines) (h)elp (m)erged		

Procedure	1.	Recovery	Scenario 1

51.	NOAM VIP GUI:	1. Navigate to Status	and Manage >	> Database	•	
	 Verify the database states Status & Manage Network Elements Server HA Database KPIs Processes Verify the OAM Max HA Role is either Active or Status SOAM; Application Max HA Role for MPs is Active; Normal: 		or Standby for Active; and the	r NOAM and status is		
		Network Element	Server	1	Role	OAM Max HA Role
		ZombieDRNOAM	ZombieDRNOAM1	1	Network OAM&P	Active
		ZombieNOAM	ZombieNOAM2	1	Network OAM&P	Standby
		ZombieSOAM	ZombieSOAM2	:	System OAM	N/A
		ZombieNOAM	ZombieNOAM1	1	Network OAM&P	Active
		ZombieSOAM	ZombieSOAM1	:	System OAM	Active
		ZombieDRNOAM	ZombieDRNOAM2	1	Network OAM&P	Standby
		ZombieSOAM	ZombieDAMP2		MP	Standby
		ZombieSOAM	ZombieSS7MP2		MP MB	Active
		ZombieSOAM	ZombielPEE1		MP	Active
		ZombieSOAM	ZombielPEE2		MP	Active
52. NOAM VIP GU 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 Hostname ZombieNOAM1 ZombieDRNOAM1 ZombieDRNOAM1 ZombieDRNOAM1 ZombieORNOAM1 	and Manage >	> HA. S. e or Standb an HA Role tive andby tive andby tive	Y. Application HA Role N/A N/A N/A N/A N/A N/A	Max Allowed HA Role Active Active
1		ZombieSOAM1	Act	aive	N/A	Acuve
		Hostname	AO	AM HA Role	Application HA Role	Max Allowed HA Role
		ZombieNOAM1	Act	tive	N/A	Active
		ZombieNOAM2	Sta	andby	N/A	Active
		ZombieDRNOAM1	Act	tive	N/A	Active
		ZombieDRNOAM2	Sta	andby	N/A	Active
		ZombieSOAM1	Act	tive	N/A	Active
i			7101			

Procedure 1. Recovery Scenario 1

r	1	
53.	NOAM GUI: Enable	1. Navigate to Status and Manage > Database.
		🖶 🚗 Status & Manage
	provisioning	Network Elements
		Server
		N Research
		Processes
		■ Tasks
		Files
		2. Click Enable Provisioning.
		Enable Provisioning Report Inhibit/
		3. A confirmation window displays. Click OK to enable Provisioning.
54.	SOAM GUI:	1. Navigate to Status and Manage > Database.
	Enable site	🖶 🚔 Status & Manage
	provisioning	A Network Elements
		Renver
		N Labase
		KPIS
		Norman Processes
		🖃 🧰 Tasks
		Files
		2. Click Enable Site Provisioning.
		Enable Site Provisioning Report Inhibit/Allo
		3. A confirmation window displays. Click OK to enable Provisioning.
55.	MP Servers:	For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS
	Disable SCTP Auth Flag	feature activation guide [14].
		Execute this procedure on all failed MP servers.

		-	
56.	SOAM VIP GUI: Enable connections, if needed	 Navigate to Diameter > Maintenance > Connections. Maintenance Route Lists Route Groups Peer Nodes Connections Select each connection and click Enable. Alternatively, you can enable all the connections by clicking EnableAll. EnableAll Disable. Verify the Operational State is Available. Note: If a Disaster Recovery was performed on an IPFE server, it may be management to disable and the connection of the performed on an IPFE server. 	
		necessary to disable and re-enable the connections to ensure proper link distribution	
57.	SOAM VIP GUI: Enable optional features	Ink distribution 1. Navigate to Diameter > Maintenance > Applications. Image: Maintenance Image: Maintenance Image: Route Lists Image: Route Groups Image: Route Groups	
58.	SOAM VIP GUI: Re-enable transports, if needed	 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. 	

Procedure 1. Recovery Scenario 1

Procedure 1. Red	covery Scenario 1
------------------	-------------------

59.	SOAM VIP GUI: Examine all alarms	1. Navigate to Alarms & Events > View Active.
		📄 😋 Alarms & Events
	alanno	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.	NOAM VIP GUI:	1. Log into the NOAM VIP if not already logged in.
	Examine all	2. Navigate to Alarms & Events > View Active.
	alainis	📄 😋 Alarms & Events
		View Active
		View History
		View Trap Log
		3. Examine all active alarms and refer to the on-line help on how to address
		them.
		If needed, contact My Oracle Support (MOS).
61.	Restore GUI	If applicable, execute Resolving User Credential Issues after Database
	usernames and	Restore to recover the user and group information restored.
<u> </u>	Passwords	Evenueta DCD Detabases Desluce to bask up the Configuration databases
62.	Backup and archive all the	Execute DSR Database Backup to back up the Configuration databases.
	databases from	
	the recovered	
	System	
63.	Recover IDIH	If IDIH were affected, refer to IDIH Disaster Recovery to perform disaster recovery on IDIH
64.	SNMP workaround	Refer to SNMP Configuration to configure SNMP as a workaround in these cases:
		1. If SNMP is not configured in DSR.
		 If SNMP is already configured and SNMPv3 is selected as enabled version.

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

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

the procedure. The actual procedure detailed steps are in Procedure 2. The major activities are summarized as follows:

- Recover standby NOAM server (if needed) by recovering base hardware, software and the database
 - Recover the base hardware
 - Recover the software
- Recover active SOAM server by recovering base hardware and software
 - Recover the base hardware
 - Recover the software
 - Recover the database
- Recover any failed **SOAM and MP** servers by recovering base hardware and software
 - Recover the base hardware
 - Recover the software
 - The database has already been restored at the active SOAM server and does not require restoration at the SO and MP servers

Procedure 2. Recovery Scenario 2

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

Check off ($\sqrt{}$) 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 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® 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 2. Recovery Scenario 2

Procedure 2. Recovery Scenario 2

4.	Active NOAM:	1. Navigate to Status and Manage > HA.	
	Set failed servers to OOS	 Status & Manage Network Elements Server HA Database KPIs Processes Click 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	
		 Set the Max Allowed HA Role drop down box to OOS for the failed servers. 	
		4. Click OK .	
		Ok Cancel	
5. □	Replace failed equipment	HW vendor to replace the failed equipment.	
6.	RMS NOAM Failure: Configure BIOS settings and update firmware	 If the failed server is NOT a rack mount server, skip to step 10. Configure and verify the BIOS settings by executing procedure Configure the RMS and Blade Server BIOS Settings from reference [10]. Verify and/or upgrade server firmware by executing procedure Upgrade Management Server Firmware from reference [10]. Note: Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server. 	

7.	RMS NOAM Failure: Backups available	 If the failed server is NOT a rack mount server, skip to step 10. This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step. 1. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media. 2. If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing Restore PMAC from Backup
8.	RMS NOAM Failure: Backups NOT available	 If the failed server is NOT a rack mount server, skip to step 10. This step assumes that TVOE and PMAC backups NOT are available, if the TVOE and PMAC have already been restored, skip this step. If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. Configure and IPM Management Server from reference [10]. 2. Install PMAC from reference [10]. 3. Configure PMAC Application from reference [10]. If the PMAC is NOT located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. Installing TVOE on Rack Mount Server(s) from reference [10].
9.	Recover failed aggregation/ enclosure switches, and OAs	 Recover failed OAs, aggregation and enclosure switches, if needed. Backups Available: 1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) section to recover failed OAs, aggregation, and enclosure switches Backups NOT Available: 1. Execute HP C-7000 Enclosure Configuration from reference [10] to recover and configure any failed OAs, if needed. 2. Execute Configure Enclosure Switches from reference [10] to recover enclosure switches, if needed.
10.	HP-Class Blade Failure: Configure blade server iLO, update firmware/BIOS settings	 If the failed server is NOT an HP C-Class Blade, skip to step 14. Execute Configure Blade Server iLO Password for Administrator Account from reference [10]. Verify/Update Blade server firmware and BIOS settings by executing Server Blades Installation Preparation from reference [10]
11.	HP-Class Blade Failure: Backups available	 If the failed server is NOT an OAM type HP C-Class Blade, skip to step 14. This step assumes TVOE backups are available. If backups are NOT available, skip this step. 1. Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10]. 2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers.

Procedure 2. Recovery Scenario 2

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

12.	HP-Class Blade Failure: Backups NOT available	If the failed server is NOT an OAM type HP C-Class Blade, skip to step 14. This step assumes TVOE backups are NOT available:			
		 Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10]. 			
		 Configure the NOAM and/or SOAM failed TVOE server blades by executing Configure SOAM TVOE Server Blades from reference [8]. 			
		Note: Although the title of the procedure is related to SOAMs only, execute this procedure for any failed NOAMs located on TVOE server blades.			
13. □	Create VMs	Execute Create NOAM/SOAM Virtual Machines to create the NOAM and SOAM VMs on failed TVOE servers.			
14.	IPM and install DSR application on failed guest/servers	 Execute IPM Blades and VMs for the failed SOAM VMs and MP blades from reference [8]. 			
		2. Execute Install the Application Software for the failed SOAM VMs and MP blades from reference [8].			
15. □	Install NetBackup client (Optional)	If NetBackup is used, execute Install NetBackup Client from reference [8].			
16. NOAM VIP GUI: 1. Establish a GUI session on the NOAM server by using the VIP of the NOAM server. Open the web browser and enter a URL of the NOAM server.					
		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, <u>Oracle</u> and/or its affiliates. All rights reserved.			

17.	NOAM VIP GUI : Export the initial configuration	If the failed server is NOT a NOAM server, skip to step 24. 1. Navigate to Configuration > Servers .			
		 Main Menu Administration Configuration Networking Servers Server Groups Resource Domains Places Place Associations From the GUI screen, select the failed NOAM server and click Export to generate the initial configuration data for that server. Insert Edit Delete Export Report 			
18. □	NOAM VIP GUI: Copy configuration file to failed NOAM server	 Obtain a terminal session to the NOAM VIP, login as the admusr user. Configure the failed NOAM server: 			
		<pre>\$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<failed_noam_hostnam e>.sh admusr@<failed_noam_control_ip_address>:/var/tmp/TKLCConf igData.sh</failed_noam_control_ip_address></failed_noam_hostnam </pre>			
19. □	Failed NOAM Server: Verify the configuration was called and reboot the server	 Establish an SSH session to the failed NOAM server, login as the admusr user. The automatic configuration daemon looks for the file named TKLCConfigData.sh in the /var/tmp directory, implements the 			
		 Configuration in the file, and asks the user to reboot the server. Verify awpushcfg was called by checking the following file. 			
		<pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre>			
		Verify this message displays: [SUCCESS] script completed successfully!			
		3. Reboot the server:			
		\$ sudo init 6			
		4. Wait for the server to reboot.			

20.	Failed NOAM Server: Configure networking for dedicated NetBackup interface (Optional)	 Note: Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup. Obtain a terminal window to the failed NOAM server, logging in as the admusr.
		<pre>\$ sudo /usr/TKLC/plat/bin/netAdm setdevice=netbackup type=Ethernetonboot=yes address=<no2_netbackup_ip_adress> netmask=<no2_netbackup_netmask></no2_netbackup_netmask></no2_netbackup_ip_adress></pre>
		<pre>\$ sudo /usr/TKLC/plat/bin/netAdm addroute=net device=netbackupaddress=<no1_netbackup_network_id> netmask=<no2_netbackup_netmask> gateway=<no2_netbackup_gateway_ip_address></no2_netbackup_gateway_ip_address></no2_netbackup_netmask></no1_netbackup_network_id></pre>
21.	Failed NOAM Server: Verify server health	Execute this command on the 2 nd NOAM server and make sure no errors are returned: \$ sudo syscheck Running modules in class hardwareOK Running modules in class diskOK Running modules in class netOK Running modules in class systemOK Running modules in class procOK LOG LOCATION: /var/TKLC/log/syscheck/fail_log

Procedure 2. Recovery Scenario 2

Procedure 2. Recovery Scenario 2

22.	NOAM VIP GUI:	1. Navigate to Status and Manage > HA.			
	Set HA on standby NOAM	 Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Click Edit at the bottom of the screen. 3. 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 4. Click OK.	Standby Spare	The maximum	
23.	NOAM VIP GUI: Restart DSR application	 Navigate to Status & Status & Network Serve Serve	o Status and Ma Manage York Elements er base esses s recovered stance Reboy	anage > Se	r ver . Server and click Restart .

24.	NOAM VIP GUI: Stop replication to the C-level servers of this site	 LiWarning!! Before continuing this procedure, replication to C-level servers at the SOAM site being recovered MUST be inhibited. 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 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 Inhibit A and B Level Replication on C-level Servers to inhibit replication to working C-level servers before continuing. 			
25.	Recover active SOAM server	 Execute Configure the SOAM Servers, steps 1-3 and 5-8, from reference [8]. <i>Note</i>: If you are using NetBackup, also execute step 10. If you are using NetBackup, execute Install NetBackup Client from reference [8]. 			
26.	NOAM VIP GUI: Set HA on SOAM server	 Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click Edit at the bottom of the screen. Select the SOAM server and set it to Active. Zombie SOAM1 Active The m Active Standby Spare Observer Observer Observer Observer Observer Observer 			

Procedure 2. Recovery Scenario 2

Procedure 2. Recovery Scenario 2

27.	NOAM VIP GUI:	1. Navigate to Status and Manage > Server.				
	Restart DSR	😑 😋 Status & Manage				
	application	Network Elements				
		Server Server				
		HA				
		Processes				
		🗈 🧰 Tasks				
		Files				
		2. Select the recovered SOAM server and click Restart .				
		p Restart Rebo				
28.	NOAM VIP GUI:	1. Navigate to Status and Manage > Files.				
	backed up	🖃 🚖 Status & Manage				
	SOAM database	Network Elements				
	file	HA				
	💽 Database					
		KPIs				
		Tasks				
		 Select the active SOAM server tab. Click Upload and select the SO Provisioning and Configuration file backed up after initial installation and provisioning. 				
		W Upload Dov				
		3. Click Browse and locate the backup file.				
		4. Check This is a backup file checkbox.				
		5. Click Upload .				
		0				
		File:				
		This is a backup file				
		upioad				
		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.				

riocedure 2. Recovery ocenano 2							
29.Recovered SOAM GUI:1.Establish a GUI session on the recovered SOAM server.2.Open the web browser and enter a URL of:							
	Login	http://cRecovered_SOAM_IP_Address>					
		2 Login as the quiadmin uppr					
		5. Login as the gulatinin 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

30. Recovered 1. Navigate to Status and Manage > Database.	
SOAM GUI: 2. Select the Active SOAM server and click Compare. Verify the 2.	
archive contents and database	
3. Click the button for the restored database file uploaded as a pa 28 of this procedure.	art of step
Database Compare	
Select archive to compare on server: 2	
Archive *	
Ok Cancel	
4. Verify the output window matches the screen below.	
Database Archive Compare	
The selected database came from ZombieSOAM1 on 10	
Archive Contents Configuration data	
Database Compatibility The databases are compatible.	
Note: Archive Contents and Database Compatibilities must be th	e following:
Archive Contents: Configuration data.	
Database Compatibility : The databases are compatible.	
Note : The following is expected output for Topology Compatibility since we are restoring from existing backed up data base t with just one SOAM:	/ Check o database
Topology Compatibility THE TOPOLOGY SHOULD BE COMPATIBLE MINUS TH	E NODEID.
Note: We are trying to restore a backed up database onto an em database. This is an expected text in Topology Compatibil	pty SOAM ity.
5. If the verification is successful, click Back , then cancel and cor next step in this procedure.	ntinue to

2

 31. Recovered SOAM GUI: Restore the database Select the Active SOAM server and click Restore. Select the proper back up provisioning and configuration Database Restore Select archive to Restore on server: ZombieSOAM2 backup/Backup.dsr.ZombieSOAM2.Configure backup/Backup.dsr.ZombieSOAM2.Configure 	n file.
Control Control Restore the database Control Contro Control Control Control Contr	n file.
Catabase Database Restore Select archive to Restore on server: ZombieSOAM2 backup/Backup.dsr.ZombieSOAM2.Configure backup/Backup.dsr.ZombieSOAM2.Configure	
Select archive to Restore on server: ZombieSOAM2 backup/Backup.dsr.ZombieSOAM2.Configure backup/Backup.dsr.ZombieSOAM2.Configure	
backup/Backup.dsr.ZombieSOAM2.Configura backup/Backup.dsr.ZombieSOAM2.Configura backup/Backup.dsr.ZombieSOAM2.Configura	
Checkup/Beckup desZembis000400 Ocefering	
Archive * Archive * Archive * Obackup/Backup.dsr.ZombieSOAM2.Configure Dbackup/Backup.dsr.ZombieSOAM2.Configure Dbackup/Backup.dsr.ZombieSOAM2.Configure Dbackup/Backup.dsr.ZombieSOAM2.Configure Dbackup/Backup.dsr.ZombieSOAM2.Configure Dbackup/Backup.dsr.ZombieSOAM2.Configure	
Ok Cancel	
3. Click OK . The following confirmation screen displays.	
 If you get an error for Node Type Compatibility, that is e other errors are displayed, mark the Force checkbox as proceed with the DB restore. 	expected. If no nd click OK to
Database Restore Confirm	
Compatible archive.	
The selected database came from Zomb:	
Archive Contents Configuration data	
Database Compatibility	
The databases are compatible.	
Note: After the restore has started, the user is logged out since the restored Topology is old data. The provis after this step.	of XMI SOAM GUI ioning is disabled
32. Recovered Wait for 5-10 minutes for the system to stabilize with the net stabilize	ew topology:
SOAM GUI: Monitor and Deptition and Monitor the Info tab for Success. This indicates the restore the system is stabilized.	e is complete and
Communication Note: Do not pay attention to alarms until all the servers i completely restored.	n the system are
Note: The Configuration and Maintenance information is i was when backed up during initial backup.	in the same state it

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

33		Recover the remaining SOAM servers (standby spare) by repeating these				
55.	Recover the	steps for each SOAM server:				
	remaining SOAM servers	1. Execute Configure the SOAM Servers , steps 1-3 and 5-8, from reference [8].				
		<i>Note</i> : If you are using NetBackup, also execute step 10.				
		 If you are using NetBackup, execute Install NetBackup Client from reference [8]. 				
34.	NOAM VIP GUI:	Un-Inhibit (Start) Replication to the recovered SOAM servers				
	Start replication	 Navigate to Status and Manage > Database. 				
	recovered	🖻 😋 Status & Manage				
	SOAMs	Network Elements				
		Server				
		Database				
		KPIs				
		Processes				
		2 Click Allow Replication on the recovered SOAM servers				
		2. Click Allow Replication on the recovered SOAIVI servers.				
		by checking Repl status column of respective server				
		1. Navigate to Status and Manage > HA.				
35.	NOAM VIP GUI:	1. Navigate to Status and Manage > HA.				
35.	NOAM VIP GUI: Set HA on recovered	 Navigate to Status and Manage > HA. 				
35. □	NOAM VIP GUI: Set HA on recovered standby SOAM	 Navigate to Status and Manage > HA. 				
35. □	NOAM VIP GUI: Set HA on recovered standby SOAM server	 Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA 				
35.	NOAM VIP GUI: Set HA on recovered standby SOAM server	 Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database 				
35.	NOAM VIP GUI: Set HA on recovered standby SOAM server	 Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes 				
35.	NOAM VIP GUI: Set HA on recovered standby SOAM server	 Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Tasks 				
35.	NOAM VIP GUI: Set HA on recovered standby SOAM server	 Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Tiles 				
35.	NOAM VIP GUI: Set HA on recovered standby SOAM server	 Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click Edit at the bottom of the screen 				
35.	NOAM VIP GUI: Set HA on recovered standby SOAM server	 Navigate to Status and Manage > HA. 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. 				
35.	NOAM VIP GUI: Set HA on recovered standby SOAM server	 Navigate to Status and Manage > HA. 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. 				
35.	NOAM VIP GUI: Set HA on recovered standby SOAM server	 1. Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Click Edit at the bottom of the screen 3. Select the recovered standby SOAM server and set it to Active. Zombie SOAM1				
35.	NOAM VIP GUI: Set HA on recovered standby SOAM server	 1. Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Click Edit at the bottom of the screen 3. Select the recovered standby SOAM server and set it to Active. Zombie SOAM1 Active Standby				
35.	NOAM VIP GUI: Set HA on recovered standby SOAM server	 Navigate to Status and Manage > HA. 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 Discrete 				
35.	NOAM VIP GUI: Set HA on recovered standby SOAM server	 Navigate to Status and Manage > HA. 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 OS 				

Procedure 2. Recovery Scenario 2

36.	NOAM VIP GUI:	1. Navigate to Status and Manage > Server.				
	Restart DSR	E G Status & Manage				
	application	Network Elements				
		Renver				
		Database				
		Coloritation and standby COAM service and slick Restart				
		2. Select the recovered standby SOAIVI server and click Restart.				
		p Restart Rebo				
37.	SOAM GUI:	1. Navigate to Status and Manage > Database.				
	Enable	📄 😋 Status & Manage				
	providiorning	Network Elements				
		Server 💽				
		🔯 HA				
		🔤 🔯 Database				
		💽 KPIs				
		Processes				
		Tasks				
		Files				
		2. Click Enable Site Provisioning.				
		Enable Site Provisioning Report Inhibit/Allo				
		3. A confirmation window displays. Click OK to enable provisioning.				
38.	SOAM VIP GUI:	1. Navigate to Diameter > Configuration > Local Node .				
	verify the local	🖻 🚖 Diameter				
		🖻 🔄 Configuration				
		Capacity Summary				
		Connection Capacity Dashb				
		Application Ids				
		Configuration Sets				
		Local Nodes				
		2. Verify all the local nodes are shown				

39.	SOAM VIP GUI:	1. Navigate to Diameter > Configuration > Peer Node.
	Verify the peer node info	 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.
40.	SOAM VIP GUI: Verify the connections info	 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.

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

41. □	NOAM VIP GUI: Start replication	Un-Inhibit (Start) Replication to the working C-level servers which belong to the same site as of the failed SOAM servers.				
	on working C- level servers	If the spare SOAM and B Level Replica SOAMs are Lost).	l is also present in ation on C-Level Se	the site and lost, e rvers (When Active,	execute Un-Inhibit A , Standby and Spare	
	Note : Wait until	If the spare SOAM is NOT deployed in the site, execute Un-Inhibit A and B Level Replication on C-level Servers.				
	audit becomes	 Navigate to Status and Manage > Database. 				
	active on SOAM	🚊 😋 Status & M	lanage			
	Click Allow	Netwo	rk Elements			
	Replication for	Server				
	each DP server until all DP	HA	_			
	servers	Databa	ase			
	this SOAM		Ses			
	Network	2 If the Reni Stat	tus is set to Inhihite	d click Allow Repl	lication using this	
	been inhibited.	order; otherwis continue with th	e, if none of the serv ne n e xt step:	vers are inhibited, s	kip this step and	
		Active NOA	M Server			
		Standby No	OAM Server			
		Active SOAM ServerStandby SOAM Server				
		Spare SOAM Server (if applicable)Active DR NOAM Server				
		Standby DI	R NOAM Server			
		MP/IPFE s the Active I	ervers (if MPs are co MP; otherwise, the c	onfigured as active/ order of the MPs do	standby, start with es not matter)	
		 SBRS (if S standby, th 	BR servers are conf en spare)	igured, start with th	e active SBR, then	
		3. Verify the replic done by checki	cation on all the worl ng the Repl Status	king servers is allov as shown here.	ved. 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	

42.	NOAM VIP GUI: Recover the C- level server (DA- MP, SBRs, IPFE)	 Execute Configure MP Blade Servers, steps 1, 7, 11-14, and 17, from reference [8]. Note: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. Repeat this step for any remaining failed MP servers 				
43.	NOAM VIP GUI: Restart DSR application on recovered C- level servers	 1. Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes 2. Click Edit at the bottom of the screen. 3. For each recovered C-level with a Max Allowed HA Role set to Standby, set it to Active. ZombieDAMP1 Active Standby Spare Oos 				
		1 Click OK				
44.	NOAM VIP GUI: Restart DSR application on recovered C- level servers	 1. Navigate to Status and Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the recovered C-level servers and click Restart.				

Procedure 2. Recovery Scenario 2

Pro	cedure 2.	Recov	ery Scenario 2
4 -			

45.	NOAM VIP GUI:	Un-Inhibit (Start) Replication to the ALL C-level servers.				
	Start replication	1. Navigate to Status and Manage > Database.				
	servers	📄 🚖 Status & Manage				
		Network Elements				
	Note: Wait until	🔤 💽 Server				
	audit becomes	🕅 HA				
	or NOAM.	🔤 💽 Databa	ase			
	Click Allow Replication for	🤤 🕅 KPIs References	ses			
	each DP server until all DP servers	2. If the Repl Stat order:	t us is set to Inhibite	ed, click Allow Rep	lication using this	
	associated with	Active NOA	MP Server			
	this SOAM Network	 Standby N 	OAMP Server			
	Element have	Active SOA	M Server			
	been innibited.	Standby S	DAM Server			
		Spare SOA	M Server (if applic	able)		
		Active DR I	NOAM Server			
		 Standby DI 	R NOAM Server			
		MP/IPFE S the Active I	ervers (if MPs are c MP; otherwise, the c	configured as active, order of the MPs do	/standby, start with es not matter).	
		3. Verify the replic checking the R	cation on all servers epl Status as show	is allowed. This ca n here:	in 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	
46.	Active NOAM:	1. Establish an SS	SH session to the ad	ctive NOAM, login a	s admusr .	
	Perform keyexchange between the	2. Execute this co to each recover	mmand to perform red server:	a keyexchange fron	n the active NOAM	
	active-NOAM and recovered	\$ keyexchange	admusr@ <recove< td=""><td>ered Server Hos</td><td>tname></td></recove<>	ered Server Hos	tname>	
	30110013					

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

47. 	Active NOAM: Estable Activate optional Note f		h an SSH session to the active NOAM, login as admusr . PCA Feature Activation:	
	teatures	If you h by exec standb recove	ave PCA installed in the system being recovered, re-activate the PCA cuting PCA Activation on Standby NOAM server on the recovered y NOAM server, and PCA Activation on Active SOAM server on the red active SOAM server from [13].	
		Refer to Optional Features to activate any features that were previously activated.		
		Note:	While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:	
			iload#31000{S/W Fault}	
		Note:	If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.	

Procedure 2. Recovery Scenario 2



Procedure 2. Recovery Scenario 2

49.	Active NOAM:	1. Log into the active NOAM using SSH terminal as admusr .		
	Verify replication between servers	2. Execute this command:		
		\$ sudo irepstat -m		
		Output:		
		Delign () st(th [DhDenligsticn]		
		Policy U Actstb [DbReplication]		
		Oahu-DAMP-1 - Act/Act		
		BC From Oahu-SOAM-2 Active 0 0.50 ^0.15%cpu 25B/s A=me		
		CC To Uanu-DAMP-2 Active U 0.10 0.14%cpu 25B/s A=me		
		PG From Ophy-SOMM-2 Active 0 0 50 00 11% any 21P/a A-G2642 212		
		CC From Oahu-DAMP-1 Active 0 0.10 0 14 1 16% cpu 31B/s		
		A=C3642.212		
		Oahu-IPFE-1 Active		
		BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 24B/s A=C3642.212		
		Oahu-IPFE-2 Active		
		BC From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 28B/s A=C3642.212		
		Oahu-NOAM-1 Stby		
		AA From Oahu-NOAM-2 Active 0 0.25 ^0.03%cpu 23B/s		
		Oahu-NOAM-2 Active		
		AA To Oahu-NOAM-1 Active 0 0.25 1%R 0.04%cpu 61B/s		
		AB To Oahu-SOAM-2 Active 0 0.50 1%R 0.05%cpu 75B/s		
		Oahu-SOAM-1 Stby		
		BB From Oahu-SOAM-2 Active 0 0.50 ^0.03%cpu 27B/s		
		Oahu-SOAM-2 Active		
		AB From Oahu-NOAM-2 Active 0 0.50 ^0.03%cpu 24B/s		
		BB To Oahu-SOAM-1 Active 0 0.50 1%R 0.04%cpu 32B/s		
		BC To Oahu-IPFE-1 Active 0 0.50 1%R 0.04%cpu 21B/s		
		irepstat (40 lines) (h)elp (m)erged		

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

50.	NOAM VIP GUI:	1. Navigate to Status	and Manage	er > Database	9.	
	Verify the database states	Status & Manage Network Elements				
		HA				
		🔤 KPIS	KPIs M Processes			
		2. Verify the OAM Max HA Role is either Active or Standby for NOAM and SOAM; Application Max HA Role for MPs is Active ; and status is Normal :				
		Network Element	Server	1	Role	OAM Max HA Role
		ZombieDRNOAM	ZombieDRNOAM1	1	Network OAM&P	Active
		ZombieNOAM	ZombieNOAM2	1	Network OAM&P	Standby
		ZombieSOAM	ZombieSOAM2	:	System OAM	N/A
		ZombieNOAM	ZombieNOAM1	1	Network OAM&P	Active
		ZombieSOAM	ZombieSOAM1	:	System OAM	Active
		ZombieDRNOAM	ZombieDRNOAM2		Network OAM&P	Standby
		ZombieSOAM	ZombieDAMP2		MP	Standby
		ZombieSOAM	ZombieSS7MP2			Active
		ZombieSOAM	ZombielPEE1		MP	Active
		ZombieSOAM	ZombielPFE2		MP	Active
51.	NOAM VIP GUI: Verify the HA status	 SUI: 1. Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Select the row for all of the servers. 3. Verify the HA Role is either Active or Standby. 		у.		
		Hostname		OAM HA Role	Application HA	Max Allowed HA
		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
		ZOTIDIESOAWZ		Stanuby	N/A	otanuby

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

52.	MP Servers: Disable SCTP auth flag	For SCTP connections without DTLS enabled, refer to Disable/Enable DTLS feature activation guide [14].	
53.	SOAM VIP GUI: Enable connections, if needed	 1. Navigate to Diameter > Maintenance > Connections. Maintenance Route Lists Peer Nodes Onnections Connections Connections Connections Select each connection and click Enable. Alternatively, you can enable all the connections by clicking EnableAll. Disable EnableAll Disable Select If disaster recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution. Select in the connection of the connections of the connections of the connections of the connections of the connection of the connections of the connection	
54.	SOAM VIP GUI: Enable optional features	 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 47. Click Enable. 	
55.	SOAM VIP GUI: Re-enable transports, if needed	 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. 	

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

56.	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).
57.	NOAM VIP GUI:	1. Log into the NOAM VIP if not already logged in.
	Examine all alarms	2. Navigate to Alarms & Events > View Active.
		🖻 😋 Alarms & Events
		View Active
		🔤 View History
		View Trap Log
		3. Examine all active alarms and refer to the on-line help on how to address them.
58.	Backup and	Execute DSR Database Backup to back up the Configuration databases.
	archive all the	
	the recovered	
	system	
59.	Recover IDIH	If IDIH were affected, refer to IDIH Disaster Recovery to perform disaster
		recovery on חוטו.

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

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

- Recover Active NOAM server by recovering base hardware, software and the database
 - Recover the base hardware
 - Recover the software
 - Recover the database
- Recover NOAM servers by recovering base hardware and software
 - Recover the base hardware

- Recover the software
- Recover any failed SOAM and MP servers by recovering base hardware and software
 - Recover the base hardware
 - Recover the software
 - Database is already intact at one SOAM server and does not require restoration at the other SOAM and MP servers

Procedure 3. Recovery Scenario 3

This procedure performs recovery if ALL NOAM servers are failed but 1 or more SOAM servers are intact. This includes any SOAM server that is in another location (spare SOAM server). Check off ($\sqrt{}$) 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. Gather required Gather the documents and required materials listed in the Required Materials materials section. \square 2. Replace failed HW vendor to replace the failed equipment. equipment \square 3. **RMS NOAM** If the failed server is **NOT** a rack mount server, **skip to step 8**. Failure: Configure and verify the BIOS settings by executing procedure Configure 1. **Configure BIOS** the RMS and Blade Server BIOS Settings from reference [10]. settings and 2. Verify and/or upgrade server firmware by executing procedure Upgrade update firmware Management Server Firmware from reference [10]. Although the procedure is titled to be run on the management server, Note: this procedure also applies to any rack mount server. **RMS NOAM** 4. If the failed server is **NOT** a rack mount server, **skip to step 8**. Failure: This step assumes that TVOE and PMAC backups are available, if backups Backups are NOT available, skip this step. Available Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media. If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing Restore PMAC from Backup. 5. **RMS NOAM** If the failed server is NOT a rack mount server, skip to step 8. Failure: This step assumes that TVOE and PMAC backups NOT are available, if the \square **Backups NOT** TVOE and PMAC have already been restored, skip this step. available If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures: 1. Configure and IPM Management Server from reference [10]. 2. Install PMAC from reference [10]. 3. Configure PMAC from reference [10]. If the PMAC is **NOT** located on the same TVOE host as the failed NOAM, Execute the following sections/procedures: 1. Installing TVOE on Rack Mount Server(s) from reference [10].

6.	Recover failed aggregation/ enclosure switches, and OAs	 Recover failed OAs, aggregation and enclosure switches, if needed. Backups Available: 1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches. Backups NOT Available, execute: 1. HP C-7000 Enclosure Configuration from reference [10] to recover and configure any failed OAs, if needed. 2. Configure Enclosure Switches from reference [10] to recover enclosure switches, if needed.
7.	HP-Class Blade Failure: Configure blade server iLO, update firmware/BIOS settings	 If the failed server is NOT an HP C-Class Blade, skip to step 11. Execute Configure Blade Server iLO Password for Administrator Account from reference [10]. Verify/Update Blade server firmware and BIOS settings by executing Server Blades Installation Preparation from reference [10].
8.	HP-Class Blade Failure: Backups available	 If the failed server is NOT an OAM type HP C-Class Blade, skip to step 11. This step assumes TVOE backups are available. If backups are NOT available, skip this step. 1. Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10]. 2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers.
9.	HP-Class Blade Failure: Backups NOT available	If the failed server is NOT an OAM type HP C-Class Blade, skip to step 11 . This step assumes TVOE backups are NOT are available. Install and configure TVOE on failed TVOE blade servers by executing section Install TVOE on Blade Servers from reference [10].
10.	Execute fast deployment file for NOAMs	The backup fdconfig file used during the initial DSR installation is available on the PMAC, if a database backup was restored on the PMAC. If a backup fast deployment xml is NOT available, execute Configure NOAM Servers from reference [8]. If a backup fast deployment xml is already present on the PMAC, execute the following procedure: Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade has been performed since initial installation). Execute these commands: \$ cd /usr/TKLC/smac/etc \$ screen \$ sudo fdconfig configfile=<created_fd_file>.xml</created_fd_file>

Procedure 3. Re	ecovery Scenario 3
-----------------	--------------------

11.	Obtain latest database backup and network configuration data	Obtain the most recent database backup file from external backup sources (ex. file servers) or tape backup sources. From required materials list in the Required Materials section; use the site survey documents and Network Element report (if available) to determine network configuration data.
12.	Execute DSR installation procedure for the first NOAM	 Configure the first NOAM server by executing procedure Configure the First NOAM NE and Server from reference [8].
		2. Configure the NOAM server group by executing procedure Configure the NOAM Server Group from reference [8].
		<i>Note</i> : Use the backup copy of network configuration data and site surveys (step 2).
13. □	NOAM GUI: Login	Log into the NOAM GUI as the guiadmin user:
	C C	ORACLE
		Oracle System Login
		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.

Procedure 3. Recovery Scenario 3

14.	NOAM GUI:	 Navigate to Status and Manage > Files.
	Upload the	🗒 🗁 Status & Manage
	backed up	Network Elements
	database file	Server
		HA HA
		- 🔯 Database
		- 🕅 KPIs
		- M Processes
		2. Coloct the potitive NOAM conver
		2. Select the active NOAM server.
		Main Menu: Status & Manage -> Files
		Filter [★] ▼ Tasks ▼
		ZombieNOAM1
		File Name
		TKLCConfigData.ZombieNOAM1.sh
		ugwrap.log
		ungrade log
		3. Click Upload and select the file 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.
		5. Check This is a backup file checkbox.
		6. Click Upload.
		File:
		Browse Backup.dsr.ZombieNOAM1.Configuration.NETWORK_OAM
		This is a backup file
		Upload
		Cancel
		The file takes a few accords to uplead derive diversity of the size of the basis
		data. The file is visible on the list of entries after the upload is complete.
1		ata. The me is visible on the list of entities after the upload is complete.
Procedure 3. Recovery Scenario 3

15.	NOAM GUI:	1. Navigate to Status and Manage > Database.
	Disable provisioning	 Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Click Disable Provisioning.
		Disable Provisioning Report Inhibit/Allow
		3. A confirmation window displays. Click OK to disable provisioning.
		Disable provisioning. Are you sure?
		OK Cancel

Procedure 3. Recovery Scenario 3

16.	NOAM GUI:	1. Se	elect the Active NOAM server and click Compare.
	Verify the archive contents and database compatibility	lication	Backup Compare Restore
		2. Cli 15	ick the button for the restored database file uploaded as a part of Step of this procedure.
		Databas	e Compare
		Select arch	hive to compare on server: ZombieNOAM1
		Archive* (backup/Backup.dsrZombieNOAM1.Configuratio
		Ok Ca	ancel
		3. Ve	rify the output window matches the screen below.
		Note:	A database mismatch regarding the Topology Compatibility and possibly User compatibility (due to authentication) displays. These warnings are expected. If these are the only mismatches, proceed; otherwise, stop and contact My Oracle Support (MOS) to ask for assistance.
		Databas	se Archive Compare
		The set	lected database came from ZombieNOAM1 on 10/10/2016 at 10:36:44 EDT and contains the fol
		Archive Configu	e Contents uration data
		Databas The dat	se Compatibility tabases are compatible.
		Node Ty The nod	<u>ype Compatibility</u> de types are compatible.
		Topolog THE TOP Discre - Serv - Serv - Serv	gy Compatibility POLOGY IS NOT COMPATIBLE. CONTACT ORACLE CUSTOMER SERVICES BEFORE RESTORING THIS DATABA epancies: ver A1860.052 on network XMI is in the current topology but not the selected backup file ver A1860.052 on network IMI is in the current topology but not the selected backup file ver A0630.238 on network XMI is in the selected backup file but not the current topology ver B2934.011 on network XMI is in the selected backup file but not the current topology
		- ser	Archive Contents and Detabase Compatibilities must be the following:
		Note.	Archive Contents and Database Compatibilities must be the following.
			Database Compatibility : The databases are compatible.
	,	Note:	The following is expected Output for Topology Compatibility Check since we are restoring from existing backed up data base to database with just one NOAM:
			Topology Compatibility THE TOPOLOGY SHOULD BE COMPATIBLE MINUS THE NODEID.
		Note:	We are trying to restore a backed up database onto an empty NOAM database. This is an expected text in Topology Compatibility.
		4. If t	he verification is successful, click Back .

Procedure 3. Recovery Scenario 3

17.	Active NOAM: Restore the	1. Navigate to Status and Manage > Database.		
database 2. Select the Active NOAM server and click Restore.		2. Select the Active NOAM server and click Restore.		
		are Restore Man A		
		3. Select the proper back up 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, that is expected. If no other errors are displayed, mark the Force checkbox as shown above and click OK to proceed with the DB restore.		
		Database Restore Confirm		
		The selected database came from ZombieNOA		
		Archive Contents Configuration data		
		Database Compatibility		
	The databases are compatible.			
Confirm archive "backup/Backup.dsr.ZombieNOAM1.Configu		Confirm archive "backup/Backup.dsr.ZombieNOAM1.Configurat		
		Force Restore? Force Force restore		
		Ok Cancel		
		Note: After the restore has started, the user is logged out of XMI NO GUI since the restored Topology is old data.		

18. □	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		
		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.		
19.		Wait for 5-10 minutes for the System to stabilize with the new topology:		
	Monitor and confirm database restoral	Monitor the Info tab for Success . This indicates the restore is complete and the system is stabilized.		
		Ignore the following 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).		
		<i>Note</i> : Do not pay attention to alarms until all the servers in the system are completely restored.		
		<i>Note</i> : The Configuration and Maintenance information is in the same state it was when backed up during initial backup.		

Procedure 3. Recovery Scenario 3

Procedure 3. Recovery Scenario 3

20.	Active NOAM:	1. Navigate to	Status and Ma	nage > HA.	
	Set failed servers to OOS	 Status Status	s & Manage etwork Elements erver A atabase PIs rocesses		
		Hostname	Max Allowed HA Role	Description	
		ZombieNOAM1	Active •	The maximum des	
		ZombieNOAM2	OOS 💌	The maximum des	
		ZombieDRNOAM1	Standby Spare Observer	The maximum des	
		Set the Ma servers.	x Allowed HA Ro	le drop down b	box to OOS for the failed
		4. Click OK .			
		Ok Can	cel		
21. □	Active NOAM: Login	Log into the red	covered active N	DAM using SS	H terminal as admusr user.
22.	NOAM VIP GUI: Recover standby NOAM	Install the seco Second NOAN Note: Execut	nd NOAM server I Server , steps 3 e step 6 if NetBa	by executing p -5, 7 from refe ckup is used.	procedure Configure the rence [8].

Procedure 3. Recovery Scenario 3

23.	NOAM VIP GUI:	1. Navigate to Status and Manage > HA.	
	Set HA on standby NOAM	 Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Click Edit. 3. 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 Spare 4. Click OK.	
24.	NOAM VIP GUI: Restart DSR application	 4. Click OK. 1. Navigate to Status and Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Select the recovered standby NOAM server and click Restart. 	

authority table\$ 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>	
26. Install If NetBackup is used, execute Install NetBackup Client from reference [8 Client (Optional) If NetBackup is used, execute Install NetBackup Client from reference [8].
 27. NOAM VIP GUI: Perform Keyexchange with export server 1. Navigate to Administration > Remote Servers > Data Export. Administration Server Administration Software Management DATA Export DATA Export DATA Export DNS Configuration 2. Click the Task Name and click Key Exchange. Insert Edit Delete Key Exchange Transfer Now Test Transfer Key Report Task Name APDE Remote Server Username Directory on Export Server Software Server Software Management Directory on Export Server Software Management Software Management Directory on Export Server Software Management Directory on Export Server Software Management Software Management Directory on Export Server Software Management Software Managem	

Procedure 3. Recovery Scenario 3

Procedure 3.	Recoverv	Scenario 3

28. NOAM VIP GUI: Recover failed SOAM servers	 Recover failed SOAM servers (standby, spare) by repeating these steps for each SOAM server: 1. Execute Configure the SOAM Servers, steps 1-3 and 5-8, from reference [8].
	Note: If you are using NetBackup, also execute step 10.
	 If you are using NetBackup, execute Install NetBackup Client from reference [8].
29. NOAM VIP GUI: Set HA on standby SOAM	 Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Click Edit. Zombie SOAM1 Active ▼ The maximum desired HA Zombie SOAM2 OOS ▼ The maximum desired HA Zombie SOAM2 OOS ▼ The maximum desired HA Standby Spare Observer OOS 3. Select the standby SOAM server and set it to Active. 4. Click OK.

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

30.	NOAM VIP GUI: Restart DSR application	 1. Navigate to Status and Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the recovered standby SOAM server and click Restart.
31.	NOAM VIP GUI: Recover the C- level server (DA- MP, SBRs, IPFE)	 Execute Configure MP Blade Servers, Steps 1, 7, 11-14, and 17, from reference [8]. Note: Also, execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. Repeat this step for any remaining failed MP servers.
32.	NOAM VIP GUI: Set HA on all C- level servers	 Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Click Edit. For each server whose Max Allowed HA Role is set to OOS, set it to Active. ZombieDAMP1 Active Status The maximum desired HA Role for ZombieDAMI Active Spare Observer OS Click OK.

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

33.	NOAM VIP GUI: Restart DSR application on recovered C- level servers	 Navigate to Status and Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes Select the recovered C-level servers and click Restart. 	
		p Restart Rebo	
34.	NOAM VIP GUI: Enable provisioning	 1. Navigate to Status and Manage > Database. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Click Enable Provisioning. Enable Provisioning Report Inhibit/. 3. A confirmation window displays. Click OK to enable Provisioning. 	
35.	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. 	

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

36.	Active NOAM: Activate optional features	Establi Note F	Establish an SSH session to the active NOAM, login as admusr. Note For PCA Activation:		
		lf you h executi NOAM standb	nave PCA installed in the system being recovered, re-activate PCA by ng PCA Activation on Active NOAM server on recovered active server and PCA Activation on Standby SOAM server on recovered y SOAM from [13].		
		Refer to activate	o Optional Features to activate any features that were previously ed.		
		Note:	While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:		
			iload#31000{S/W Fault}		
		Note:	If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.		

Procedure 3. Recovery Scenario 3



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

38.	Active NOAM:	1. Log into the active N	IOAM using SSH termir	nal as admusr .	
	between servers	2. Execute this command:			
		\$ sudo irepstat -	m		
		Output:			
		Policy 0 ActSt	b [DbReplication]		
		RDU06-MP1 Stby			
		BC From RDU06-SO1 Act	ive 0 0.50 ^0.17%	cpu 42B/s A=none	
		CC From RDU06-MP2 Act RDU06-MP2 Active	ive 0 0.10 ^0.17 ().88%cpu 32B/s A=	none
		BC From RDU06-SO1 Act	ive 0 0.50 ^0.10%	cpu 33B/s A=none	
		CC TO RDU06-MP1 Act RDU06-N01 Active	ive 0 0.10 0.08%	cpu 20B/s A=none	
		AB TO RDU06-SO1 Act	ive 0 0.50 1%R 0.0)3%cpu 21B/s	
		RDU06-SO1 Active		-	
		AB From RDU06-NO1 Act	ive 0 0.50 ^0.04%	cpu 24B/s	
		BC TO RDU06-MP1 Act	ive 0 0.50 1%R 0.0)4%cpu 21B/s	
		BC TO RDU06-MP2 Act	ive 0 0.50 1%R 0.0)7%cpu 21B/s	
39 . □	NOAM VIP GUI: Verify the	1. Navigate to Status a	and Manager > Databa	ISE.	
	database states	Status & Manage	e		
		Network Elei	ments		
		Server 💓			
		🕅 HA			
		💽 Database			
		💮 🕅 KPIs			
		Processes			
		2. Verify the OAM Max	HA Role is either Activ	ve or Standby for N	NOAM and
		SOAM; Application I	Max HA Role for MPs is	Active; and status	s is Normal :
		Network Element	Server	Role	OAM Max HA Role
		ZombieDRNOAM	ZombieDRNOAM1	Network OAM&P	Active
		ZombieNOAM	ZombieNOAM2	Network OAM&P	Standby
		ZombieSOAM	ZombieSOAM2	System OAM	N/A
		ZombieNOAM	ZombieNOAM1	Network OAM&P	Active
		ZombieSOAM	ZombieSOAM1	System OAM	Active
		ZombieDRNOAM	ZombieDRNOAM2	Network OAM&P	Standby
		ZombieSOAM	ZombieDAMP2	MP	Active
		ZombieSOAM	ZombieSS7MP2	MP	Active
		ZombieSOAM	ZombielPFE1	MP	Active
		ZombieSOAM	ZombielPFE2	MP	Active

Procedure 3. Recovery Scenario 3

40.	NOAM VIP GUI:	1. Navigate to Status and Mana	age > HA.		
	 NOAM VIP GUI: Verify the HA status Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the row for all of the servers. Verify the HA Pole is either Active or Standby 		lby.		
		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
41.	SOAM VIP GUI: Verify the local node info	 Navigate to Diameter > Configuration Configuration Capacity Summary Connection Capacity Date Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Verify all the local nodes are set 	iguration > Lo shb	ocal Node.	
42.	SOAM VIP GUI: Verify the peer node info	 Navigate to Diameter > Configuration Configuration Capacity Summary Connection Capacity C Application Ids CEX Parameters Configuration Sets Local Nodes Peer Nodes Verify all the peer nodes are s 	iguration > Po	eer Node.	

43.	SOAM VIP GUI:	1. Navigate to Diameter > Configuration > Connections .		
	Verify the connections info	 Diameter Configuration Capacity Summary Connection Capacity Dash Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes Peer Node Groups Connections 2. Verify all the connections are shown.		
44.	SOAM VIP GUI: Enable Connections, if needed	 Navigate to Diameter > Maintenance > Connections. Maintenance Route Lists Route Groups Peer Nodes Connections Select each connection and click Enable. Alternatively, you can enable all the connections by clicking EnableAll. EnableAll Disable. 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 		
45.	SOAM VIP GUI: Enable optional features	 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 36 Click Enable. 		

46. SOAM VIP GUI : Re-enable		1. Navigate to Transport Manager > Maintenance > Transport.
	transports, if	
	needed	Maintenance
		Transport
		2. Select each transport and click Enable .
		Enable Disable Block
		3. Verify the Operational Status for each transport is Up .
47.	SOAM VIP GUI:	1. Navigate to Alarms & Events > View Active.
	Examine all	🖻 😋 Alarms & Events
	alarmo	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).
48.	NOAM VIP GUI: Examine all alarms	1. Log into the NOAM VIP if not already logged in.
		2. Navigate to Alarms & Events > View Active.
		📄 😋 Alarms & Events
		View Active
		View History
		View Trap Log
		3. Examine all active alarms and refer to the on-line help on how to address them.
		If needed, contact My Oracle Support (MOS).
49. □	Restore GUI usernames and passwords	If applicable, execute Resolving User Credential Issues after Database Restore to recover the user and group information restored.
50. □	Backup and archive all the databases from the recovered system	Execute DSR Database Backup to back up the Configuration databases.
51.	Recover IDIH	If IDIH were affected, refer to IDIH Disaster Recovery to perform disaster recovery on IDIH.

-					
52.	SNMP workaround	Refer SNMP Configuration to configure SNMP as a workaround in the following cases:			
		1. If SNMP is not configured in DSR.			
		 If SNMP is already configured and SNMPv3 is selected as enabled version. 			

Procedure 3. Recovery Scenario 3

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

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

- Recover standby NOAM server by recovering base hardware and software.
 - Recover the base hardware
 - Recover the software
- The database is intact at the active NOAM server and does not require restoration at the standby NOAM server.
 - Recover any failed SO and MP servers by recovering base hardware and software.
 - Recover the base hardware
 - Recover the software
- The database is intact at the active NOAM server and does not require restoration at the SO and MP servers.
 - Re-apply signaling networks configuration if the failed blade is an MP

Procedure 4. Recovery Scenario 4

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

Check off ($\sqrt{}$) 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 SNMP Configuration to configure SNMP as a workaround in the following cases: 1. If SNMP is not configured in DSR 2. If SNMP is already configured and SNMPv3 is selected as enabled version
2.	Gather required materials	Gather the documents and required materials listed in Required Materials section.

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		
		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 4. Recovery Scenario 4

Procedure 4. Recovery Scenario 4

4.	Active NOAM:	1. Navigate to	Status and Ma	nage > HA.	
	Set failed servers to OOS	 Status Status	 Status & Manage Network Elements Server HA Database KPIs Processes 2. Click Edit. Modifying HA attributes		
		Hostname	Max Allowed HA Role	Description	
		ZombieNOAM1	Active •	The maximum des	
		ZombieNOAM2	OOS Active	The maximum des	
		ZombieDRNOAM1	Standby Spare Observer	The maximum des	
		 Set the Ma Select OK. Ok Candidation 	x Allowed HA Ro	le to OOS for t	he failed servers.
5.	RMS NOAM	If the failed ser	ver is NOT a rack	c mount server	, skip to step 9.
	Configure BIOS	1. Configure a the RMS a	and verify the BIC Ind Blade Server	OS settings by BIOS Setting	executing procedure Configure s from reference [10].
	update firmware	2. Verify and/ Manageme	or upgrade serve ent Server Firmy	r firmware by e vare from refe	executing procedure Upgrade rence[10].
		Note: Althoug this pro	gh the procedure ocedure also app	is titled to be r lies to any rack	un on the management server, mount server.
6.	RMS NOAM Failure: Backups available	If the failed ser This step assur are NOT availa 1. Restore the Backup Me 2. If the PMA restore the	ver is NOT a rack mes that TVOE a ble, skip this ste e TVOE backup b edia. C is located on th PMAC backup b	c mount server nd PMAC back pp. by executing Ro e same TVOE y executing Ro	, skip to step 9. kups are available, if backups estore TVOE Configuration from host as the failed NOAM, estore PMAC from Backup.

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

7.	RMS NOAM Failure: Backups NOT available	This step assumes that TVOE and PMAC backups are NOT available, if the TVOE and PMAC have already been restored, skip this step . If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures:
		1. Configure and IPM Management Server from reference [10].
		2. Install PMAC from reference [10].
		3. Configure PMAC from reference [10].
		If the PMAC is NOT located on the same TVOE host as the failed NOAM, execute the following sections/procedures.
		1. Installing TVOE on Rack Mount Server(s) from reference [10].
8.	Recover failed aggregation/ enclosure switches, and OAs	 Recover failed OAs, aggregation and enclosure switches, if needed. Backups Available: 1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches
	0/10	Backups NOT available, execute:
		1. HP C-7000 Enclosure Configuration from reference [10] to recover and configure any failed OAs, if needed.
		2. Configure Enclosure Switches from reference [10] to recover enclosure switches, if needed.
9.	HP-Class	If the failed server is NOT an HP C-Class Blade, skip to step 12.
	Blade Failure: Configure blade server iLO, update firmware/BIOS settings	1. Configure Blade Server iLO Password for Administrator Account from reference [10].
		 Verify/Update blade server firmware and BIOS settings by executing Server Blades Installation Preparation from reference [10]
10.	HP-Class	If the failed server is NOT an OAM type HP C-Class Blade, skip to step 13.
	Blade Failure: Backups available	This step assumes that TVOE backups are available, if backups are NOT available, skip this step .
		 Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10].
		 Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers.
11.	HP-Class	If the failed server is NOT an OAM HP C-Class Blade, skip to step 13.
	Blade Failure:	This step assumes that TVOE backups are NOT available
	available	 Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10].
		 Configure the NOAM and/or SOAM failed TVOE server blades by executing Configure SOAM TVOE Server Blades from reference [8].
		Note: Although the title of the procedure is related to SOAMs only, execute this procedure for any failed NOAMs located on TVOE server blades.

12.	Create VMs	Execute Create NOAM/SOAM Virtual Machines to create the NOAM and SOAM VMs on failed TVOE servers.
13. □	IPM and install DSR application on failed guest/servers	 Execute IPM Blades and VMs for the failed SOAM VMs and MP blades from reference [8]. Execute Install the Application Software for the failed NOAM and SOAM VMs and MP blades from reference [8].
14. □	Install NetBackup client (Optional)	If NetBackup is used, execute Install NetBackup Client from reference [8].
15.	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> 2. Login as the guiadmin user: Oracle System Login Tue Jun 7 13:49:06 2016 EDT 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 Empire 9.0</primary_noam_vip_ip_address>
		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.

-		
16. Excl keys PMA faile	Exchange SSH keys between PMAC and	 Use the PMAC GUI to determine the Control Network IP address of the failed NOAM server VM. From the PMAC GUI, navigate to Software > Software Inventory.
	failed NOAM	2. Note the IP address for the failed NOAM server VM.
	301701	3. Log into the PMAC terminal as the admusr .
		4. From a terminal window connection on the PMAC as the admusr user, exchange SSH keys for admusr between the PMAC and the failed NOAM server VM control network IP address. When prompted for the password, enter the password for the admusr user of the NOAM server.
		<pre>\$ keyexchange admusr@<no2_control_ip address=""></no2_control_ip></pre>
		Note: If Key exchange fails, edit /home/admusr/.ssh/known_hosts and remove blank lines, and retry the keyexchange commands.
17.	NOAM VIP GUI:	1. Navigate to Configuration > Servers .
	Export the Initial configuration	Main Menu Main Menu Administration Configuration Networking Servers Server Groups Resource Domains Places Places Place Associations 2. From the GUI screen, select the failed NOAM server and click Export to generate the initial configuration data for that server.
18.	NOAM VIP: Copy configuration file to failed NOAM server	 Obtain a terminal session to the NOAM VIP, login as the admusr. Use the awpushcfg utility to copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the active NOAM to the failed NOAM server, using the Control network IP address for the failed NOAM VM. The configuration file has a filename like TKLCConfigData.<hostname>.sh.</hostname> \$ sudo awpushcfg The awpushcfg utility is interactive, so the user is prompted for the following: IP address of the local PMAC server: Use the local control network address from the PMAC. Username: Use admusr Control network IP address for the target server: In this case, enter the control IP for the failed NOAM VM).
		• Hostname of the target server: Enter the server name from Step 17 .

19.	Failed NOAM Server: Verify awpushcfg was called and reboot the server	 Establish an SSH session to the failed NOAM server, login as the admusr user. The automatic configuration daemon looks for the file named TKLCConfigData.sh in the /var/tmp directory, implements the configuration in the file, and asks the user to reboot the server. Verify awpushcfg was called by checking the following file <pre>\$</pre>	
		5 Sudo Init 6	
20.	Failed NOAM Server: Configure networking for dedicated NetBackup interface (Optional)	5. Wait for the server to reboot Note: Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup. Obtain a terminal window to the failed NOAM server, logging in as the admusr. \$ sudo /usr/TKLC/plat/bin/netAdm setdevice=netbackup type=Ethernetonboot=yes address= <no2_netbackup_ip_adress> netmask=<no2_netbackup_netmask> \$ sudo /usr/TKLC/plat/bin/netAdm addroute=net device=netbackupaddress=<no1_netbackup_network_id> netmask=<no2_netbackup_netmask> netmask=<no2_netbackup_netmask></no2_netbackup_netmask></no2_netbackup_netmask></no1_netbackup_network_id></no2_netbackup_netmask></no2_netbackup_ip_adress>	
21.	Failed NOAM Server: Verify server health	Execute this command on the 2 nd NOAM server and make sure no errors are returned: \$ sudo syscheck Running modules in class hardwareOK Running modules in class diskOK Running modules in class netOK Running modules in class systemOK Running modules in class procOK LOG LOCATION: /var/TKLC/log/syscheck/fail_log	

Procedure 4. Recovery Scenario 4

22.	NOAM VIP GUI:	1. Navigate to Status and Manage > HA.	
	Set HA on standby NOAM	 Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Click Edit. 3. 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	
		Standby Standby ZombieDRNOAM1 Spare 4. Click OK.	
23.	NOAM VIP GUI: Restart DSR application	 1. Navigate to Status and Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Select the recovered standby NOAM server and click Restart. 	
24.	NOAM VIP GUI: Recover failed SOAM servers	 Recover failed SOAM servers (standby, spare) by repeating these steps for each SOAM server: 1. Execute Configure the SOAM Servers, steps 1-3 and 5-8, from reference [8]. Note: If you are using NetBackup, also execute step 10. 2. If you are using NetBackup, execute Install NetBackup Client from 	
		reference [8].	

Procedure 4. Recovery Scenario 4

25.	NOAM VIP GUI:	 Navigate to Status and Manage > HA. 	
	Set HA on standby SOAM	 Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click Edit. 	
		3. Select the SOAM server and set it to Active .	
		Zombie SOAM1 Active The m	
		Zombie SOAM2 Spare The m Observer OOS	
		4. Click OK .	
26.	NOAM VIP GUI: Restart DSR application	 1. Navigate to Status and Manage > Server. Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files 2. Select the recovered SOAM server and click Restart. p Restart Rebc 	
27.	NOAM VIP GUI: Recover the C- level server (DA-MP, SBRs, IPFE)	1. Execute Configure MP Blade Servers , steps 1, 7, 11-14, and 17, from reference [8].	
		Note: Also execute step 15 and 16 if you plan to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network.	
		2. Repeat this step for any remaining failed MP servers.	

Procedure 4. Recovery Scenario 4

28.	NOAM VIP GUI:	1. Navigate to Status and Manage > HA .		
	Set HA on all C- level servers	 Status & Manage Network Elements Server HA Database KPIs Processes Click Edit. 		
		Active.		
		ZombieDAMP1 Active The maximum desired HA Role for ZombieDAMI		
		ZombieDAMP2 Spare The maximum desired HA Role for ZombieDAMI Observer OOS		
29.	NOAM VIP GUI:	 4. Click OK. 1. Navigate to Status and Manage > Server. 		
	Restart DSR application	 Status & Manage Network Elements Server HA Database KPIs Processes Select the recovered C-level servers and click Restart. 		
30.	Active NOAM: Login	Log into the recovered active NOAM using SSH terminal as admusr user.		
31.	Active NOAM:	1. Establish an SSH session to the active NOAM, login as admusr .		
	exchange	2. Perform a keyexchange from the active NOAM to each recovered server:		
	between the active-NOAM and recovered servers	<pre>\$ keyexchange admusr@<recovered hostname="" server=""></recovered></pre>		

32.	Active NOAM: Activate optional features	Establi Note F	sh an SSH session to the active NOAM, login as admusr . For PCA Activation:
		If you h execut standb recove	nave PCA installed in the system being recovered, re-activate PCA by ing PCA Activation on Standby NOAM Server on the recovered y NOAM server and PCA Activation on Standby SOAM server on the red standby SOAM server from [13].
		Refer t activate	o Optional Features to activate any features that were previously ed.
		Note:	While running the activation script, the following error message (and corresponding messages) output may be seen, this can safely be ignored:
			iload#31000{S/W Fault}
		Note:	If any of the MPs are failed and recovered, then these MP servers should be restarted after Activation of the feature.
33.	MP Servers:	DSR C	only, SDS Skip This Step .
	Disable SCTP auth flag (DSR Only)	For SC from re	TP connections without DTLS enabled, refer to Enable/Disable DTLS eference [14].
		Execut	e this procedure on all failed MP servers.

Procedure 4. Recovery Scenario 4

Procedure 4. Recovery Scenario 4



FIU	Flocedule 4. Recovery Scenario 4				
35. □	Active NOAM: Verify replication between	1. Log into the active N	IOAM using SSH termin	al as admusr .	
		2. Execute this comma	and:		
		\$ sudo irepstat -	·m		
	servers	Output like below is ge	nerated:		
		Policy 0 ActSt	b [DbReplication]		
		RDU06-MP1 Stby	- ,		
		BC From PDII06-SO1 Act	ive 0 0 50 ^0 17%	CDU 42B/S A=none	
		CC From RDU06-MP2 Act	ive 0 0.10 ^0.17	0 88% (1011) 32B/g A=1	none
		RDII06-MP2 Active	100 0 0.10 0.1	0.0000pu 020,5 11-1	lione
		BC From RDU06-SO1 Act	ive 0 0 50 ^0 10%	cou 33B/s A=none	
		CC TO RDU06-MP1 Act	ive 0 0.10 0.08%	cpu 20B/s A=none	
		RDU06-NO1 Active			
		AB TO RDU06-S01 Act	ive 0 0.50 1%R 0.	03%cpu 21B/s	
		RDU06-SO1 Active		0000pu 212,5	
		AB From RDU06-NO1 Act	ive 0 0.50 ^0.04%	cpu 24B/s	
		BC TO RDU06-MP1 Act	ive 0 0.50 1%R 0.	04%cpu 21B/s	
		BC TO RDU06-MP2 Act	ive 0 0.50 1%R 0.	07%cpu 21B/s	
00			- Maria - Datala		
	Verify the database states	 Status & Manag Network Ele Server HA Database KPIs Processes Verify the OAM Max SOAM and Application Normal. 	e ments : HA Role is either Activ ion Max HA Role for MP	e or Standby for NC s is Active , and that	DAM and t the status
		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
		ZombieDRNOAM		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 4. Recovery Scenario 4

Procedure 4. Recovery Scenario 4

37. NOAM VIP GUI: 1. Navigate to Status and Manager > HA.					
Verify the HA status		 Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the row for all of the serv Verify the HA Role is either Act 	ers. ive or Standb	y.	
		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
38.	SOAM VIP GUI: Verify the local node info	 Navigate to Diameter > Config Diameter Configuration Connection Capacity Dashboar Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Verify all the connections are short 	uration > Loc d nown.	al Nodes.	
39.	SOAM VIP GUI: Verify the peer node info	 Navigate to Diameter > Config Diameter Configuration Capacity Summary Connection Capacity E Application Ids CEX Parameters Configuration Sets Cocal Nodes Peer Nodes Verify all the peer nodes are shownow 	uration > Pee	er Node.	

Procedure 4. Recovery Scenario 4

40.	SOAM VIP GUI:	1. Navigate to Diameter > Configuration > Connections .		
	Verify the connections info	 Diameter Configuration Capacity Summary Connection Capacity Dash Application Ids CEX Parameters Command Codes Configuration Sets Local Nodes Peer Nodes Peer Node Groups Connections 2. Verify all the connections are shown.		
41.	SOAM VIP GUI: Enable connections, if needed	 Navigate to Diameter > Maintenance > Connections. Maintenance Route Lists Route Groups Peer Nodes Connections Select each connection and click Enable. Alternatively, you can enable all the connections by clicking EnableAll. EnableAll Disable. Verify the Operational State is Available. Note: If a Disaster Recovery was performed on an IPFE server, it may be necessary to disable and re-enable the connections to ensure proper link distribution. 		
42.	SOAM VIP GUI: Enable optional features	 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 32. Click Enable. 		

43	SOAM VIP GUI	1 Navigate to Transport Manager > Maintenance > Transport
	Re-enable transports, if needed (Applicable ONLY for DSR 6.0+)	 Transport Manager Configuration Maintenance Transport 2. Select each transport and click Enable. Enable Disable Block 3. Verify the Operational Status for each transport is United St
44.	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).
45.	NOAM VIP GUI: Examine all alarms	 Log into the NOAM VIP if not already logged in. 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).
46.	Restart oampAgent, if needed	 Note: If alarm 10012: The responder for a monitored table failed to respond to a table change is raised, the oampAgent needs to be restarted. 1. Establish an SSH session to each server that has the alarm., login as admusr. 2. Execute these commands: \$ sudo pm.set off oampAgent \$ sudo pm.set on oampAgent
47 .	Backup and archive all the databases from the recovered system	Execute DSR Database Backup to back up the Configuration databases.

Procedure 4. Recovery Scenario 4

Procedure 4.	Recovery	/ Scenario 4

48.	Recover IDIH	If IDIH were affected, refer to IDIH Disaster Recovery to perform disaster
		recovery on IDIH.

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

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

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

Procedure 5. Recovery Scenario 5

This procedure performs recovery if both NOAM servers have failed but a DR NOAM is available Check off (\checkmark) 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 SNMP Configuration to configure SNMP as a workaround in the following cases: 1. If SNMP is not configured in DSR.	
		 If SNMP is already configured and SNMPv3 is selected as enabled version. 	
		Note : The Active Network server allows SNMP administration. The Global SNMP configuration cannot be modified if DR site is made Primary. It can be updated once original site becomes Primary again.	
2.	Gather required materials	Gather the documents and required materials listed in Required Materials section.	
3.	Switch DR NOAM to primary	Refer to DSR/SDS 8.x NOAM Failover User's Guide [17].	
4.	Recover failed SOAMs	If ALL SOAM servers have failed, execute Procedure 2.	

5. □	DR-NOAM VIP GUI: Login	1. Establish a GUI session on the DR-NOAM server by using the VIP IP address of the DR-NOAM server. Open the web browser and enter a URL of:
		http:// <primary_dr-noam_vip_ip_address></primary_dr-noam_vip_ip_address>
		2. Login as the guiadmin user:
		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 5. Recovery Scenario 5

6.	6. DR-NOAM VIP 1. Navigate to Status and Manage > HA.		
	GUI: Set failed NOAM servers to standby	 Status & Manage Network Elements Server HA Database KPIs Processes 2. Click 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	
		 Set the Max Allowed HA Role drop down box to OOS for the failed servers. Click OK. Ok Cancel 	
7.	RMS NOAM Failure: Configure BIOS settings and update firmware	 If the failed server is NOT a rack mount server, skip to step 11. 1. Configure and verify the BIOS settings by executing procedure Configure the RMS and Blade Server BIOS Settings from reference [10]. 	
		 Verify and/or upgrade server firmware by executing procedure Upgrade Management Server Firmware from reference[10]. 	
		Note: Although the procedure is titled to be run on the management server, this procedure also applies to any rack mount server.	
8.	RMS NOAM Failure: Backups available	 If the failed server is NOT a rack mount server, skip to step 11. This step assumes that TVOE and PMAC backups are available, if backups are NOT available, skip this step. 1. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media. 2. If the PMAC is located on the same TVOE host as the failed NOAM, restore the PMAC backup by executing Restore PMAC from Backup. 	

9.	Recover failed aggregation/ enclosure switches, and OAs	 Recover failed OAs, aggregation, and enclosure switches, if needed. Backups available: 1. Refer to Recover/Replace Failed 3rd Party Components (Switches, OAs) to recover failed OAs, aggregation, and enclosure switches. Backups NOT available, execute: 1. HP C-7000 Enclosure Configuration from reference [10] to recover and configure any failed OAs, if needed. 2. Configure Enclosure Switches from reference [10] to recover enclosure
		switches, if needed.
10.	RMS NOAM Failure: Backups NOT available	 If the failed server is NOT a rack mount server, skip to step 11. This step assumes that TVOE and PMAC backups are NOT available, if the TVOE and PMAC have already been restored, skip this step. If the PMAC is located on the same TVOE host as the failed NOAM, execute the following sections/procedures: Configure and IPM Management Server from reference [10]. Install PMAC from reference [10]. Configure PMAC from reference [10]. If the PMAC is NOT located on the same TVOE host as the failed NOAM, execute the following sections/procedures: Install PMAC from reference [10]. If the PMAC is NOT located on the same TVOE host as the failed NOAM, execute the following sections/procedures: Installing TVOE on Rack Mount Server(s) from reference [10].
11.	HP-Class Blade Failure: Configure blade server iLO, update firmware/BIOS settings	 If the failed server is NOT an HP C-Class Blade, skip to step 14. 1. Execute Configure Blade Server iLO Password for Administrator Account from reference [10]. 2. Verify/Update Blade server firmware and BIOS settings by executing Server Blades Installation Preparation from reference [10]
12.	HP-Class Blade Failure: Backups available	 If the failed server is NOT an OAM type HP C-Class Blade, skip to step 14. This step assumes that TVOE backups are available. If backups are NOT available, skip this step. 1. Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10]. 2. Restore the TVOE backup by executing Restore TVOE Configuration from Backup Media on ALL failed TVOE Host blade servers.
13.	HP-Class Blade Failure: Backups NOT available	If the failed server is NOT an OAM type HP C-Class Blade, skip to step 14 . This step assumes TVOE backups are NOT are available. Install and configure TVOE on failed TVOE blade servers by executing Install TVOE on Blade Servers from reference [10].

Procedure 5.	Recovery Scenario 5						
--------------	----------------------------						
14.	Execute fast deployment file for NOAMs	 The backup fdconfig file used during the initial DSR installation is available on the PMAC, if a database backup was restored on the PMAC. If a backup fast deployment xml is NOT available, execute Configure NOAM Servers from reference [8]. If a backup fast deployment xml is already present on the PMAC, execute the following procedure: 1. Edit the .xml file with the correct TPD and DSR ISO (Incase an upgrade bas been performed since initial installation). 					
-----	--	---	--	--	--	--	--
		2. Execute these commands:					
		<pre>\$ cd /usr/TKLC/smac/etc \$ screen \$ sudo fdconfig configfile=<created_fd_file>.xml</created_fd_file></pre>					
15.	DR-NOAM VIP GUI: Export the initial configuration	 Navigate to Configuration > Servers. Main Menu Administration Configuration Networking Servers Server Groups Resource Domains Places Place Associations From the GUI screen, select the failed NOAM server and click Export to generate the initial configuration data for that server. 					
16.	DR-NOAM VIP GUI: Copy configuration file to failed NOAM server	 Obtain a terminal session to the DR-NOAM VIP, login as the admusr user. Configure the failed NOAM server: \$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<failed_noam_hostnam< li=""> sh admusr@<failed_noam_xmi_ip_address>:/var/tmp/TKLCConfigData.ta.sh</failed_noam_xmi_ip_address> </failed_noam_hostnam<> 					

Procedure 5.	Recovery	Scenario 5
--------------	----------	------------

-							
17. □	Recovered NOAM Server:	 Establish an SSH session to the Recovered NOAM server (Recovered_NOAM_xmi_IP_address) 					
	Verify configuration was called and reboot the server	2. Login as the admusr user.					
		 The automatic configuration daemon looks for the file named TKLCConfigData.sh in the /var/tmp directory, implements the configuration in the file, and asks the user to reboot the server. 					
		4. Verify awpushcfg was called by checking the following file.					
		<pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log Verify this message displays: [SUCCESS] script completed successfully!</pre>					
		5. Now reboot the server:					
		\$ sudo init 6					
		6. Wait for the server to reboot					
18. 	Recovered NOAM Server: Configure	<i>Note</i> : Only execute this step if your NOAM is using a dedicated Ethernet interface for NetBackup.					
	networking for	<pre>\$ sudo /usr/TKLC/plat/bin/netAdm setdevice=netbackup</pre>					
	dedicated	type=Ethernetonboot=yes					
	netbackup	address= <no2_netbackup_ip_adress></no2_netbackup_ip_adress>					
	(Optional)	netmask= <no2_netbackup_netmask></no2_netbackup_netmask>					
		\$ sudo /usr/TKLC/plat/bin/netAdm addroute=net					
		device=netbackupaddress= <no1_netbackup_network_i< th=""></no1_netbackup_network_i<>					
		netmask= <no2_netbackup_netmask></no2_netbackup_netmask>					
		gateway= <no2_netbackup_gateway_ip_address></no2_netbackup_gateway_ip_address>					
19. □	Recovered NOAM Server:	Execute this command on the failed NOAM server and make sure no errors are returned:					
	verify server	\$ sudo syscheck					
	liouiti	Running modules in class hardwareOK					
		Running modules in class diskOK					
		Running modules in class netOK					
		Running modules in class systemOK					
		Running modules in class procOK					
		LOG LOCATION: /var/TKLC/log/syscheck/fail_log					
20.	Repeat for additional 2 nd failed NOAM	Repeat steps 15-19 for the 2 nd failed NOAM server.					

Procedure 5.	Recovery Scenario 5
--------------	----------------------------

21.	Perform keyexchange between active NOAM and recovered NOAMs	 Perform a keyexchange between the newly active NOAM and the recovered NOAM servers: 1. From a terminal window connection on the active NOAM as the admusr user, exchange SSH keys for admusr between the active NOAM and the recovered NOAM servers using the keyexchange utility, using the host names of the recovered NOAMs. 						
		2. When prompted for the password user of the recovered NOAM ser	d, enter the password for the admusr vers.					
		<pre>\$ keyexchange admusr@<reco< pre=""></reco<></pre>	vered_NOAM Hostname>					
22.	NOAM VIP GUI: Set HA on recovered NOAMs	 Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes Click Edit. For each NOAM server whose Max Allowed HA Role is set to Standby, set it to Active. 						
		ZombieDAMP1 Active Active Standby	ZombieDAMP1 Active The maximum desired HA Role for ZombieDAMI					
		ZombieDAMP2 Spare Observer OOS	The maximum desired HA Role for ZombieDAMI					
		4. Click OK .						
23.	NOAM VIP GUI: Restart DSR application	 Navigate to Status and Manage Status & Manage Network Elements Server HA Database KPIs Processes Select each recovered NOAM set Stop Restart Reboot 	erver and click Restart .					

		-		
24.	Recovered NOAM Servers: Activate optional features	 Policy and Charging Application (PCA) Activate the feature Policy and Charging Application (PCA) as follows: For PCA: Establish SSH sessions to the all the recovered NOAM servers and login as admusr. Refer [13] and execute PCA Activation on Standby NOAM Server on all recovered NOAM servers to re-activate PCA. Establish SSH session to the recovered active NOAM, login as admusr. Note: If any of the MPs are failed and recovered, then these MP servers should be restarted after activation of the feature. 		
25.	Switch DR NOAM back to secondary	Once the system have been recovered, refer to DSR/SDS 8.x NOAM Failover User's Guide [17].		
26.	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.) 		
27.	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.		
28.	Recover IDIH	If IDIH were affected, refer to IDIH Disaster Recovery section to perform disaster recovery on IDIH.		

Procedure 5. Recovery Scenario 5

4.6 Recovery Scenario 6 (Database Recovery)

4.6.1 Recovery Scenario 6: Case 1

For a partial outage with

- Server having a corrupted database
- Replication channel from parent is inhibited because of upgrade activity; or
- Server is in a different release then that of its active parent because of upgrade activity
- Verify the server runtime backup files, performed at the start of the upgrade, are present in /var/TKLC/db/filemgmt area in the following format
 - Backup.DSR.HPC02-NO2.FullDBParts.NETWORK_OAMP.20140524_223507.UPG.tar.bz2
 - Backup.DSR.HPC02-NO2.FullRunEnv.NETWORK_OAMP.20140524_223507.UPG.tar.bz2
- *Note*: During recovery, the corrupted database is replaced by the server runtime backup. Any configuration done after taking the backup is not available post recovery.

Procedure 6. Recovery Scenario 6 (Case 1)

This procedure performs recovery if database is corrupted in the system Check off (\checkmark) each step as it is completed. Boxes have been provided for this purpose under each step number.								
lf th	If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.							
1.	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: 						
		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 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.	NOAM VIP GUI: Set failed servers to standby	 Navigate to Status and Manage > HA. Status & Manage Network Elements Server HA Database KPIs Processes 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 drop down box to OOS for the failed servers					
		4. Click CK					
		Ok Cancel					
3.	Server in Question: Login	Establish an SSH session to the server in question. Login as admusr .					
4.	Server in	Bring the system to runlevel 3.					
	Question: Change runlevel to 3	\$ sudo init 3					
5.	Server in	Execute this command and follow the instructions appearing in the console					
	Question: Recover	prompt.					
	system	<pre>\$ sudo /usr/TKLC/appworks/sbin/backout_restore</pre>					
6.	Server in	Bring the system back to runlevel 4.					
	Question : Change runlevel to 4	\$ sudo init 6					

Procedure 6. Recovery Scenario 6 (Case 1)



Procedure 6. Recovery Scenario 6 (Case 1)

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)

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

Check off ($\sqrt{}$) each step as it is completed. Boxes have been provided for this purpose under each step number.

1. NOAM VIP GUI: Login 1. Establish a GUI session on the NOAM server by using the VIP IP a 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,			
		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.	NOAM VIP GUI: Set failed servers to standby	 Navigate to Status Status<!--</th--><th>o Status and Mar s & Manage etwork Elements erver A atabase Pls occesses</th><th>nage > HA.</th><th></th><th></th>	o Status and Mar s & Manage etwork Elements erver A atabase Pls occesses	nage > HA.				
		Hostname	Max Allowed HA Role	Description				
		ZombieNOAM1	Active 💌	The maximum des				
		ZombieNOAM2	OOS Active	The maximum des	s			
		ZombieDRNOAM1	Standby Spare Observer	The maximum des	5			
		3 Set the Max Allowed HA Role drop down box to OOS for the failed set						
		4. Click OK .						
		Ok Cancel						
3. □	Server in Question: Login	Establish an S	SH session to the	e server in que	stion. Login as adm	usr.		
4.	Server in	Stop the httpd :	service.					
	Question: Stop	\$ sudo bas	h -l					
		\$ service	httpd stop					
5.	Server in	Take the serve	r out of service.					
	Question: Take server out of service	\$ prod.clobber						
6.	Server in	Take the serve	r to Dbup and sta	art the DSR ap	plication.			
	Question: Take server to	\$ prod.sta	rt					
	DbUp state and start the							

Procedure 7. Recovery Scenario 6 (Case 2)

7.	Server in	1. Start the httpd service.					
	Question: Start httpd service	\$ service httpd start					
		2. Exit out of	root.			J	
		¢ evit				1	
Q		1 Novigate t	• Status and M:		۸		
	GUI: Set failed servers to active	 Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Click Edit at the bottom of the screen. 					
		3. Select the	failed server and	d set it to A	ctive.		
		Modifying HA attributes					
		Hostname	Max Allowed HA Role	Description			
		ZombieNOAM1	Active 💌	The maximum			
		ZombieNOAM2	Active Active	The maximum			
		ZombieDRNOAM1 4. Click OK.	Standby Spare	The maximum			
9.	NOAM VIP	1. Navigate t	o Status and Ma	anage > Se	erver.		
	GUI : Restart DSR application	 Status & Manage Network Elements Server HA Database KPIs Processes Select each recovered server and click Restart. Restart Rebo 					

Procedure 7. Recovery Scenario 6 (Case 2)



Procedure 7. Recovery Scenario 6 (Case 2)

5. Resolving User Credential Issues after Database Restore

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

Perform this procedure to keep users restored by system restoration.

Check off ($\sqrt{}$) each step as it is completed. Boxes have been provided for this purpose under each step number.

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: 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 System Login Tue Jun 7 13:49:06 2016 EDT Image: Comparison of the com		

Procedure 8.	Keep Restored Use	r
--------------	-------------------	---



5.3 Remove a Restored User

Procedure 9. Remove the Restored User

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 1. Establish a GUI session on the NOAM server by using the VIP IP add of the NOAM server. Open the web browser and enter a URL of: http:// <primary_noam_vip_ip_address> 2. Login as the guiadmin user: Oracle System Login</primary_noam_vip_ip_address>			
		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 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:

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

5.5 Restore an Archive that does not contain a Current User

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

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

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

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

Perf	Perform this procedure to remove users restored by system restoration.		
Che num	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.		
lf thi	is procedure fails, i	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:	 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:	
ORACLE® Oracle System Login		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 10. Restore an Archive That Does Not Contain a Current User

4.	After Restoration:	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:		
	Login	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 10. Restore an Archive That Does Not Contain a Current User

FIU		Te all Archive That I	Does Not Contain a	
5.	After restoration: recreate affected user	 Navigate to Adr Main Menu Administration General Op Access Con Users Groups Session Certifica Authorize SFTP Users 2. Click Insert. Insert Edit 3. Recreate the use Adding new user	ninistration > Acces tions ttrol s te Management ed IPs sers De eer using the data coll	ected from step 3.
		Username *		Sele long
		Group *	admin 🔶	Sele
		Authentication Options	Allow Remote Authentication	Sele "Adr actic [Def
		Access Options	 ✓ Allow GUI Access ✓ Allow MMI Access 	Sele
		Access Allowed	Account Enabled	Is th
		Maximum Concurrent Logins	0	The
		Session Inactivity Limit	120	The
		Comment*		Con
		4. Click OK .		
6.	After Restoration: Repeat for additional users	Repeat step 5 to rec	create additional user	S.

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

7.	After Restoration: Reset the	See Procedure 8 for resetting passwords for a user.
	passwords	

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 hostname-upgrade_xx-xx-xx.xml file format. It took out the oracle server installation part since for disaster recovery it is not needed.

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

Procedure 11. IDIH Disaster Recovery Preparation

This procedure performs disaster recovery preparation steps for the IDIH. Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.			
1.	PMAC GUI:	1. Open web browser and enter:	
	Login	http:// <pmac_mgmt_network_ip></pmac_mgmt_network_ip>	
		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.	

2.	PMAC GUI: Verify necessary IDIH images are available	 Navigate to Software > Manage Software Images. Software Software Inventory Manage Software Images Verify the current IDIH TVOE, TPD, Oracle, Application and Mediation images are listed. Note: If the necessary software images are not available, follow the instructions from Load Application and TPD ISO onto PMAC Server 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.	Perform database health check	<pre>Periorin a database nearin check: \$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i Output: admusr@thunderboltcors [admusr@thunderbolt-ora -]\$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i 10:10:52: sTARTING HEALTHCHECK PROCEDURE 10:10:52: sTARTING HEALTHCHECK PROCEDURE 10:10:52: strap vsstow: 7.0.10.0-66.20.0 10:10:52: how disk space issues found 10:10:52: how disk space issues found 10:10:52: checking disk free space 10:10:52: checking syscheck - this can take a while 10:10:52: how orrors in syscheck modules 10:10:53: checking statefiles 10:10:53: checking statefiles 10:11:00: checking unlevel 10:11:00: checking unlevel 10:11:00: checking unprade log 10:11:00: Statefiles do not exist 10:11:00: checking unprade log 10:11:00: NTP deamon is running 10:11:00: NTP deamon is running 10:11:00: Server is synchronized with ntp server 10:11:00: Ntp status 10:11:00: Ntp status in degrated 10:11:00: Ntp status is nost file. 10:11:00: Checking server entries in host file. 10:11:00: Ting server is present in /etc/hosts 10:11:00: Ping server oracle 10:11:00: Ping server addition 10:11:00: Ping server addition 10:11:00: Ping server addition 10:11:00: Ping server addition 10:11:00: Check cacle Server 10:11:00: Check ca</pre>
		[admusr@thunderbolt-ora ~]\$

Procedure 11. IDIH Disaster Recovery Preparation



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

Check off ($\sqrt{}$) each step as it is completed. Boxes have been provided for this purpose under each step number.

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 ED1
		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.
2.	Remove existing application server	1. Navigate to Main Menu > VM Management.
		Software
		Manage Software Images
		M Management
		2. Select the application guest.
		3. Click Delete.
		Edit Delete Clone
		Upgrade
		Patch

3.	Remove existing mediation server	 Navigate to Main Menu > VM Management. Software Software Inventory Manage Software Images VM Management Select the Mediation guest. 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	<pre>Execute this command (Enter your upgrade file): \$ cd /var/TKLC/smac/guest-dropin \$ screen \$ sudo fdconfig configfile=<hostname-upgrade_xx-xx- xx="">.xml</hostname-upgrade_xx-xx-></pre>
		STOP
		IIWarning!! If you run the fdconfig without "upgrade" in the XML filename, the database is
		 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.

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



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

Appendix A. DSR Database Backup

Procedure 13. DSR Database Backup

The SOA	The intent of this procedure is to back up the provision and configuration information from an NOAM or SOAM server after the disaster recovery is complete			
Che num	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.			
1.	NOAM/SOAM VIP: Login	 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 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.	NOAM/SOAM VIP: Backup configuration data for the system	 Navigate to Status and Manage > Database. Status & Manage Network Elements Server A HA Database KPIs Processes Select the active NOAM server and click Backup.
		plication Backup Compa 3. Make sure that the Configuration checkbox is marked. Database Backup
		Field Value
		Server: ZombieNOAM1
		Select data for backup
		© gzip Compression *
		Archive Name * Backup.dsr.ZombieNOAM1.Configuration.NETV
		Comment
		Ok Cancel
		4. Enter a filename for the backup and click OK .

3.	NOAM/SOAM	1. Navigate to Status and Manage > Files.							
	VIP: Verify the	🗒 🗁 Status & Manage							
	existence	Metwork Elements							
		Server							
		KPIs Processes							
		Files							
		Main Menu: Status & Manage -> Files							
		Filter* Tasks							
		ZombieNOAM1 ZombieNOAM2 ZombieDRNOAM1 ZombieDRNOAM2 ZombieSOAM1 ZombieSOA							
		File Name							
		Lbackup/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.ZombieSOAM1.sh							
		TKLCConfigData.ZombieSOAM2.sh							
		ugwrap.log							
		upgrade.log							
		2. Select the active NOAM or SOAM tab.							
		3. The files on this server display. Verify the existence of the backup file.							
4									
4.	VIP Download	1. From the previous step, select the backup file.							
	the file to a	2. Click Download .							
	local machine								
		bload Download							
		GB available I System ut							
		3 Click OK to confirm the download							
5.	Upload the image to secure location	where the server backup files are located in case of system disaster recovery.							
6.	Backup active SOAM	Repeat Steps 2 through 5 to back up the active SOAM.							

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

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

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

The intent of this procedure is to recover a failed Aggregation (4948E/4948E-F) Switch. Prerequisites for this procedure are:

- A copy of the networking xml configuration files
- A copy of HP Misc Firmware DVD or ISO
- IP address and hostname of the failed switch
- Rack Mount position of the failed switch

Refer to Appendix M for the workaround on cipher mismatch issue with Cisco switches.

Check off ($\sqrt{}$) each step as it is completed. Boxes have been provided for this purpose under each step number.

1.	Recover failed Aggregation Switches: Cisco	Log into the PMAC using SSH as admusr .					
		Remove the old SSH key of the switch from the PMAC by executing this command from a PMAC command shell:					
	4940E/4940E-F	sudo ssh-keygen -R <4948_switch_ip>					
		Refer to procedure Replace a failed 4948/4948E/4948E-F switch (c-Class system) (netConfig) to replace a failed Aggregation switch from reference [2].					
		Note : You need a copy of the HP Misc Firmware DVD or ISO (or firmware file obtained from the appropriate hardware vendor) and the original networking XML files custom for this installation. These are either stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.					
		<i>Note</i> : Copy switch appropriate init file and use it for respective switch:					
		Copy the switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy 'switch1A_4948_4948E_init.xml'.					
		The templates can be found using the following method:					
		1. From the PMAC CLI					
		df grep -I DSR					
		Sample output:					
		/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso					
		1118514 0 100% /usr/TKLC/smac/html/TPD/DSR- 8.2.0.0.0_82.4.0-x86_64 0 100% /usr/TKLC/smac/html/TPD/DSR-					
		/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso					
		1118372 1118372 0 100% /usr/TKLC/smac/html/TPD/DSR- 8.2.0.0.0 82.4.0-x86 64					
		/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0-x86_64.iso					
		1117976 1117976 0 100% /usr/TKLC/smac/html/TPD/DSR- 8.2.0.0.0_82.4.0-x86_64					
		2. From the output of step 1, determine the applicable directory of the DSR release being recovered.					

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

	cd usr/TKLC/smac/html/TPD/<dsr dir="" release="">/upgrade/overlay/</dsr>							
	Example:							
	cd /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-							
	x86_64/upgrade/overlay/							
	4. Locate the DSR_NetConfig_Templates.zip file.							
	Example:							
	\$ 11							
	total 286							
	-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
	-rr 1	root	root	13346	Feb	21	19:18	DSR_NOAM_FD_RMS.xml
	dr-xr-xr-x 2	root	root	2048	Feb	21	19:18	RMS
	-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	128703	Feb	21	19:18	UpgradeHCplugin.php-ovl
	-rr 1	root	root	19658	Feb	21	19:18	upgradeHealthCheck-ovl
	5. Unzip the switch init	DSR t file.	_Net	Config_	Tem	npla	ates.zi	p file and retrieve the required
	Example:							
	\$ unzip DS	R Ne	tCon	fia Te	empl	at	es.zi	q
	6 Edit the d	_ esire	d file v	with site	sne	cifi	r detail	The existing file from original
	deployment /usr/TKLC/smac/etc/switch/xml can be used as a reference.							
	7. Copy the	new i	nit file	e to the	/usr/	тк	LC/sm	ac/etc/switch/xml dir.
	Example:							
	\$ cp <swit< th=""><th>ch_x</th><th>ml_f</th><th>ile> /</th><th>′usr</th><th>/T</th><th>KLC/s</th><th>mac/etc/switch/xml/</th></swit<>	ch_x	ml_f	ile> /	′usr	/T	KLC/s	mac/etc/switch/xml/

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

The intent of this procedure is to recover a failed Enclosure (3020) Switch. Prerequisites for this procedure are:

- A copy of the networking xml configuration files
- A copy of HP Misc. Firmware DVD or ISO
- IP address and hostname of the failed switch
- Interconnect Bay position of the enclosure switch

Refer to Appendix M for the workaround on cipher mismatch issue with Cisco switches.

Check off ($\sqrt{}$) 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.	Recover Failed Enclosure Switch: Cisco 3020	 Log into the PMAC using SSH as admusr. 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 <enclosure_switch_ip></enclosure_switch_ip></pre>			
		3. Refer to procedure Replace a failed 3020 switch (netConfig) to replace the failed enclosure switch from reference [2].			
		Note: You need a copy of the HP Misc Firmware DVD or ISO and of the original networking xml files custom for this installation. These either be stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.			

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

The intent of this procedure is to recover a failed Enclosure (6120XG/6125XLG/6125G) Switch. Prerequisites for this procedure are:

• A copy of the networking xml configuration files

Refer to Appendix M for the workaround on cipher mismatch issue with Cisco switches.

Check off ($\sqrt{}$) each step as it is completed. Boxes have been provided for this purpose under each step number.

1.	Recover Failed Enclosure Switch: HP 6120XG/6125XL G/6125G	 Log into the PMAC using SSH as admusr. 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 <enclosure_switch_ip></enclosure_switch_ip></pre>
		 Refer to procedure Replace a failed HP (6120XG, 6125G, 6125XLG switch (netConfig) to replace the failed enclosure switch from reference [2]
		Note: You need a copy of the HP Misc Firmware DVD or ISO and of the original networking xml files custom for this installation. These are either stored on the PMAC in a designation location, or the information used to populate them can be obtained from the NAPD.

Flocedule 10. Recove							
	<i>Note</i> : Copy switch appropriate init file and use it for respective switch:						
	4. Copy the switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy 'switch1A_4948_4948E_init.xml'.						
	The templates can be found by the following method: a. From the PMAC CLI:						
	al grep -1 DSK						
	x86_64.iso						
	1118514 1118514 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64						
	<pre>/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0- x86_64.iso</pre>						
	1118372 1118372 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64						
	<pre>/var/TKLC/smac/image/repository/DSR-8.2.0.0.0_82.4.0- x86_64.iso</pre>						
	1117976 1117976 0 100% /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0-x86_64						
	 b. From the output of step 1, determine the applicable directory of the DSR release being recovered. 						
	C. cd usr/TKLC/smac/html/TPD/ <dsr release<br="">dir>/upgrade/overlay/</dsr>						
	Example:						
	cd /usr/TKLC/smac/html/TPD/DSR-8.2.0.0.0_82.4.0- x86_64/upgrade/overlay/						
	d. Locate the DSR_NetConfig_Templates.zip file.						
	Example:						
	\$ 11						
	total 286						
	-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						
	-rr 1 root root 13346 Feb 21 19:18 DSR_NOAM_FD_RMS.xml						
	dr-xr-xr-x 2 root root 2048 Feb 21 19:18 RMS						
	-rrr 1 root root 812 Feb 21 19:18 SAMPLE-NetworkElement.Xml						
	-r - r - r - r - 1 root root 2186 Feb 21 19:18 TWOEcfa sh						
	-r-xr-xr-x 1 root root 598 Feb 21 19:18 TVOEclean sh						
	-rr 1 root root 128703 Feb 21 19:18 UpgradeHCplugin.php-ovl						
	-rr 1 root root 19658 Feb 21 19:18 upgradeHealthCheck-ovl						
	 e. Unzip the DSR_NetConfig_Templates.zip file and retrieve the required switch init file. 						
	Example:						
	\$ unzip DSR_NetConfig_Templates.zip						
	l						

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

f	. 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.
Ş	g. Copy the new init file to the /usr/TKLC/smac/etc/switch/xml dir.
Exar	nple:
\$ CI	<pre>switch_xml_file> /usr/TKLC/smac/etc/switch/xml/</pre>
Note	While restoring 6120XG switch, some features enabled on a 6120XG may not restore properly if they reference a port channel that does not currently exist on the switch ahead of the restore operation. Identify any port channels that need to be created on the switch according to the backup file and create them before restoring the configuration:
\$ sı "^tı	udo /bin/cat <switch_hostname>-backup /bin/grep runk"</switch_hostname>
Exar	nple output:
trur	nk <int list=""> Trk<id> LACP</id></int>
trur	nk <int list=""> Trk<id> Trunk</id></int>
5. 2 0	f any port-channels are found, then for each portchannel identified by the above command, use the netConfig setLinkAggregation command to create it and the netConfig showConfiguration command to verify its configuration:
6. l	f an LACP port channel was found, add the port-channel with this command:
\$ su devi id=<	udo /usr/TKLC/plat/bin/netConfig ice=6120XG_IOBAY2 setLinkAggregation <id> addPort=tenGE<int list=""> mode=active</int></id>
7. I	f a Trunk port-channel was found (as labeled after the Trk<id></id>), add the port-channel with this command:
\$ su devi id=<	ado /usr/TKLC/plat/bin/netConfig ice=6120XG_IOBAY2 setLinkAggregation <id> addPort=tenGE<int list=""> mode=static</int></id>
Verif	y the port-channels were added to the running configuration:
\$ sı devi	udo /usr/TKLC/plat/bin/netConfig ice=6120XG_IOBAY2 showConfiguration grep "^trunk"
trur	nk <int list=""> Trk<id> LACP</id></int>
trur	nk <int list=""> Trk<id> Trunk</id></int>
8. F	For all switch types and configurations found, use netConfig to restore the configuration:
\$ su devi serv	udo /usr/TKLC/plat/bin/netConfig ice= <switch_hostname> restoreConfiguration vice=ssh_service filename=<switch_hostname>-backup</switch_hostname></switch_hostname>
Note	This causes the switch to reboot. It takes approximately 120-180 seconds before connectivity is restored.
Note : For information ab Hardware and Software	out Downgrade Firmware on a 6125 Switch, see [10] DSR C-Class Installation Procedure 1/2.

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

Procedure 17. Recover a Failed Enclosure OA

The intent of this procedure is to recover a failed Enclosure Onboard Administrator.
 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. Recover Failed Enclosure OA
 Refer to procedure Restore OA Configuration from Management Server to replace a failed Enclosure OA from reference [2].

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

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

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

1.	Active NOAM: Login	Log into the active NOAM server using SSH as admusr .					
2 .	Active NOAM: Inhibit replication on all C-level servers	Execute this comm \$ for i in \$("nodeId like site>'"); do where "nodeNa Note: SOAM Site active NOA	hand: iqt -p -z 'C*' and iset -fin me='\$i'"; e_NE name of AM GUI and	-h -fhostName siteId=' <soam hibitRepPlans= done of the site can be fo navigating to Conf</soam 	NodeInfo Site_NE r 'A B' Noc pund out by iguration >	o where name of the deInfo logging into the Server Groups .	
Please see the snapshot below for more details, for example, if belongs to the site being recovered, then siteID is SO_HPC03.							
		Hostname	Role	System ID	Server Group	Network Element	
		ZombieNOAM1	Network OAM&P		ZombieNOAM	ZombieNeOAM	
		ZombieNOAM2	Network CAMAP		ZombieNOAM	ZombielsOAM	
		ZombieDRNOAM1	Network CABISP		ZombieDRNOAM	ZombieDRNOAM	
		ZombieDRbsD44/2	Network CAM&P		ZombieDRNOAM	ZombieDRINDAM	
		ZombieSCAM1	System CAM		ZombieSOAM	ZombieSDAM	
		ZombieSO4M2	System OAM		ZombieSOAM	ZumbieSCAM	
		ZombieDA8P1	ШÞ		ZombieD4MP	ZombieSCAM	
		ZombieDAMP2	MP		ZombieDAMP	ZombieSCAM	

3.	Active NOAM: Verify replication has been Inhibited	After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled. Verification of replication inhibition on MPs can be done by analyzing NodeInfo output. InhibitRepPlans field for all the MP servers for the selected site, for example, Site SO_HPC03 is set as A B .					
		Execute this command:					
		\$ iqt NodeInf	C				
		Output:					
		nodeId nodeName excludeTables	hostName	nodeCapability	inhibitRepPlans	siteId	
		A1386.099 NO.	. NO1	Active		NO_HPC03	
		B1754.109 SOI	. SO1	Active		SO_HPC03	
		C2254.131 MP2	2 MP2	Active	A B	SO_HPC03	
		C2254.233 MP3	MP1	Active	A B	SO_HPC03	

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

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

Procedure 19. Un-Inhibit A and B Level Replication on C-level Servers

The intent of this procedure is to Un-inhibit A and B level replication on all C-level servers of this site							
Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.							
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.							
1.	Active NOAM: Login	Log into the active NOAM server using SSH as admusr .					

2.	Active NOAM: Un-Inhibit replication on all C-level servers	Execute this command:					
		<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 Note: SOAM Site NE name of the site can be found out by logging into the active NOAM GUI and navigating to Configuration > Server Groups. Please see the snapshot below for more details, for example, if ServerSO1 belongs to the site being recovered, then siteID is SO_HPC03. Main Menu: Configuration > Servers</soam_site_ne_name></pre>					
		Filter" • Indo" •		<i>6</i> 2			
		Hostname	Rok		System 10	Server Group	Network Element
		ZombieNOAM1	Net	work OAM&P		ZombielNOAM	ZombieNOAM
		ZombieNO4M2	Net	work OAM&P		ZombieNOAM	ZombieNOAM
		ZombieDRNOAtr1	Neb	WORK CABIEP		ZombieDRNOAM	ZombieDRNOAM
		ZombieDRIVO4842	tieth	work CANNEP		ZombieDRHQAM	ZombieDRNOAM
		ZombieSOAM1	Syst	tem OAM		ZombieSOAM	ZombieSOAM
		ZombieSO4M2	Set	tem 04M		ZombieSOAM	ZombieSOAM
		ZombieDAMP1	ШÞ			ZombieD4MP	ZombieSGAM
		ZombieDAMP2	шР			ZombieDAMP	ZombieSOAM
3.	Active NOAM: Verify replication has been Inhibited	After executing above steps to un-inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled. Verification of replication un-inhibition on MPs can be done by analyzing NodeInfo output. The InhibitRepPlans field for all the MP servers for the selected site, for example, Site SO_HPC03 is set as A B . Execute this command:					
		\$ sudo iqt NodeInfo					
		Output: nodeId no excludeTables A1386.099 B1754.109	odeName 5 NO1 SO1	hostName NO1 SO1	nodeCapability Active Active	inhibitRepP	lans siteId NO_HPC03 SO_HPC03
		C2254.131	MP2	MP2	Active	A B	SO_HPC03
		C2254.233	MP1	MP1	Active	A B	SO_HPC03

Procedure 19. Un-Inhibit A and B Level Replication on C-level Servers

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

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

The intent of this procedure is to inhibit A and B level replication on all C-level servers of this site when active, standby, and spare SOAMS are lost Check off ($\sqrt{}$) 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. Active NOAM: Log into the active NOAM server using SSH as admusr. 1. Login \square 2. Active NOAM: Execute the script from /usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh, Inhibit if available. replication on all If the /usr/TKLC/dsr/tools/ path does not have the C-level servers InhibitReplicationToCLevel.sh script, then use this manual command. /usr/TKLC/dsr/tools/InhibitReplicationToCLevel.sh -replication=inhibit --SO_SG_Name=<SOAM server group name> Alternatively to the above script, if the script is not in the specific path: \$ for i in \$(sudo Imysql.client -B -N -e " SELECT DISTINCT CS.hostname FROM appworks.Server CS, appworks.Server PS, appworks.Server2SG C2SG, appworks.Server2SG P2SG, appworks.ServerGroup CSG, appworks.ServerGroup PSG, comcol.ClusterInfo CCI, comcol.ClusterInfo PCI, comcol.ClusterGroupInfo WHERE CS._h_Server_ID = C2SG._h_Server_ID AND C2SG._h_SG_ID = CSG._h_SG_ID AND CSG.clusterId = CCI.clusterId AND CCI.groups = comcol.ClusterGroupInfo.groupId AND comcol.ClusterGroupInfo.parentGroup = PCI.groups AND PCI.clusterId = PSG.clusterId AND PSG.ServerGroupName= '<SOAM_SG_NAME>' "); do iset -finhibitRepPlans='A B' NodeInfo where "nodeName='\$i'"; done Note: SOAM SG NAME is the name of the server group found by logging into the active NOAM GUI and navigating to Configuration > Server Groups. For example, if SOAM1 belongs to the site being recovered, then the server group is SO_SG. Network Element DSR_DR_NO_NE Server DRNOAM1 Node HA Pref VIPs DRNO_SG ά. NONE DRNOAM2 Network Element DSR_NO_NE DSR (active/standby 1 Server Node HA Pref NO SG NONE NOAM1 NOAM2 Network Element DSR_SO_NE DSR (active/standby Server SOAM1 SOAM2 Node HA Pref VIPs SO_SG NO_SG в
|--|

3.	Active NOAM: Verify replication has been inhibited	After executing above steps to inhibit replication on MP(s), no alarms on GUI would be raised informing that replication on MP is disabled. Verification of replication inhibition on MPs can be done by analyzing Nodeln output. InhibitRepPlans field for all the MP servers for the selected server group, for example, server group SO_SG is set as A B . Execute this command:					
		\$ iqt No	deInfo				
		Output:					
		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)

Procedure 21. Un-Inhibit A and B Level Replication on C-Level Servers

The intent of this procedure is to Un-inhibit A and B level replication on all C-level servers of this site when active, standby and spare SOAMS are lost.

Check off ($\sqrt{}$) 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:	Log into the active NOAM server using SSH as admusr.
	Login	

Procedure 21	. Un-Inhibit A and E	3 Level Replication	on C-Level Servers
--------------	----------------------	---------------------	--------------------

Active NOAM							
Un-Inhibit	if available.	ript	from /usr/T	KLC/dsr/	tools/In	hibitReplicationToCLevel.sh	
replication on all C-level servers	If the /usr/TKLC/dsr/tools/ path does not have the InhibitReplicationToCL evel sh script, then use this manual command						
	/usr/TKLC/d	sr, =a	/tools/In	hibitRe SG Nam	plicat e= <soz< th=""><th>ionToCLevel.sh</th></soz<>	ionToCLevel.sh	
	Alternatively to	the	e above scri	nt_if the s	cript is r	not in the specific path:	
	s for i in	¢			ont -F		
	SELECT DIS	TIT	NCT CS.ho	stname			
	FROM app	woi	rks.Serve	r CS, aj	ppwork	s.Server PS,	
	appworks.S	erv	ver2SG C2 verGroup	SG, app [.] CSG ap [.]	works. nworks	Server2SG P2SG,	
	comcol.Clu	ste	erInfo CC	I, comc	ol.Clu	sterInfo PCI,	
	comcol.Clu	ste	erGroupIn	fo			
	WHERE CS	ł	n_Server_	ID = C2	SGh_	_Server_ID	
	AND C2SGh_SG_ID = CSGh_SG_ID						
	AND CS	G.(clusteria	= CCL.	Cluste	erid	
	AND CCI.groups = comcol.ClusterGroupInfo.groupId						
	PCI.groups						
	AND PC	I.d	clusterId	= PSG.	cluste	erId	
	AND PS	G.S	ServerGro	upName=	' <mark><soam< mark=""></soam<></mark>	1_SG_NAME>'	
"); do iset -finhibitRepPlans='' NodeInfo where					NodeInfo where		
	"nodename=	· ၃ -	L'", done				
	Note: SOAM into the Group:	_S(e ac s .	G_NAME is ctive NOAM	the name GUI and i	of the s navigati	server group found by logging ng to Configuration > Server	
	For example, if group is SO_S	SC G.	DAM1 belon	gs to the s	site beir	ng recovered, then the server	
	DRNO_3G	A	NONE	DSR (active/standby pair)	1	Network Element DSR_DR_NO_NE Server Node HA Pref VIPs DRNOAM1 DRNOAM2	
	NO_SG	A	NONE	DSR (active/standby pair)	1	Network Element DSR_NO_NE Server Node HA Pref VIPs NOAM1 NOAM2	
	80_8G	в	NO_SC	DSR (active/standby pair)	1	Network Element DSR_SO_NE Server Node HA Pref VIPe SO/M1 SOAM2 VIPE VIPE	
	Un-Inhibit replication on all C-level servers	Un-Inhibit replication on all C-level servers	Un-Inhibit replication on all C-level servers	Un-Inhibit replication on all C-level servers if available. If the /usr/TKLC/dsr/tools/ painhibitReplicationToCLevel. /usr/TKLC/dsr/tools/In replication=allowSO Alternatively to the above scription \$ for i in \$(sudo Imy SELECT DISTINCT CS.ho FROM appworks.Server2SG C2 appworks.Server3 AND C2SG.h_SG_ID AND CCI.groups AND PCI.clusterId AND PSG.Server3 Note: SOAM_SG_NAME is into the active NOAM Groups A No.96 A NOS A <th>Un-Inhibit replication on all C-level servers if the /usr/TKLC/dsr/tools/ path does n InhibitReplicationToCLevel.sh script, /usr/TKLC/dsr/tools/InhibitRe replication=allowSO_SG_Nam Alternatively to the above script, if the s \$ for i in \$(sudo Imysql.cli SELECT DISTINCT CS.hostname FROM appworks.Server 2SG C2SG, app appworks.Server2SG C2SG, app appworks.ServerGroup CSG, ap comcol.ClusterInfo CCI, comc comcol.ClusterInfo CCI, comc comcol.ClusterInfo CCI, comc comcol.ClusterInfo CCI, comc comcol.ClusterId = CCI. AND C2SGh_SG_ID = CSG. AND CSG.clusterId = CCI. AND CCI.groups = comcol. AND comcol.ClusterGroupInfo VHERE CS_hServerGroupName= "); do iset -finhibitRepPlan "nodeName='\$i'"; done Note: SOAM_SG_NAME is the name into the active NOAM GUI and is Groups. For example, if SOAM1 belongs to the s group is SO_SG. Officiententangy provid</th> <th>Un-Inhibit replication on all C-level servers if available. If the /usr/TKLC/dsr/tools/ path does not have inhibitReplicationToCLevel.sh script, then us /usr/TKLC/dsr/tools/InhibitReplicat replication=allowSO_SG_Name=<soz Alternatively to the above script, if the script is in \$ for i in \$(sudo Imysql.client -F SELECT DISTINCT CS.hostname FROM appworks.Server2SG C2SG, appworks appworks.Server2SG C2SG, appworks appworks.Server2Group CSG, appworks comcol.ClusterInfo CCI, comcol.Clu comcol.ClusterGroupInfo WHERE CSh_Server_ID = C2SGh_ AND C2SGh_SG_ID = CSGh_SG_ AND CSG.clusterId = CCI.cluster AND CCI.groups = comcol.Cluster AND CCI.groups = comcol.Cluster AND PSG.ServerGroupInfo.pa PCI.groups AND PSG.ServerGroupName='<soan "); do iset -finhibitRepPlans='' N "nodeName='\$i'"; done Note: SOAM_SG_NAME is the name of the s into the active NOAM GUI and navigati Groups. For example, if SOAM1 belongs to the site bein group is SO_SG. DMMOLSS NOE DMMOLSS NOE</soan </soz </th>	Un-Inhibit replication on all C-level servers if the /usr/TKLC/dsr/tools/ path does n InhibitReplicationToCLevel.sh script, /usr/TKLC/dsr/tools/InhibitRe replication=allowSO_SG_Nam Alternatively to the above script, if the s \$ for i in \$(sudo Imysql.cli SELECT DISTINCT CS.hostname FROM appworks.Server 2SG C2SG, app appworks.Server2SG C2SG, app appworks.ServerGroup CSG, ap comcol.ClusterInfo CCI, comc comcol.ClusterInfo CCI, comc comcol.ClusterInfo CCI, comc comcol.ClusterInfo CCI, comc comcol.ClusterId = CCI. AND C2SGh_SG_ID = CSG. AND CSG.clusterId = CCI. AND CCI.groups = comcol. AND comcol.ClusterGroupInfo VHERE CS_hServerGroupName= "); do iset -finhibitRepPlan "nodeName='\$i'"; done Note: SOAM_SG_NAME is the name into the active NOAM GUI and is Groups. For example, if SOAM1 belongs to the s group is SO_SG. Officiententangy provid	Un-Inhibit replication on all C-level servers if available. If the /usr/TKLC/dsr/tools/ path does not have inhibitReplicationToCLevel.sh script, then us /usr/TKLC/dsr/tools/InhibitReplicat replication=allowSO_SG_Name= <soz Alternatively to the above script, if the script is in \$ for i in \$(sudo Imysql.client -F SELECT DISTINCT CS.hostname FROM appworks.Server2SG C2SG, appworks appworks.Server2SG C2SG, appworks appworks.Server2Group CSG, appworks comcol.ClusterInfo CCI, comcol.Clu comcol.ClusterGroupInfo WHERE CSh_Server_ID = C2SGh_ AND C2SGh_SG_ID = CSGh_SG_ AND CSG.clusterId = CCI.cluster AND CCI.groups = comcol.Cluster AND CCI.groups = comcol.Cluster AND PSG.ServerGroupInfo.pa PCI.groups AND PSG.ServerGroupName='<soan "); do iset -finhibitRepPlans='' N "nodeName='\$i'"; done Note: SOAM_SG_NAME is the name of the s into the active NOAM GUI and navigati Groups. For example, if SOAM1 belongs to the site bein group is SO_SG. DMMOLSS NOE DMMOLSS NOE</soan </soz 	

3.	Active NOAM: Verify replication has been Un- Inhibited	After execut GUI would b Verification output. Un-li group, for ex Execute this	ing above solve raised in of replication nhibitRepP kample, set socommand	steps to un forming th on inhibitic lans field rver group :	n-inhibit replicatio nat replication on f on on MPs can be for all the MP serv SO_SG is set as	n on MP(s), no ala MP is disabled. done by analyzing /ers for the selecte < blank> .	rms on NodeInfo d server
		\$ sudo i	qt NodeI	nfo			
		Output:					
		nodeId excludeTab	nodeName les	hostName	e nodeCapability	inhibitRepPlans	siteId
		A1386.099	NO1	NO1	Active		NO_HPC03
		B1754.109	S01	S01	Active		SO_HPC03
		C2254.131	MP2	MP2	Active		SO_HPC03
		C2254.233	MP1	MP1	Active		SO_HPC03

Procedure 21. Un-Inhibit A and B Level Replication on C-Level Servers

Appendix G. Restore TVOE Configuration from Backup Media

Procedure 22. Restore TVOE Configuration from Backup Media

This Che num If thi	procedure provides ck off ($$) each step ber. is procedure fails, it	s steps to restore the TVOE application configuration from backup media. as it is completed. Boxes have been provided for this purpose under each step is recommended to contact My Oracle Support (MOS) and ask for assistance.
1.	Install TVOE application	 If the PMAC is NOT hosted on the failed rack mount server, execute IPM Servers Using PMAC Application from reference [10]. If the PMAC is hosted on the failed rack mount server, execute Installing TVOE on the Management Server from reference [10].
2.	Establish network connectivity	 If the PMAC is NOT hosted on the failed rack mount server, skip this step. If the PMAC is hosted on the failed rack mount server, execute TVOE Network Configuration, steps 1-11, from reference [10]. 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 image to the TVOE host (NetBackup)	 If using NetBackup to restore the TVOE backup ISO image, then execute this step; otherwise, skip this step. 1. Execute Application NetBackup Client Installation Procedures from reference [8]. 2. Interface with the NetBackup master server and initiate a restore of the TVOE backup ISO image. Note: Once restored, the ISO image is in /var/TKLC/bkp/ on the TVOE server.

	Procedure 22.	Restore '	TVOE	Configuration	from	Backup	Media
--	---------------	-----------	------	---------------	------	--------	-------

4.	Transfer TVOE	Restore TVOE backup ISO using SCP.					
	backup ISO image to the	Using the IP of the TVOE host, transfer the backup ISO image to the TVOE. Linux:					
	I VOE HOST	From th backup	ne command line of a Linux machine use this command to copy the ISO image to the TVOE host:				
		# scr	<pre>p <path_to_image> tvoexfer@<tvoe_ip>:backup/</tvoe_ip></path_to_image></pre>				
		where - system	<pre><path_to_image> is the path to the backup ISO image on the local and <tvoe_ip> is the TVOE IP address.</tvoe_ip></path_to_image></pre>				
		Note:	If the IP is an IPv4 address, then <tvoe_ip> is a normal dot-decimal notation (for example, 10.240.6.170).</tvoe_ip>				
		Note:	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>				
		Note:	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:					
		# scr	p /path/to/image.iso tvoexfer@10.240.6.170:backup/				
		IPv6 Ex	xample:				
		<pre># scp /path/to/image.iso</pre>					
		tvoexfer@[fe80::21e:bff:fe76:5e1c%control]:backup					
		Windows:					
		Use WinSCP to copy the Backup ISO image into the /var/TKLC/bkp direct Please refer to [10] procedure Using WinSCP to copy the backup image the customer system.					
5.	TVOE Server : Login	Establis	sh an SSH session to the TVOE server, login as admusr .				



Procedure 22. Restore TVOE Configuration from Backup Media



Procedure 22. Restore TVOE Configuration from Backup Media



Procedure 22. Restore TVOE Configuration from Backup Media



Procedure 22. Restore TVOE Configuration from Backup Media

Procedure 22. Restore TVOE Configuration from Backup Media

10.	TVOE Server: Wait for restart to successfully complete	1401715649: Upstart Job TKLChpacucli: 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 hostname71e968a495e6 login:
11. □	TVOE Server: Verify storage pools are active	 Login as admusr. Verify all storage pools are listed and are in the active state:
		\$ sudo virsh -c "qemu:///system" pool-list
		[admusr@5010441-TVOE ~]\$ sudo virsh -c "qemu:///system" pool-list
		[admusr@5010441-TVOE ~]\$
		Note: If any storage pools are missing or inactive, contact My Oracle Support (MOS).
12. □	TVOE Server: Enable HIDS	Note: Enabling HIDS is optional. This step is skipped if HIDS is not required to be enabled.
	(Optional)	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:
		\$ /usr/TKLC/plat/bin/hidsMgr -initialize
		LOG: HIDS monitoring has been Initialized
		HIDS baseline has been initialized
		\$ /usr/TKLC/plat/bin/hidsMgrenable
		New State: ENABLED
		<pre>\$ /usr/TKLC/plat/bin/hidsMgrupdateall</pre>
		HIDS baseline has successfully been updated



Procedure 22. Restore TVOE Configuration from Backup Media

Appendix H. Restore PMAC from Backup

Procedure 23. Restore PMAC from Backup Media

This procedure provides steps to restore the PMAC application configuration from backup media. **Prerequisite**: TVOE management server has been restored.

Check off ($\sqrt{}$) 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. □	Deploy the PMAC guest	Execute Install PMAC from reference [10].					
2.	PMAC: Login	Establish an SSH session to the PMAC server, 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	Verify no alarms are present.					
	present	<pre>\$ sudo /usr/TKLC/plat/bin/alarmMgralarmStatus</pre>					
5.	Restore the	Restore the PMAC data from backup.					
	from Backup	<pre>\$ sudo /usr/TKLC/smac/bin/pmacadm restore PM&C Restore been successfully initiated as task ID 1</pre>					
		Check the status of the background task.					
		<pre>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</pre>					
		Note: The result eventually displays PMAC Restore successful.					

110	cedure 25. Restor						
6.	PMAC GUI : Login	1. Open web browser and navigate to the PMAC GUI.					
		2. Login as PMACadmin user:					
		https:// <pmac_network_ip></pmac_network_ip>					
		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.					
7.	PMAC GUI:	1. Navigate to Task Monitoring.					
	task completed	2. Verify the restore background task completed successfully.					
		Note: After the restore is complete, you should see Add Enclosure tasks start for all proviously provisioning servers. These should be allowed					
		to complete before continuing.					
		Note: After the restore is complete, you may see some tasks mentioning					
		added in the next step.					
8.	PMAC GUI:	1. Navigate to Hardware > System Inventory.					
	verity system	🖃 💻 Main Menu					
	2	😑 😋 Hardware					
		🖃 😋 System Inventory					
		Cabinet 1					
		Cabinet 2					
		Cabinet Undesignated					
		FRU Info					
		 Verify previously provisioned enclosures are present. 					

Procedure 23. Restore PMAC from Backup Media

		•
9.	PMAC: Verify	Perform a system health check on the PMAC
	РМАС	<pre>\$ sudo /usr/TKLC/plat/bin/alarmMgralarmStatus</pre>
		This command should return no output on a healthy system.
	<pre>\$ sudo /usr/TKLC/smac/bin/sentry status</pre>	
		All processes should be running, displaying output similar to the following:
		PM&C Sentry Status
		sentryd started: Mon Jul 23 17:50:49 2012
		Current activity mode: ACTIVE
		Process PID Status StartTS NumR
		smacTalk 9039 running Tue Jul 24 12:50:29 2012 2
		smacMon 9094 running Tue Jul 24 12:50:29 2012 2
		hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2
		snmpEventHandler 9176 running Tue Jul 24 12:50:29 2012 2
		Fri Aug 3 13:16:35 2012
		Command Complete.
10. □	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].
1		1

Procedure 23. Restore PMAC from Backup Media

Procedure 24. Restore PMAC from Backup Server

This procedure provides steps to restore the PMAC application configuration from backup server.

Prerequisite: TVOE management server has been restored.

Check off ($\sqrt{}$) 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.	Deploy the PMAC guest	Execute Install PMAC from reference [10].		
		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 Host: Log into PMAC guest console	1. On the TVOE host, execute this command: \$sudo virsh list This produces a listing of currently running virtual machines. [admusr@Oahu-TVOE-1 ~]\$ sudo virsh list Id Name State
		1 Oahu-PMAC running
		2. Find the VM name for your PMAC and note its ID number in the first column.
4.	Connect to console of the VM using the VM number obtained in Step 3	On the TVOE host, execute this command:
		\$sudo virsh console <pmac-vmid></pmac-vmid>
		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 +].

Procedure 24. Restore PMAC from Backup Server

Procedure 24.	Restore	PMAC from	Backup	Server
---------------	---------	-----------	--------	--------

5. PMAC : P	repare	Execute these commands on the PMAC.
PMAC gue	est to	<pre>\$ sudo /sbin/service iptables stop</pre>
appropriat	te	iptables: Flushing firewall rules: [
backup fro	om	OK]
backup se	erver.	iptables: Setting chains to policy ACCEPT: filter [
Disable ipi	Disable iptables,	OK]
TPD platc	fa	<pre>\$ sudo /usr/TKLC/smac/etc/services/netbackup start</pre>
backup	3	Modified menu NBConfig
configurati	ion	
menus		show
		Set the following menus: NBConfig to visible=1
		Modified menu NBInit
		show
		Set the following menus: NBInit to visible=1
		Modified menu NBDeInit
		show
		Set the
		following menus: NBDeInit to visible=1
		Modified menu NBInstall
		show
		Set the following menus: NBInstall to visible=1
		Modified menu NBVerifyEnv
		show
		Set the following menus: NBVerifyEnv to visible=1
		Modified menu NBVerify
		show
		Set the following menus: NBVerify to visible=1=

6.	PMAC : Verify the TPD platcfg backup menus are visible, then exit the TPD platcfg Utlility	Verify the TPD platcfg backup menus are visible.
		\$ sudo /bin/su - platcfg
		Main Menu Maintenance Diagnostics Server Configuration Network Configuration Remote Consoles NetBackup Configuration Exit Note: 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 guest	<pre>\$ sudo /sbin/iptables -nL INPUT (policy ACCEPT) target prot opt source destination Chain FORWARD (policy ACCEPT) target prot opt source destination Chain OUTPUT (policy ACCEPT) target prot opt source destination</pre>
8.	PMAC: Install backup utility client software on the PMAC guest	 Execute PMAC NetBackup Client Installation and Configuration from reference [10] - Start at step 1. Note: The Initialize PMAC Application and Configure PMAC Application prerequisites can be ignored.
9.	Backup server: verify appropriate PMAC backup exists	 This step is likely executed by customer IT personnel. 1. Log into the backup server as the appropriate user using the user password. 2. Execute the appropriate commands to verify the PMAC backup exists for the desired date. <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. <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 24. Restore PMAC from Backup Server

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

Procedure 24. Restore PMAC from Backup Server

Pro	Procedure 24. Restore PMAC from Backup Server				
13. □	PMAC GUI:	1. Open web browser and navigate to the PMAC GUI.			
	Login	https:// <pmac_network_ip></pmac_network_ip>			
		2. Login as PMACadmin 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			
		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: Verify restore	1. Navigate to Task Monitoring.			
	task completed	2. Verify 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.			
15.	PMAC GUI:	1. Navigate to Hardware > System Inventory.			
	verify system inventory	🖃 💻 Main Menu			
		E 🔄 Hardware			
		Cabinet 1			
		Cabinet 2			
		Cabinet 101			
		🖃 🧰 Cabinet Undesignated			
		FRU Info			
		2. Verify previously provisioned enclosures are present			

andura 24 Postora PMAC from Backup S П

16.	PMAC: Verify	Perform a system health check on the PMAC
	PMAC	\$ sudo /usr/TKLC/plat/bin/alarmMgralarmStatus
		This command should return no output on a healthy system.
		<pre>\$ sudo /usr/TKLC/smac/bin/sentry status All processes should be running, displaying output similar to the following: PM&C Sentry Status </pre>
		Command Complete.
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 24. Restore PMAC from Backup Server

Appendix I. Configure TVOE Hosts

Procedure 25. Configure TVOE

This Prei Che step If thi	 This procedure configures networking on TVOE hosts. Prerequisite: Server has been IPM'ed with TVOE OS as described in [10]. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance. 					
1.	Determine bridge names and interfaces	1. Determine t the TVOE s	the bridge names server for the NO	and physical bridge interfaces to be used on AM XMI and IMI networks.		
	for XMI and IMI, and NetBackup (if	what bonds those bonds	are used, and a s.	so the actual Ethernet interfaces that make up		
	used) networks	3. If the NetBa server when	ackup bridge and n PMAC was inst	interface were not previously configured on this alled, determine those values as well.		
		4. Fill in the ap	opropriate values	in the table below:		
		NOAM Guest Interface Name	TVOE Bridge Name	TVOE Bridge Interface		
		xmi	xmi	Interface Bond (for example, bond0, bond1, etc.):		
		imi	imi	Interface Bond:(for example, bond0, bond1, etc.):		
		NetBackup	NetBackup	Interface Name (for example, eth11, eth04, eth03, etc.): <tvoe_netbackup_bridge_interface></tvoe_netbackup_bridge_interface>		
		management	management	Interface Name (for example, bond0.2, bond0.37, etc.): <tvoe_mgmt_bridge_interface></tvoe_mgmt_bridge_interface>		
2 .	RMS Server : Login	Log in to the T∖	OE prompt of the	e RMS server as admusr using the iLO facility.		

Procedure 25. Configure TVOE

3. RMS Server :	1. Verify the XMI bridge interface bond.
Configure XMI bridge interface bond	<pre>\$ sudo /usr/TKLC/plat/bin/netAdm query device=<tvoe_xmi_bridge_interface_bond> Protocol: none On Boot: yes Persistent: yes Bonded Mode: active-backup Enslaving: eth01 eth02</tvoe_xmi_bridge_interface_bond></pre>
	<i>Note</i> : The output below is for illustrative purposes only. The example output shows the control bridge configured.
	If the bond has already been configured, output, similar to what you see above, displays. If this is so, skip to the next step; otherwise, continue with this step.
	2. Create bonding interface and associate subordinate interfaces with bond:
	<pre>\$ sudo /usr/TKLC/plat/bin/netAdm add</pre>
	device= <tvoe_xmi_bridge_interface_bond></tvoe_xmi_bridge_interface_bond>
	onboot=yestype=Bondingmode=active-backup
	miimon=100
	Interlace <tvoe_xmi_bridge_bond> added</tvoe_xmi_bridge_bond>
	<pre>\$ sudo /usr/TKLC/plat/bin/netAdm set device=<tvoe_xmi_bridge_bond_ethernet1></tvoe_xmi_bridge_bond_ethernet1></pre>
	type=Ethernet
	slave=yesonboot=yes
	Interface <tvoe_xmi_bridge_bond_ethernet1> updated</tvoe_xmi_bridge_bond_ethernet1>
	\$ sudo /usr/TKLC/plat/bin/netAdm set
	device= <tvoe_xmi_bridge_bond_ethernet2></tvoe_xmi_bridge_bond_ethernet2>
	type=Ethernet
	master= <tvoe_xmi_bridge_interface_bond></tvoe_xmi_bridge_interface_bond>
	slave=yesonboot=yes
	finterface <100E_AMI_Bridge_Bond_Ethernetz> updated
	setvar=DEVICES
	<pre>val=<tvoe_xmi_bridge_interface_bond>,[bondX,bondX+1,,bondN]</tvoe_xmi_bridge_interface_bond></pre>
	Note : All other existing bonds should be included in the val= statement, for example, if TVOE_XMI_Bridge_Bond = bond1, val=bond0,bond1.
	\$ sudo syscheckAdm net ipbond -enable

Procedure 25. Configure TVOE

4.	RMS Server: Create XMI bridge interface, if needed. (Only for VLAN tagging interfaces)	If you are using VLAN tagging for the XMI bridge interface, then you must create the VLAN interface first.
		<pre>\$ sudo /usr/TKLC/plat/bin/netAdm add device=<tvoe_xmi_bridge_interface>onboot=yes Interface <tvoe_xmi_bridge_interface> created.</tvoe_xmi_bridge_interface></tvoe_xmi_bridge_interface></pre>
5.	RMS Server: Create XMI bridge	Now, create the XMI bridge:
		<pre>\$ sudo /usr/TKLC/plat/bin/netAdm addtype=Bridge name=xmionboot=yesbridgeInterfaces=<tvoe_xmi_bridge_interface> Interface <toe_xmi_bridge_interface> updated.</toe_xmi_bridge_interface></tvoe_xmi_bridge_interface></pre>
		Bridge xmi created.

Procedure 25. Configure TVOE

6. RMS S	erver: 1. Verify the IMI bridge interface bond.
Configu bridge interfac	rre IMI e bond protocol: none On Boot: yes Persistent: yes Bonded Mode: active-backup Enslaving: eth01 eth02
	Note : The output below is for illustrative purposes only. The example output shows the control bridge configured.
	If the bond has already been configured, output, similar to what you see above, displays. If this is so, skip to the next step; otherwise, continue with this step.
	2. Create bonding interface and associate subordinate interfaces with bond.
	\$ sudo /usr/TKLC/plat/bin/netAdm add
	device= <tvoe_imi_bridge_interface_bond></tvoe_imi_bridge_interface_bond>
	onboot=yestype=bondingmode=active-backup
	Interface <tv added<="" bonds="" bridge="" imi="" of="" td=""></tv>
	Ś sudo /usr/TKLC/plat/bin/netAdm_set
	device= <tvoe bond="" bridge="" ethernet1="" imi=""></tvoe>
	type=Ethernet
	master= <tvoe_imi_bridge_bond>slave=yes</tvoe_imi_bridge_bond>
	Interface <tvoe_imi_bridge_bond_ethernet1> updated</tvoe_imi_bridge_bond_ethernet1>
	\$ sudo /usr/TKLC/plat/bin/netAdm set
	device= <tvoe_imi_bridge_bond_ethernet2> type=Ethernet</tvoe_imi_bridge_bond_ethernet2>
	master= <tvoe_imi_bridge_bond>slave=yes onboot=yes</tvoe_imi_bridge_bond>
	<pre>Interface <tvoe_imi_bridge_bond_ethernet2> updated</tvoe_imi_bridge_bond_ethernet2></pre>
	 Execute these 2 commands ONLY IF <tvoe_xmi_bridge_bond> is different from <tvoe_imi_bridge_bond>.</tvoe_imi_bridge_bond></tvoe_xmi_bridge_bond>
	\$ sudo syscheckAdm net ipbondsetvar=DEVICES
	val= <tvoe_xmi_bridge_interface_bond>,</tvoe_xmi_bridge_interface_bond>
	<tvoe_imi_bridge_interface_bond>,[other bonds]</tvoe_imi_bridge_interface_bond>
	\$ sudo syscheckAdm net ipbond -enable

Procedure 25.	Configure TVOE
---------------	----------------

7.	RMS Server: Create IMI bridge interface	If you are using VLAN tagging for the IMI bridge interface, then you must create the VLAN interface first.
		<pre>\$ sudo /usr/TKLC/plat/bin/netAdm add device=<tvoe_imi_bridge_interface>onboot=yes Interface <tvoe_imi_bridge_interface> created.</tvoe_imi_bridge_interface></tvoe_imi_bridge_interface></pre>
8. RMS Server:		Create the IMI bridge:
	Create IMI bridge	<pre>\$ sudo /usr/TKLC/plat/bin/netAdm addtype=Bridge name=imionboot=yes</pre>
		bridgeInterfaces= <tvoe_imi_bridge_interface></tvoe_imi_bridge_interface>
		<pre>Interface <tvoe_imi_bridge_interface> updated.</tvoe_imi_bridge_interface></pre>
		Bridge imi created.

Trocedure 25. Configure 140L	Procedure	25.	Configure	TVOE
------------------------------	-----------	-----	-----------	------

		-
9.	RMS Server iLO: Create	1. Execute this step only if the TVOE host is a rack mount server and is NOT the PMAC server.
	management bridge and assign TVOE management IP	<i>Note</i> : The output below is for illustrative purposes only. The site information for this system determines the network interfaces (network devices, bonds, and bond enslaved devices) to configure.
		2. If <tvoe_management_bridge_interface>, or the bond it is based on (if using tagged interface), has not yet been created, then execute the next 3 commands; otherwise, skip to the EXAMPLE section:</tvoe_management_bridge_interface>
		\$ sudo /usr/TKLC/plat/bin/netAdm add
		device= <tvoe_mgmt_bridge_interface_bond></tvoe_mgmt_bridge_interface_bond>
		onboot=yestype=Bondingmode=active-backup
		miimon=100
		Interface <tvoe_management_bridge_interface> added</tvoe_management_bridge_interface>
		<pre>\$ sudo /usr/TKLC/plat/bin/netAdm set</pre>
		device= <tvoe_mgmt_bridge_bond_interface1></tvoe_mgmt_bridge_bond_interface1>
		type=Ethernet master= <tvof bond="" bridge="" interface="" momt="">slave=ves</tvof>
		onboot=yes
		Interface <mgmt_ethernet_interface1> updated.</mgmt_ethernet_interface1>
		\$ sudo /usr/TKLC/plat/bin/netAdm set
		device= <tvoe_mgmt_bridge_bond_interface2></tvoe_mgmt_bridge_bond_interface2>
		type=Ethernetmaster- <tvoe_mgmt_bridge_interface_bond>slave=yes onboot=yes</tvoe_mgmt_bridge_interface_bond>
		Interface <mgmt_ethernet_interface2> updated</mgmt_ethernet_interface2>
		EXAMPLE 1: Create Management bridge using untagged interfaces
		\$ sudo /usr/TKLC/plat/bin/netAdm addtype=Bridge
		name=managementbootproto=noneonboot=yes
		address= <tvoe_mgmt_ip_address></tvoe_mgmt_ip_address>
		netmask= <tvoe_mgmt_netmask prefix=""></tvoe_mgmt_netmask>
		bridgeInterfaces= <tvoe_mgmt_bridge_interface></tvoe_mgmt_bridge_interface>
		EXAMPLE 2: Create Management bridge using tagged interfaces
		<pre>\$ sudo /usr/TKLC/plat/bin/netAdm add</pre>
		device= <tvoe_management_bridge_interface></tvoe_management_bridge_interface>
		<pre>\$ sudo /usr/TKLC/plat/bin/netAdm addtype=Bridge</pre>
		name=managementaddress= <tvoe_mgmt_ip_address></tvoe_mgmt_ip_address>
		netmask= <tvoe_mgmt_netmask prefix="">onboot=yes</tvoe_mgmt_netmask>
		bridgeInterfaces= <tvoe_mgmt_bridge_interface></tvoe_mgmt_bridge_interface>

10.	RMS Server	Add a default route using the xmi or management address (if configured).							
	default route	<pre>\$ sudo /usr/TKLC/plat/bin/netAdm addroute=default</pre>							
		gateway= <tvoe_mgmt_gateway_ip_address></tvoe_mgmt_gateway_ip_address>							
		device= <management or="" xmi=""></management>							
		Route to management created.							
11. RMS Server: Verify the XMI and IMI bridges have been created successfully (Ex for illustrative purposes only).									
	creation status	\$ brctl show							
		<pre>[root@SunNetralTvoe admusr]# brctl show bridge name bridge id STP enabled interfaces control 8000.002128a1a5a8 no bond0 vnet0 vnet12 wnet15</pre>							
		imi 8000.002128a1a5a8 no bond0.641 vnet10 vnet10 vnet14 vnet17							
		vnet5 management 8000.002128a1a5a8 no bond0.637							
		vnet1 xmi 8000.002128a1a5a8 no bond0.638 vnet13							
		Verify imi and xmi are listed under the bridge name column.							
	 Verify <tvoe_xmi_bridge_interface> is listed under the interfaces column for xmi.</tvoe_xmi_bridge_interface> 								
		Verify <tvoe_imi_bridge_interface> is listed under the interfaces column for imi.</tvoe_imi_bridge_interface>							
		 Verify the <tvoe_mgmt_bridge_interface> is listed under the interface column for <tvoe_mgmt_bridge_interface></tvoe_mgmt_bridge_interface></tvoe_mgmt_bridge_interface> 							
12. 	Perform this command if you have a dedicated NetBackup interface within your NOAM guests (and if the NetBackup bridge was NOT configured when setting up the PMAC earlier).								
	bridge (Optional)	<pre>\$ sudo /usr/TKLC/plat/bin/netAdm addtype=Bridge</pre>							
	(Optional)	name=NetBackuponboot=yes							
		MTU= <netbackup_mtu_size></netbackup_mtu_size>							
		bridgeInterfaces= <tvoe_netbackup_bridge_interface></tvoe_netbackup_bridge_interface>							

Procedure 25. Configure TVOE



Procedure 25. Configure TVOE

Procedure 25. Configure TVOE



Procedure 25. Configure TVOE





Procedure 25. Configure TVOE

Appendix J. Create NOAM/SOAM Virtual Machines

Procedure 26. Create NOAM Guest VMs

This procedure creates a DSR NOAM virtual machine (referred to as a guest) on a TVOE server blade or TVOE RMS. It is repeated for every NOAM server you want to install.						
Prei	Prerequisite: TVOE has been installed and configured on the target blade server or RMS					
Che num	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.					
lf thi	s procedure fails,	, it is recommended to contact My Oracle Support (MOS) and ask for assistance.				
1.	PMAC GUI:	1. Open web browser and enter:				
	Login	http:// <pmac_mgmt_network_ip></pmac_mgmt_network_ip>				
		2. Login as pmacadmin user:				
		ORACLE [®]				
		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:	1. Navigate to Main Menu > VM Management.
	Navigate to VM management of the target server blade	 Software Software Inventory Manage Software Images VM Management Select the TVOE server blade or rack mounted server from the VM Entities listing on the left side of the screen. The selected server's guest machine configuration displays in the remaining area of the window.
		View host on RMS pc5010439
		VM Info Software Network Media
		Summary Bridges Storage Pools Memory
		Host Name: 5010439-TVOE Location: RMS pc5010439
		Guests
		Name Status
		Zombie_DSRDR NOAM2 Running
		Zombie_DSRNO AM2 Running
		3. Click Create Guest.

3.	PMAC GUI:	1. Click Impo	rt Prof	ile.						
	Configure VM guest	Import Profile								
	parameters	ISO/Profile:	DSR-8	.0.0.0.0_	_80.11.0->	×86_64 =	> DSR_NO	AMP_LARGE		
		Num CPUs: Memory (MBs):	12 24576							
		Virtual Disks:	sks: Prim Size (M		B)	Pool	TPD Dev			
			1	10240)0 vg	guests				
		NICs:	Bri	dge 1	TPD Dev					
			cor	itrol	control					
				imi	imi					
				xmi	xmi					
		Select Profile	Cance	el						
		depending and your pr	on the referen	hardw ice for	are that NetBac	t your N kup inte	IOAM VI erfaces:	M TVOE se	erver is runnir	ng on
		NOAM VM TVOE Hardware Type(s)			Netba Inter	ackup face?	Navig (<app< th=""><th>ate to Proposition IS</th><th>file 60 NAME>)</th><th></th></app<>	ate to Proposition IS	file 60 NAME>)	
		HP DL380 Ge HP BL460 Ge HP BL460 Ge HP BL460 Ge	n 8 RN n 9 RN n 8 Bla n 9 Bla	AS, AS, ade, ade	Ν	lo	DS	R_NOAMF	P_LARGE	
		HP DL380 Ge HP BL460 Ge HP BL460 Ge HP BL460 Ge	n 8 RN n 9 RN n 8 Bla n 9 Bla	AS, AS, ade, ade	Y	es	DSR_	NOAMP_L	ARGE_NBD	
		Note: Applica	tion_Is	SO_NA	AME is t AM	he nam	ne of the	DSR Appli	ication ISO to	be
		3. Click Selec	t Prof	ile.						
		4. Click Creat	е							
		Create Im	nport P	rofile	Cano	el				

Procedure 26. Create NOAM Guest VMs

Procedure 26. Create NOAM Guest VMs

4. □	PMAC GUI: Wait for guest creation to	 Navigate to Main Menu > Task Monitoring to monitor the progress of the guest creation task. A separate task displays for each guest creation you start. 						
	complete	2. Wait or refresh the screen until you see the guest creation task has completed successfully.						
		Create Guest RMS: <u>pc5010439</u> Guest: <u>Zombie DSRNOAM2</u> Guest creation completed (Zombie_DSRNOAM2)						
5.	PMAC GUI:	1. Navigate to Main Menu > VM Management.						
	Verify guest	2. Select the TVOE server blade on which the guest machine was just created.						
	running	3. Look at the list of guests present on the blade and verify you see a guest that matches the name you configured and that its status is Running .						
		View guest Zombie_DSRNOAM2						
		VM Info Software Network Media						
		Summary Virtual Disks Virtual NICs						
		Current Power State: Running						
		Set Power State On Change						
		Guest Name (Required): Zombie_DSRNOAM2						
		Host: RMS: pc5010439						
		Number of vCPUs: 4						
		Memory (MBs): 6,144						
		VM UUID: e9e22407-c289-4d2a-						
		Enable Virtual Watchdog 🖌						
		 VM creation for this guest is complete. Repeat from step 2 for any remaining NOAM VMs (for instance, the standby NOAM) that must be created. 						
Procedure 27. Create SOAM Guest VMs

This procedure creates a DSR SOAM virtual machine (referred to as a **guest**) on a TVOE server blade. It is repeated for every SOAM server you want to install.

Prerequisite: TVOE has been installed and configured on the target blade server.

Check off ($\sqrt{}$) 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.	PMAC GUI:	1. Open web browser and enter:
	Login	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 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.

2.	PMAC GUI: Navigate to VM management of the target server blade	 Navigate to Main Menu > VM Management. Software Software Inventory Manage Software Images VM Management Select the TVOE server blade or rack mounted server from the VM Entities listing on the left side of the screen. The selected server's guest machine configuration displays in the remaining area of the window.
		VM Info Software Network Media Summary Bridges Storage Pools Memory Host Name: 5010439-TVOE Location: RMS pc5010439 Guests Image: Storage Pools Storage Pools Storage Pools
		Name Status
		Zombie_DSRDR Running
		Zombie_DSRNO AM2 Running
		3. Click Create Guest.

Procedure 27. Create SOAM Guest VMs

110								
3.	PMAC GUI: Configure VM guest	1. Click Import	Profile.					
		Import Profile						
	parameters	ISO/Profile: DS	R-8.0.0.0.0_	80.11.0-x86_64 =	=> DSR_S	SOAM		
		Num CPUs: 4						
		Memory (MBs): 6144	1					
		Virtual Disks: Prin	m Size (MB) Pool	TPD D	ev		
		~	10240	0 vgguests				
		NICs:	Bridge T	PD Dev				
			control	control				
			imi	imi				
			xmi	xmi				
		Select Profile Ca	ncel					
		2. From the ISO depending on and your pref	/Profile of the hard erence for	drop-down bo ware that yo r NetBackup	ox, sele our SO/ o interfa	ect the AM VM aces.	e entry that matches / TVOE server is runnir	ng on
		SOAM VM TVO Hardware Type	E (s)	Dedicate Netback Interface	ed up e?	Naviga (<app< th=""><th>ate to Profile lication ISO NAME>)</th><th></th></app<>	ate to Profile lication ISO NAME>)	
		HP BL460 Gen 8 HP BL460 Gen 9	3 Blade, 9 Blade	No			DSR_SOAM	
		HP BL460 Gen 8 HP BL460 Gen 9	3 Blade, 9 Blade	Yes		D	SR_SOAM_NBD	
		Note: Application installed of installed of 3. Click Select If 4. Edit the name DSR_SOAM_ for the VM ho 5. Click Create. Create Import Pr	on_ISO_N on this SC Profile. e, if you w _B. This st manag	IAME is the DAM vant. For ins is not the ult jer.	tance: imate f	of the DSR_	DSR Application ISO to SOAM_A or me. It is just an interna	be I tag
4.	PMAC GUI: Wait for guest creation to complete	 Navigate to N guest creation start. Wait or refres completed out 	h the scro	u > Task Mo separate tas een until you	onitori sk disp i see th	ng to r plays fo nat the	monitor the progress of or each guest creation you guest creation task has	the ou
		Create Guest	RMS: po Guest: Zombie	<u>. 5010441</u> <u>DSRSOAM1</u>	G (2	iuest cr Zombie_	eation completed _DSRSOAM1)	

Procedure 27. Create SOAM Guest VMs



Procedure 27. Create SOAM Guest VMs

Appendix K. SNMP Configuration

Procedure 28. Configure SNMP

This Trap Che num	This workaround configures SNMP with SNMPv2c and SNMPv3 as the enabled versions for SNMP Traps configuration, as PMAC does not support SNMPv3. Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.			
lf th	is procedure fails,	t is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1.	(Workaround) NOAM VIP GUI: Login	 Note: This workaround step should be performed only in the following cases: If SNMP is not configured. If SNMP is already configured and SNMPv3 is selected as enabled version. Note: This is a workaround step to configure SNMP with 'SNMPv2c and SNMPv3' as the enabled versions for SNMP Traps configuration, since PMAC does not support SNMPv3. If not already done, establish a GUI session on the NOAM server the VIP IP address of the NOAM server. Open the web browser and enter a URL of: <a href="http://<Primary_NOAM_VIP_IP_Address>">http://<primary_noam_vip_ip_address></primary_noam_vip_ip_address> Log into the NOAM GUI as the guiadmin user: 		
		Correction State System Login The Unit of the System Login of the System Reader and password to log in Password:		

Procedure 28.	Configure	SNMP
---------------	-----------	------



3.	PMAC GUI:	1. Open web browser and enter:
	Login	http:// <pmac ip="" mgmt="" network=""></pmac>
		2. Login as guiadmin user:
		ORACLE
		Oracle System 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, Oracle and/or its affiliates. All rights reserved.

Procedure 28. Configure SNMP

Procedure 28.	Configure	SNMP
---------------	-----------	------

4.	PMAC GUI: Update the TVOE host SNMP community string	 Navigate to Administration > Credentials > SNMP Community String Update. Check the Use Site Specific Read/Write Community String checkbox.
		Select Read Only or Read/Write Community String: Read Only Read/Write
		Check this box if updating servers using the Site Specific SNMP Community String: Use Site Specific Read/Write Community String
		Community String: Note: The Community String value can be 1 to 31 uppercase, lowercase, or numeric characters.
		Update Servers 3. Click Update Servers. 4. Click OK. You are about to update the Read/Write SHAMP Credentals on all known supporting TVOE servers and the PMAC guest on the control network of this PMAC. Changing of SHAMP Community Shings is only supported across product release versions that support this functionality and attempting to do so with product versions not supporting it may cause the system to become imperable. Are you sure you want to continue?

Appendix L. Backup Directory

Procedure 29. Backup Directory

This	This procedure checks and creates the backup directory.					
Che	Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number					
If th	If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.					
1.	NOAM/SOAM VIP Console: Determine if backup directory	 Execute this command an active NOAM/SOAM server console (accessed using the VIP) and compare the output. 				
		<pre>\$ cd /var/TKLC/db/filemgmt/ \$ ls -ltr</pre>				
	exists	2. Look for the backup directory in the output.				
		 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				
		 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 backup	cd /var/TKLC/db/filemgmt/				
	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.				
3.	NOAM/SOAM	1. Verify directory has been created.				
	VIP Console: Change	<pre>\$ ls -ltr /var/TKLC/db/filemgmt/backup</pre>				
	permissions of backup directory	Note: A No such file or directory error message should not display. The directory should show as empty with the total as 0 for content.				
		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				

Procedure 29. Backup Directory

4.	NOAM/SOAM VIP Console: Copy the backup file to the backup directory	1. Copy the backup file to the backup directory.
		<pre>\$ cp BACKUPFILE /var/TKLC/db/filemgmt/backup</pre>
		2. Change permissions of files in the backup directory.
		\$ 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 7.6.0.0._88.50.0 and later, 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) since these switches use other ciphers. Executing these commands with the restricted ciphers would fail as shown here:

[admusr@p5-pmac ~]\$ sudo 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 Procedure 30 must be executed before and after netConfig backup and restore operations.

Procedure 30. Turn Off Cipher List Before backupConfiguation/restoreConfiguration/upgradeFirmware Command

This procedure prepares the PMAC to avoid the cipher mismatch issue with Cisco switches. This is performed before the netConfig backup or restore operations.

Check off ($\sqrt{}$) 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.	Turn off cipher list	 4. From the PMAC shell enter: <u>sudo vi /etc/ssh/sshd_config</u> 5. Add # in the beginning of the following three lines to comment them out, the result is:
		#Ciphers aes256-ctr,aes192-ctr,aes128-ctr
		#MaxAuthfries 4 #LoginGraceTime 1m
2 .	Restart sshd	sudo service sshd restart
3.	Run the netConfig backupConfig uation/restore Configuration/ upgradeFirmw are command	<pre>For a backup operation: [admusr@pmac ~]\$ sudo /usr/TKLC/plat/bin/netConfig backupConfigurationdevice=<switch_name> service=<ssh_service> filename=<switch_name>-backup For a restore operation: [admusr@pmac ~]\$ sudo /usr/TKLC/plat/bin/netConfig restoreConfigurationdevice=<switch_name> service=<ssh_service> filename=<switch_name>-backup For a upgrade operation: [admusr@pmac ~]\$ sudo /usr/TKLC/plat/bin/netConfig</switch_name></ssh_service></switch_name></switch_name></ssh_service></switch_name></pre>
		upgradeFirmwaredevice= <switch_name> service=<ssh_service> filename=<cisco ios=""></cisco></ssh_service></switch_name>

Procedure 31. Resume Cipher List After backupConfiguation/restoreConfiguration/upgradeFirmware Command

This procedure restores the PMAC restricted cipher list after perform the netConfig backup and restore operations.

Check off ($\sqrt{}$) 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	 From the PMAC shell enter: sudo vi /etc/ssh/sshd_config Add # in the beginning of the following three lines to comment them out, the result is: and a statement of the following three lines to comment them out, the result is:
		Ciphers aes256-ctr,aes192-ctr,aes128-ctr MaxAuthTries 4 LoginGraceTime 1m
2.	Restart sshd	sudo service sshd restart

Appendix N. DSR Database Restore

Procedure 32. DSR Database Restore

The intent of this procedure is to restore the provision and configuration information from an NOAM server after the disaster recovery is complete							
Check off ($$) each step as it is completed. Boxes have been provided for this purpose under each step number.							
lf thi	If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.						
1.	NOAM VIP : 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					
		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.					

2.	NOAM VIP: Restore configuration data for the system	 3. Navigate to Status and Manage > Database. Status & Manage Network Elements Server HA Database KPIs Processes 4. Select the active NOAM server and click Disable Provisioning. Plication Backup Compa 5. Click OK.
3.	NOAM VIP:	1. Navigate to Status and Manage > Files.
3.	Verify the restore file existence	 Status & Manage Network Elements Server HA Database KPIs Processes Tasks Files Select the NOAM with OAM Max HA Role.
		3. Select Restore.
		4. Select the backup file to be used in the restore and click [Ok].
		The Database Restore Confirm screen displays.
		5. If there are any inconsistencies between the current state of the system and the information found in the backup file, a message displays indicating Incompatible database selected . If this is the case, mark the Force checkbox, and click OK . If not, simply click OK to start the restore process.
		The system begins restoring the database. After the restore is completed, the user is logged out of the NOAM GUI. Allow up to ten minutes for the restore to complete before the GUI returns to the login prompt.
4.	NOAM VIP: Enable Provisioning	1. On the NOAM GUI navigate to Status and Manage >Database
		 Enable Provisioning by clicking on Enable Provisioning button at the bottom left hand side of the GUI form
		3. Click Ok on the pop-up window, Provisioning will now be enabled Log into the Application GUI using the NOAM VIP as user with admin privileges.

Procedure 32. DSR Database Restore

5.	NOAM VIP: Allow provisioning	1.	Allow replication on all servers in this order: a. Active NOAM server b. Standby NOAM server c. Active SOAM server d. Standby SOAM server e. Active MP servers f. Standby MP servers
		2.	Navigate to Status and Manage > HA.
		3.	Click Edit.
		4.	Select the Standby NOAM and change the Max Allowed HA Role to Active.
		5.	Verify proper configuration displays.

Appendix O. My Oracle Support (MOS)

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

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

- 1. Select 2 for New Service Request.
- 2. Select 3 for Hardware, Networking and Solaris Operating System Support.
- 3. Select one of the following options:

For technical issues such as creating a new Service Request (SR), select 1.

For non-technical issues such as registration or assistance with MOS, select 2.

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

Emergency Response

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

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

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

• Loss of the system ability to provide any required critical or major trouble notification

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

Locate Product Documentation on the Oracle Help Center

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

- 1. Access the Oracle Help Center site at http://docs.oracle.com.
- 2. Click Industries.
- 3. Under the Oracle Communications subheading, click the Oracle Communications documentation link. The Communications Documentation page appears. Most products covered by these documentation sets display under the headings Network Session Delivery and Control Infrastructure or Platforms.
- 4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release displays. To download a file to your location, right-click the PDF link, select **Save target as** (or similar command based on your browser), and save to a local folder.