

Oracle® Communications
Diameter Signaling Router
DSR Rack Mount Server Installation Guide
Release 8.0/8.1
E76182-03

July 2017

Oracle ® Communication Diameter Signaling Router DSR Rack Mount Server Installation Guide

Copyright © 2016,2017 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 will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, 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 on MOS in the Appendix section.

Table of Contents

Table of Contents.....	3
List of Procedures.....	6
List of Figures and Tables	9
1.0 Introduction	10
1.1 Purpose and Scope	10
1.2 References.....	10
1.3 Acronyms.....	11
1.4 Terminology.....	12
1.5 Revision History	14
2.0 General Description.....	15
2.1 Acquiring Firmware.....	16
2.1.1 HP DL380	16
2.1.2 Oracle X5-2/Netra X5-2/X6-2.....	17
3.0 Install Overview.....	17
3.1 Required Materials	17
3.2 Installation Summary	17
3.2.1 Installation Matrix	18
3.3 Optional Features	20
3.4 Rack Mount Server Network Interface Reference	21
4.0 Software Installation Procedure.....	21
4.1 Prepare Servers for IPM.....	21
4.1.1 Configure the BIOS Settings	22
4.1.2 Upgrade Rack Mount Server Firmware.....	24
4.2 Install and Configure TVOE on First RMS (PMAC Host)	25
4.3 Install PMAC	45
4.4 Initialize the PMAC Application.....	51
4.5 Configure Cisco 4948E-F Aggregation Switches (HP DL380 Gen 8 Servers Only)	54
4.5.1 Configure netConfig Repository (HP DL380 Gen 8 Servers Only)	54
4.5.2 Configure Cisco 4948E-F Aggregation Switches (HP DL380 Gen 8 Servers Only)	63
4.6 Configure PMAC Server (NetBackup Only)	72
4.7 Add Rack Mount Server to PMAC	77
4.8 Install TVOE on Additional Rack Mount Servers	81
4.9 Configure TVOE on Additional Rack Mount Servers	87
4.10 Determine VM Placement and Socket Pinning.....	102
4.11 Deploy Redundant PMAC (Optional).....	102
4.12 Virtual Machine/Network Fast Deployment	110
4.13 CPU Pinning	121

4.14	Application Configuration: DSR.....	124
4.14.1	DSR Configuration: NOAMs	124
4.14.2	DSR Configuration: NetBackup Client Installation (Optional)	143
4.14.3	DSR Configuration: Disaster Recovery NOAM (Optional)	144
4.14.3	DSR Configuration: SOAMs	153
4.14.5	DSR Configuration: Activate PCA	167
4.14.6	DSR Configuration: Activate DCA	168
4.14.7	DSR Configuration: MPs.....	169
4.14.8	DSR Configuration: Signaling Network	190
4.14.9	DSR Configuration: DSCP (Optional).....	196
4.14.10	DSR Configuration: SNMP	199
4.14.11	DSR Configuration: IP Front End (IPFE).....	206
4.15	Application Configuration: SDS	212
4.15.1	SDS Configuration: NOAMs.....	212
4.15.2	SDS Configuration: NetBackup Client Installation (Optional).....	230
4.15.3	SDS Configuration: Disaster Recovery SDS NOAM (Optional)	231
4.15.4	SDS Configuration: Query Servers.....	240
4.15.5	SDS Configuration: SOAMs	248
4.15.6	SDS Configuration: DPs.....	260
4.15.7	SDS Configuration: DSCP (Optional)	269
4.15.8	SDS Configuration: SNMP (Optional)	273
4.16	IDIH Installation and Configuration (Optional).....	276
4.16.1	IDIH Installation.....	276
4.16.2	Post IDIH Installation Configuration	281
4.17	Post-Install Activities	301
4.17.1	Optimization (DSR & Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only).....	301
4.17.2	Configure ComAgent Connections (DSR + SDS Only)	303
4.17.3	Activate Optional Features	311
4.17.4	Shared Secret Encryption Key Revocation (RADIUS Only).....	311
4.17.5	Enable/Disable DTLS (SCTP Diameter Connections Only)	311
4.17.6	Backup TVOE Configuration	312
4.17.7	Backup PMAC Application	314
4.17.8	Backup NOAM Database	317
4.17.9	Backup SOAM Database	321
Appendix A: Pre-IPM Procedures.....		324
Appendix A.1: Setting the Server's CMOS Clock		324
Appendix A.2: Configure the RMS Server BIOS Settings		324
Appendix A.2.1: Configure HP Gen 8 Servers		324
Appendix A.2.2: Configure HP Gen 9 Servers.....		327

Appendix A.2.3: Configure Oracle X5-2/Netra X5-2/X6-2 Server	331
Appendix B: Upgrade Server Firmware.....	336
Appendix B.1: HP DL 380 Server	336
Appendix B.2: Oracle X5-2/Netra X5-2/X6-2.....	343
Appendix C: Changing the SNMP Configuration Settings.....	344
Appendix D: TVOE iLO/iLOM GUI Access	346
Appendix D.1: iLO GUI Access (HP DL380).....	346
Appendix D.2: iLOM GUI Access (Oracle X5-2/Netra X5-2/X6-2).....	348
Appendix E: Changing the TVOE iLO/iLOM Address	351
Appendix E.1: HP DL 380 Servers (iLO4).....	351
Appendix E.2: Oracle X5-2/Netra X5-2/X6-2 Servers (Changing iLOM IP address using Keyboard/Monitor) ..	354
Appendix E.3: Oracle X5-2/Netra X5-2/X6-2 Servers (Changing iLOM IP address using Serial Console).....	360
Appendix F: Attaching an ISO Image to a Server using the iLO or iLOM	361
Appendix F.1: HP DL380 Servers (iLO4).....	361
Appendix F.2: Oracle X5-2/Netra X5-2/X6-2 Servers (iLOM).....	365
Appendix G: Configuring for TVOE iLO Access.....	369
Appendix H: SNMP Configuration	371
Appendix I: Application NetBackup Client Installation Procedures	372
Appendix I.1: NetBackup Client Install using PLATCFG	373
Appendix I.2: NETBACKUP CLIENT INSTALL/UPGRADE WITH NBAUTOINSTALL	383
Appendix I.3: Create NetBackup Client Config File	385
Appendix I.4: Configure PMAC Application NetBackup Virtual Disk	386
Appendix J: List of Frequently used Time Zones	392
Appendix K: Upgrade Cisco 4948 PROM	393
Appendix L: Sample Network Element	395
Appendix M: IDIH Fast Deployment Configuration	397
Appendix N: Creating a Bootable USB Drive on Linux	403
Appendix O: IDIH External Drive Removal	404
Appendix P: Growth/De-Growth/Re-Shuffle (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)	407
Appendix P.1: Growth (X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)	407
Appendix P.2: De-Growth (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)	427
Appendix P.3: Re-Shuffle (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)	451
Appendix Q: Non-HA Lab Node Instructions (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Non-HA Lab Node Only)	490
Appendix Q.1: Non-HA Lab Node Pre-IPM Procedures	491
Appendix Q.2: Non-HA Lab Node PMAC Deployment	510
Appendix Q.3: Non-HA Lab Node VM Automation Profile Values.....	516
Appendix Q.4: Non-HA Lab Node IDIH Procedure Deviation.....	517
Appendix R: VM Automation Profile Values	522

Appendix S: VM placement in HP DL380 Gen8/Gen9 (Onboard 1Gbps NICs) and CPU Pinning in HP DL380 Gen9 (Onboard 1Gbps NICs).....	523
Appendix T: Restoring SNMP configuration to SNMPv3 (Optional).....	525
Appendix U: My Oracle Support (MOS)	527

List of Procedures

Procedure 1. Configure the BIOS settings.....	22
Procedure 2. Upgrade Rack Mount Server Firmware.....	24
Procedure 3. Install and Configure TVOE on First RMS (PMAC Host).....	25
Procedure 4. First RMS Configuration.....	29
Procedure 5. PMAC Deployment	45
Procedure 6. Initialize the PMAC.....	51
Procedure 7. Configure netConfig Repository (HP DL380 Gen 8 Servers Only)	56
Procedure 8. Configure Cisco 4948E-F Aggregation Switches-netConfig (HP DL 380 Servers Only)	64
Procedure 9. Configure the PMAC Server (NetBackup Only)	72
Procedure 10. Add RMS to the PMAC system Inventory	77
Procedure 11. Install TVOE on Additional Rack Mount Servers.....	81
Procedure 12. Configure TVOE on Additional Rack Mount Servers.....	87
Procedure 13. Installing a Redundant PMAC.....	102
Procedure 14. Load DSR, SDS, and TPD ISOs to the PMAC Server	110
Procedure 15. Execute VM/Network Fast Deployment.....	114
Procedure 16. CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)	121
Procedure 17. Configure First NOAM NE and Server	124
Procedure 18. Configure the NOAM Server Group	131
Procedure 19. Configure the Second NOAM Server	135
Procedure 20. Complete NOAM Server Group Configuration.....	138
Procedure 21. Install NetBackup Client (Optional).....	143
Procedure 22. NOAM Configuration for DR Site (Optional).....	144
Procedure 23. Pairing for DR-NOAM Site (Optional)	149
Procedure 24. Configure the SOAM NE	153
Procedure 25. Configure the SOAM Servers.....	155
Procedure 26. Configure the SOAM Server Group	161
Procedure 27. Configure RMS-Specific B-Level Resources (HP DL 380 Gen 8 Servers ONLY)	167
Procedure 28. Activate PCA (PCA Only)	167
Procedure 29. Activate DCA (DCA Only)	168
Procedure 30. Configure the MP Servers	169
Procedure 31. Configure Places and Assign MP Servers to Places (PCA & DCA ONLY)	179
Procedure 32. Configure the MP Server Group(s) and Profile(s).....	182

Procedure 33. Configure the Signaling Network Routes	190
Procedure 34. Configure DSCP Values for Outgoing Traffic (Optional).....	196
Procedure 35. Configure SNMP Trap Receiver(s)	199
Procedure 36. IP Front End (IPFE) Configuration (Optional).....	206
Procedure 37. Configure First SDS NOAM NE and Server.....	212
Procedure 38. Configure the SDS NOAM Server Group	219
Procedure 39. Configure the Second SDS NOAM Server.....	222
Procedure 40. Complete SDS NOAM Server Group Configuration	226
Procedure 41. Install NetBackup Client (Optional).....	230
Procedure 42. SDS NOAM Configuration for DR Site (Optional)	231
Procedure 43. Pairing for SDS DR-NOAM Site (Optional).....	236
Procedure 44. Configuring SDS Query Servers	240
Procedure 45. Query Server SDS NOAM Pairing.....	245
Procedure 46. Configure the SDS DP SOAM NE	248
Procedure 47. Configure the SDS DP SOAM Servers	250
Procedure 48. Configure the SDS DP SOAM Server Group.....	255
Procedure 49. Configure the SDS DP Servers.....	260
Procedure 50. Configure the SDS DP Server Group(s)	265
Procedure 51. Configure DSCP Values for Outgoing Traffic (Optional).....	269
Procedure 52. Configure SNMP Trap Receiver(s) (Optional).....	273
Procedure 53. IDIH Installation (Optional)	276
Procedure 54. Configure DSR Reference Data Synchronization for IDIH (Optional)	281
Procedure 55. IDIH Configuration: Configuring the SSO Domain (Optional)	283
Procedure 56. IDIH Configuration: Configure IDIH in the DSR (Optional).....	290
Procedure 57. IDIH Configuration: Configure Mail Server-Optional (Optional).....	294
Procedure 58. IDIH Configuration: Configure SNMP Management Server-Optional (Optional)	296
Procedure 59. IDIH Configuration: Change Network Interface-Optional (Optional)	298
Procedure 60. IDIH Configuration: Backup the upgrade and Disaster Recovery FDC File-Optional (Optional)	299
Procedure 61. Optimization Procedure (DSR & Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)	301
Procedure 62. Configure ComAgent Connections (DSR + SDS Only).....	303
Procedure 63. Activate Optional Features	311
Procedure 64: Shared secret encryption key revocation (RADIUS Only).....	311
Procedure 65. Enable/Disable DTLS (SCTP Diameter Connections Only	312
Procedure 66. Backup TVOE Configuration	312
Procedure 67. Backup PMAC Application.....	314
Procedure 68. NOAM Database Backup	317
Procedure 69. SOAM Database Backup.....	321
Appendix A.2.1. Configure HP Gen 8 Server BIOS Settings.....	324

Appendix A.2.2. Configure HP Gen 9 Server BIOS Settings.....	327
Appendix A.2.3.1. Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings	331
Appendix A.2.3.2. Enable Oracle Netra X5-2/X6-2 CPU Power Limit for NEBS (Optional).....	334
Appendix A.2.3.3. Disable Oracle Netra X5-2/X6-2 CPU Power Limit for NEBS (Optional).....	335
Appendix B.1.1 Upgrade HP DL380 Server Firmware	337
Appendix C.1. Changing SNMP Configuration Settings for HP DL 380.....	344
Appendix D.1. TVOE iLO4 GUI Access	346
Appendix D.2. TVOE iLOM GUI Access.....	348
Appendix E.1. Changing the TVOE iLO Address.....	351
Appendix E.2. Changing the TVOE Oracle X5-2/Netra X5-2/X6-2 iLOM Address using keyboard/Monitor.....	354
Appendix E.3. Changing the TVOE Oracle X5-2/Netra X5-2/X6-2 iLOM Address using Serial Console	360
Appendix F.1.1 HP DL380 Servers Mounting the ISO image via iLO4	362
Appendix F.2.2. Oracle X5-2/Netra X5-2/X6-2 Servers Mounting the ISO image via iLOM.....	365
Appendix G.1 Connecting to the TVOE iLO	369
Appendix I.1. Application NetBackup Client Installation (Using Platcfg).....	373
Appendix I.2. Application NetBackup Client Installation (NBAUTOINSTALL)	383
Appendix I.3. Create NetBackup Client Config File	385
Appendix I.4. Configure the PMAC Application Guest NetBackup Virtual Disk	386
Appendix K.1. Upgrade Cisco 4948 PROM.....	393
Appendix P.1. Creating a Bootable USB Drive on Linux	403
Appendix O.2. IDIH External Drive Removal	404
Appendix P.1.1 Perform Backups	408
Appendix P.1.2 Perform Health Check	409
Appendix P.1.3 Adding a new TVOE Server/VMs.....	411
Appendix P.1.4 Growth: DR-NOAM.....	412
Appendix P.1.5 Growth: SOAM spare (DSR/PCA Only)	413
Appendix P.1.6 Growth: MP/DP	414
Appendix P.1.6.1 Growth: MP (7.x to 8.x upgraded system)	415
Appendix P.1.7 Growth: Query Server (SDS Only).....	423
Appendix P.1.8 Post Growth Health Check	423
Appendix P.1.9 Post Growth Backups.....	426
Appendix P.2.1 Perform Backups	427
Appendix P.2.2 Perform Health Check	428
Appendix P.2.3 Removing Server from Server Group	431
Appendix P.2.4 Deleting Server/Server Group.....	442
Appendix P.2.5 Deleting the server VM.....	445
Appendix P.2.6 Post De-Growth Health Check.....	448
Appendix P.2.7 Post De-Growth Backups.....	450
Appendix P.3.1 Perform Backups	452

Appendix P.3.2 Perform Health Check	453
Appendix P.3.3 Adding a new TVOE Server	456
Appendix P.3.4 Placing Server in OOS	457
Appendix P.3.5 Deleting the server VM.....	459
Appendix P.3.6 Moving/Re-Shuffle: Creating/Configuring Virtual Machines	462
Appendix P.3.7 Moving/Re-Shuffle: NOAM/DR-NOAM.....	463
Appendix P.3.8 Moving/Re-Shuffle: SOAM.....	466
Appendix P.3.9 Moving/Re-Shuffle: MP/DP	469
Appendix P.3.10 Moving/Re-Shuffle: Query Server (SDS Only)	475
Appendix P.3.11 Moving/Re-Shuffle: IDIH	478
Appendix P.3.12 Moving/Re-Shuffle: PMAC.....	481
Appendix P.3.13 Moving/Re-Shuffle: Redundant PMAC.....	485
Appendix P.3.14 Post Moving/Re-Shuffle Health Check.....	486
Appendix P.3.15 Post Move/Re-Shuffle Backups	489
Appendix Q.1.1 RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X5-2/Netra X5-2)	491
Appendix Q.1.2 RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2)	496
Appendix Q.1.3 RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380 Gen9).....	503
Appendix Q.2.1 PMAC Deployment: Procedure 6 Deviation	510
Appendix Q.4.1 IDIH Installation: Procedure 58 Deviation	517

List of Figures and Tables

Table 1. Acronyms.....	11
Figure 1. Example of an instruction that indicates the server to which it applies	12
Table 2. Terminology	14
Figure 2. Initial Application Installation Path-Example Shown	15
Figure 3. DSR Installation Procedure Map	19
Table 3. Time Zones	392
Figure 4. Example Network Element XML File	396
Table 4: VM Automation Profile Values	522
Figure 5. HP DL380 Gen8/Gen9(1Gbps) VM placement non-HA LAB deployment	523
Figure 6. HP DL380 Gen8/Gen9(1Gbps) VM placement small production DSR with IDIH.....	523
Figure 7. HP DL380 Gen8/Gen9(1Gbps) VM placement scaled DSR.....	523
Figure 8. HP DL380 Gen9(1Gbps) VM placement scaled DSR with SS7 MPs and IDIH.....	524
Table 5.HP DL380 Gen9 (1Gbps) CPU Pinning without SS7MPs	524
Table 6.HP DL380 Gen9 (1Gbps) CPU Pinning with SS7MPs.....	525

1.0 Introduction

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to configure HP DL-380 Gen8/9 or Oracle Rack Mount Servers (RMS) to be used with Oracle Communication Diameter Signaling Router. It is assumed that the hardware installation and network cabling were executed beforehand. The audience for this document includes Oracle customers as well as these groups: Software System, Product Verification, Documentation, and Customer Service including Software Operations and First Office Application. Throughout the remainder of this document, the term RMS refers to either HP DL-380 Gen8/9 or Oracle Rack Mount Servers.

Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only: In scenarios where the DSR installation has already been executed, and system **growth, de-growth, or re-shuffle** is necessary; refer to **Appendix P: Growth/De-Growth/Re-Shuffle (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)**

[FIPS integrity verification test failed]: Throughout this procedure, an error message of *“FIPS integrity verification test failed”* will be displayed while performing various procedures on the command line (SSH, feature activations, etc.). This error message is harmless, and should be ignored.

1.2 References

Software Centric Customers do not receive firmware upgrades through Oracle. Instead, refer to the HP Solutions Firmware Upgrade Pack, Software Centric Release Notes on <https://docs.oracle.com> under Platform documentation. The latest version is recommended if an upgrade is performed, otherwise version 2.2.9 is the minimum.

- [1] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes (Min 2.2.9)
- [2] HP Solutions Firmware Upgrade Pack, version 2.x.x (Min 2.2.9)
- [3] Oracle Firmware Upgrade Pack Release Notes (Min 3.1.7)
- [4] Oracle Firmware Upgrade Pack Upgrade Guide
- [5] Communication Agent User's Guide
- [6] DSR Communication Agent Configuration Guide
- [7] DSR Range Based Address Resolution (RBAR) Feature Activation
- [8] DSR MAP-Diameter IWF Feature Activation Procedure
- [9] DSR Meta Administration Feature Activation Procedure
- [10] DSR Full Address Based Resolution (FABR) Feature Activation
- [11] Gateway Location Application (GLA) Feature Activation
- [12] DSR PCA Activation Guide
- [13] DSR IPv6 Migration Guide
- [14] DSR Hardware and Software Installation Procedure 1/2
- [15] DSR DTLS Feature Activation Procedure
- [16] DSR VM Placement and CPU Socket Pinning Tool
- [17] DSR RADIUS Shared secret encryption key revocation MOP MO008572
- [18] TPD Initial Product Manufacture Software Installation Procedure
- [19] DSR Security Guide
- [20] DCA Framework and Application Activation and Deactivation Guide

1.3 Acronyms

An alphabetized list of acronyms used in the document:

Table 1. Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CD	Compact Disk
DSR	Diameter Signaling Router
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
FRU	Field Replaceable Unit
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 (e.g. 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
PCA	Policy and Charging Application
IDIH	Integrated Diameter Intelligence Hub
PCA	Policy and Charging Application
SDS	Subscriber Database Server

1.4 Terminology

Multiple server types may be involved with the procedures in this manual. Therefore, most steps in the written procedures begin with the name or type of server to which the step applies. For example:

Each step has a checkbox for every command within the step that the technician should check to keep track of the progress of the procedure.

The title box describes the operations to be performed during that step.

Each command that the technician is to enter is in 10 point bold Courier font.

5	ServerX: Connect to the console of the server	Establish a connection to the server using cu on the terminal server/console. <code>\$ cu -l /dev/ttyS7</code>

Figure 1. Example of an instruction that indicates the server to which it applies

Management Server	HP ProLiant DL380 or Oracle X5-2/ Netra X5-2/X6-2 deployed to run TVOE and host a virtualized PMAC application.
PMAC Application	PMAC is an application that provides platform-level management functionality for HP DL380, and Oracle X5-2/Netra X5-2/X6-2 system, such as the capability to manage and provision platform components of the system so it can host applications.
Site	Applicable for various applications, a Site is type of "Place". A Place is configured object that allows servers to be associated with a physical location. A Site place allows servers to be associated with a physical site. For example, Sites may be configured for Atlanta, Charlotte, and Chicago. Every server is associated with exactly one Site when the server is configured. For the Policy & Charging DRA application, when configuring a Site only put DA-MPs and SBR MP servers in the site. Do not add NOAM, SOAM or IPFE MPs to a Site

Place Association	Applicable for various applications, a “Place Association” is a configured object that allows Places to be grouped together. A Place can be a member of more than one Place Association. The Policy & Charging DRA application defines two Place Association Types: Policy Binding Region and Policy & Charging Mated Sites.
Two Site Redundancy	Two Site Redundancy is a data durability configuration in which Policy and Charging data is unaffected by the loss of one site in a Policy & Charging Mated Sites Place Association containing two sites. Two Site Redundancy is a feature provided by Server Group configuration. This feature provides geographic redundancy. Some Server Groups can be configured with servers located in two geographically separate Sites (locations). This feature will ensure that there is always a functioning Active server in a Server Group even if all the servers in a single site fail.
Session Binding Repository Server Group Redundancy	The DCA application may use SBR Server Groups to store Application Session data. The SBR Server Groups with support both Two and Three Site Redundancy. The Server Group Function name is “Session and Binding Repository”.
SBR Server Group Redundancy	The Policy and Charging application will use SBR Server Groups to store the application data. The SBR Server Groups will support both Two and Three Site Redundancy. The Server Group Function name is “SBR”.
Server Group Primary Site	A Server Group Primary Site is a term used to represent the principle location within a SOAM or SBR Server Group. SOAM and SBR Server groups are intended to span several Sites (Places). For the Policy & Charging DRA application, these Sites (Places) are all configured within a single “Policy and Charging Mated Sites” Place Association. For the Diameter Custom application, these Sites (Places) are configured in “Applications Region” Place Association. The Primary Site may be in a different Site (Place) for each configured SOAM or SBR Server Group. A Primary Site is described as the location in which the Active and Standby servers to reside, however there cannot be any Preferred Spare servers within this location. All SOAM and SBR Server Groups will have a Primary Site.

Server Group Secondary Site	A Server Group Secondary Site is a term used to represent location in addition to the Primary Site within a SOAM or SBR Server Group. SOAM and SBR Server groups are intended to span several Sites (Places). For the Policy & Charging DRA application, these Sites (Places) are all configured within a single “Policy and Charging Mated Sites” Place Association. For the Diameter Custom application, these Sites (Places) are configured in “Applications Region” Place Association. The Secondary Site may be in a different Site (Place) for each configured SOAM or SBR Server Group. A Secondary Site is described as the location in which only Preferred Spare servers reside. The Active and Standby servers cannot reside within this location. If Two or Three Site Redundancy is wanted, a Secondary Site is required for all SOAM and SBR Server Groups.
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, and is not responsible for hardware installation, configuration, or maintenance.
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.

Table 2. Terminology

1.5 Revision History

Date	Description
October 2016	Initial Release

2.0 General Description

This document defines the steps to execute the initial installation of the Diameter Signaling Router application.

DSR installation paths are shown in the figures below. The general timeline for all processes to perform a software installation/configuration and upgrade is also included below.

This document covers initial installation of the DSR application on a Rack mount server system.

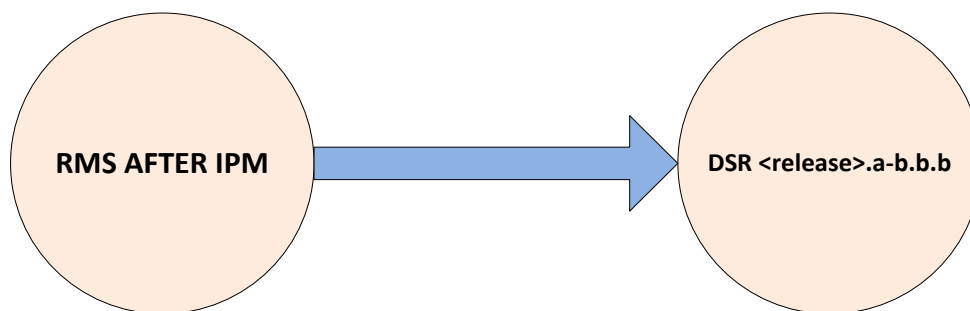


Figure 2. Initial Application Installation Path-Example Shown

2.1 Acquiring Firmware

Several procedures in this document pertain to the upgrading of firmware on various servers and hardware devices.

DSR rack mount servers and devices requiring possible firmware updates are:

- HP Rack Mount Servers (DL380)
- Oracle Rack Mount Server
- Cisco 4948/4948E/4948E-F Rack Mount Network Switches

2.1.1 HP DL380

Software Centric Customers do not receive firmware upgrades through Oracle. Instead, refer to the HP Solutions Firmware Upgrade Pack, Software Centric Release Notes on <https://docs.oracle.com> under Platform documentation. The latest release is recommended if an upgrade is performed, otherwise release 2.2.9 is the minimum.

The required firmware and documentation for upgrading the firmware on HP hardware systems and related components are distributed as the HP Solutions Firmware Upgrade Pack 2.x.x. The minimum firmware release required is HP Solutions Firmware Upgrade Pack 2.2.9. However, if a firmware upgrade is needed, the current GA release of the HP Solutions Firmware Upgrade Pack 2.x.x should be used.

Each version of the HP Solutions Firmware Upgrade Pack contains multiple items including media and documentation. This document provides its own upgrade procedures for firmware. The two pieces of required firmware media provided in the HP Solutions Firmware Upgrade Pack 2.x.x releases are:

- HP Service Pack for ProLiant (SPP) firmware ISO image

Refer to the HP Solutions Firmware Upgrade Pack Release Notes [1] of the HP FUP release to determine specific firmware versions provided.

Contact Appendix U: My Oracle Support (MOS) for more information on obtaining the HP Firmware Upgrade Pack.

2.1.2 Oracle X5-2/Netra X5-2/X6-2

The Oracle Firmware Upgrade Pack (FUP) consists of documentation used to assist in the upgrading of Oracle rack mount servers. The pack consists of an upgrade guide and release notes. The current minimum supported release is 3.1.7. However, if a firmware update is required, it is recommended to use the latest available release. Firmware components can be downloaded from My Oracle Support at <https://support.oracle.com>. Refer to the appropriate FUP release notes for directions on how to acquire the firmware.

3.0 Install Overview

This section provides a brief overview of the recommended method for installing the Target Release software. .

3.1 Required Materials

1. One (1) target release DSR Media ISO
2. One (1) target release SDS Media ISO (If equipped)
3. One (1) target release PMAC Media ISO
4. Three (3) target release IDIH Media ISOs
5. One (1) ISO of TPD release, or later shipping baseline as per Oracle ECO
6. One (1) ISO of TVOE release, or later shipping baseline as per Oracle ECO
7. One (1) TVOE release bootable USB, or later shipping baseline as per Oracle ECO
8. To obtain the default passwords refer to document cgbu_eng_24_2229.
9. HP Solutions Firmware Upgrade Pack Release Notes[2]

3.2 Installation Summary

This section lists the procedures required for installation with estimated times. **Section 3.2.1** contains a matrix of deployment features and the required procedures needed to install them. Section 3.2.2 lists the steps required to install a DSR system. These latter sections expand on the information from the matrix and provide a general timeline for the installation.

3.2.1 Installation Matrix

Figure 3. DSR Installation Procedure Map illustrates the overall process that each DSR installation will involve. In summary:

- 1) An overall installation requirement is decided upon. Among the data that should be collected:
 - The Total number of Rack Mount Servers
 - The number of VMs and servers on each Rack Mount Server and their role(s)
 - Does the deployment include 4948 aggregation switches (HP DL380 Gen 8 Only)?
 - What time zone should be used across the entire collection of DSR sites?
 - Will SNMP traps be viewed at the NOAM, or will an external NMS be used? (Or both?)
 - PCI cards installed? (HP DL380 Gen 9 (10Gbps) Only) – Segregated Signaling Only

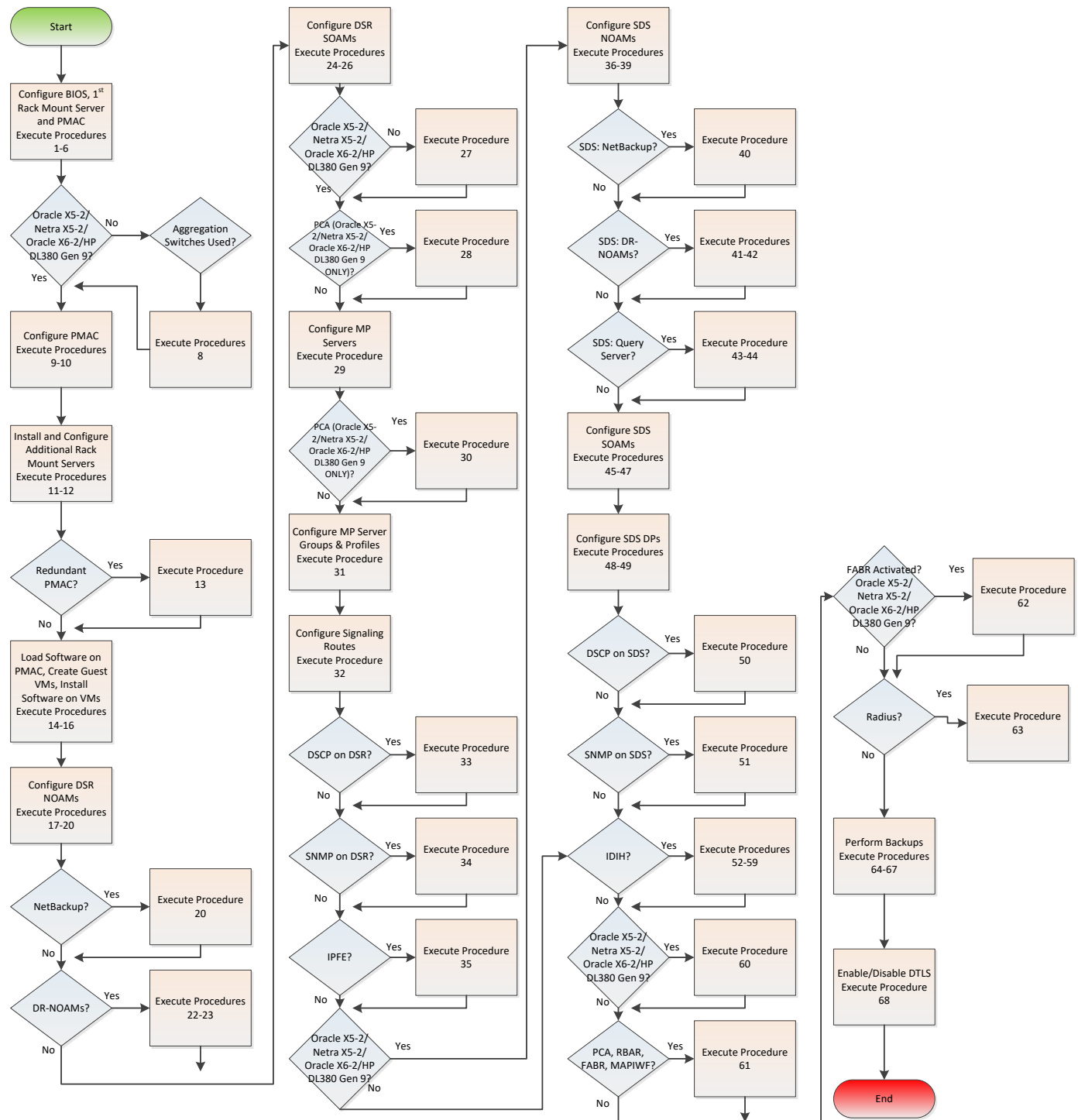


Figure 3. DSR Installation Procedure Map

3.3 Optional Features

When DSR installation is complete, further configuration and/or installation steps will need to be taken for optional features that may be present in this deployment. Please refer to these documents for the post-DSR install configuration steps needed for their components.

Feature	Document
Diameter Mediation	DSR Meta Administration Feature Activation Procedure, E58661
Policy and Charging Application (PCA)	DSR PCA Activation Procedure E81528
Diameter Custom Applications (DCA)	DCA Framework and Application Activation and Deactivation Guide, E76934
Full Address Based Resolution (FABR)	DSR FABR Feature Activation Procedure, E78925
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation Procedure, E78926
Map-Diameter Interworking (MAP-IWF)	DSR MAP-Diameter IWF Feature Activation Procedure, E78927
Gateway Location Application (GLA)	DSR GLA Feature Activation Procedure, E78916
Host Intrusion Detection System (HIDS)	DSR Security Guide, E76974 (Section 3.2)

3.4 Rack Mount Server Network Interface Reference

Throughout the installation procedure, configuration steps will reference Ethernet interfaces. Depending on the hardware type, these Ethernet interfaces can vary. The following table describes the Ethernet Interface to <Ethernet_interface_x> variables:

Note: For HP DL380 Gen 9 servers with 10Gbps, one 2pt 10 Gigabit FlexibleLOM cards is required. One 2 pt 10 Gigabit PCIe card is required while running the segregated signaling network topology.

Network Interface	HP DL380 (with 4pt Gigabit in PCI Slot 1) (Gen 8/Gen9 Onboard)	HP DL380 (with FlexibleLOM and 2pt 10 Gigabit in PCI slot 3) (Gen 9 10Gbps)	Oracle X5-2/Netra X5-2/X6-2 (without 10GigE card)
<ethernet_interface_1>	eth01	eth05	eth01
<ethernet_interface_2>	eth02	eth06	eth03
<ethernet_interface_3>	eth11	eth31	eth02
<ethernet_interface_4>	eth12	eth32	eth04

4.0 Software Installation Procedure

As mentioned earlier, the hardware installation and network cabling should be done before executing the procedures in this document.

SUDO

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

IPv6

IPv6 configuration of XMI and IMI networks has been introduced in DSR 7.1. Standard IPv6 formats for IPv6 and prefix can be used in all IP configuration screens which enable the DSR to be run in an IPv6 only environment. When using IPv6 for XMI and management, you must place the IPv6 address in brackets (highlighted in red below), example as followed:

```
https://[<IPv6 address>]
```

If a dual-stack (IPv4 & IPv6) network is required, it is recommended that you first configure the topology with IPv4, and then "Migrate" to IPv6. Reference [13] for instructions on how to accomplish this migration.

4.1 Prepare Servers for IPM

This section explains the steps needed to configure the BIOS settings and update the firmware (if needed) for the HP and Oracle rack mount servers.

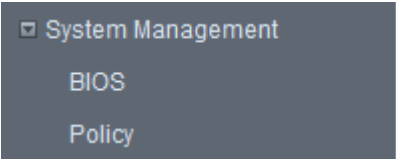
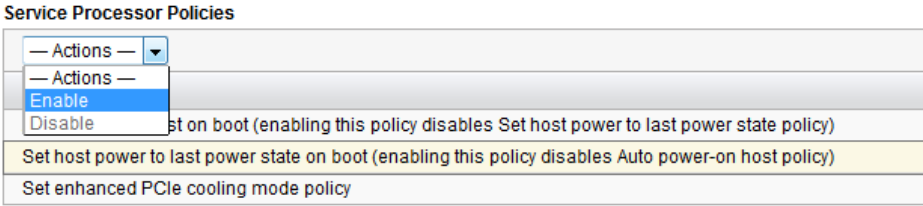
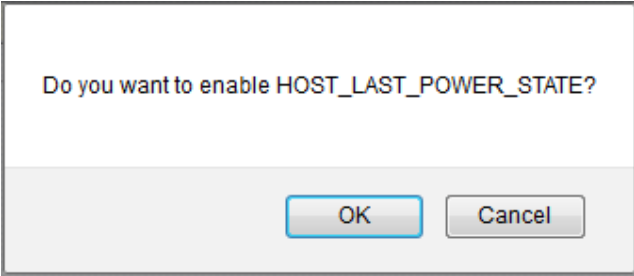
4.1.1 Configure the BIOS Settings

The following procedure explains the steps needed to configure the BIOS settings.

Procedure 1. Configure the BIOS settings

S T E P #	This procedure explains the steps needed to configure HP DL380 and Oracle Server BIOS Settings. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	RMS Server: Configure the BIOS Settings	Follow the appropriate Appendix procedure for the corresponding hardware type: • HP DL 380 Gen 8 RMS: Appendix A.2.1: Configure HP Gen 8 Servers • HP DL 380 Gen 9 RMS: Appendix A.2.2: Configure HP Gen 9 Servers • Oracle X5-2/Netra X5-2/X6-2: Appendix A.2.3: Configure Oracle X5-2/Netra X5-2/X6-2 Only, HP DL380 SKIP THIS STEP
2 ☐	Oracle X5-2/Netra X5-2/X6-2 Server: Login	Login to the Oracle X5-2/Netra X5-2/X6-2 iLOM: Please Log In SP Hostname: DSR10307Loc37TVOE User Name: Password: Log In  Copyright © 2015, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Procedure 1. Configure the BIOS settings

3 ☐	Oracle X5-2/Netra X5-2/X6-2 Server: Update Power Settings	Oracle X5-2/Netra X5-2/X6-2 Only, HP DL380 SKIP THIS STEP Navigate to System Management -> Policy  Select <i>“Set host power to last power state on boot”</i>  Select Enable from the Actions drop down box Select Ok to confirm 

4.1.2 Upgrade Rack Mount Server Firmware

The following procedure explains the steps needed to upgrade the firmware of the rack mount servers (if needed).

Procedure 2. Upgrade Rack Mount Server Firmware

STEP #	This procedure explains the steps needed to update the firmware if needed.																																													
	Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.																																													
	If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.																																													
1	RMS Server: Verify Firmware	Verify firmware version of the rack mount server: For Oracle X5-2/Netra X5-2/X6-2: From the iLOM, login and verify firmware version under System Information -> Summary: General Information <table><tr><td>System Type</td><td>Rack Mount</td></tr><tr><td>Model</td><td>SUN SERVER X4-2</td></tr><tr><td>QPart ID</td><td>Q10540</td></tr><tr><td>Part Number</td><td>33300320+2+1</td></tr><tr><td>Serial Number</td><td>1507NML0TC</td></tr><tr><td>System Identifier</td><td>-</td></tr><tr><td>System Firmware Version</td><td>3.2.4.46</td></tr><tr><td>Primary Operating System</td><td>Oracle Linux Server release 6.6</td></tr><tr><td>Host Primary MAC Address</td><td>00:10:e0:70:43:54</td></tr><tr><td>ILOM Address</td><td>10.250.50.193</td></tr><tr><td>ILOM MAC Address</td><td>00:10:E0:70:43:58</td></tr></table> For HP DL380: From the iLO, login and verify firmware version under Information -> System Information [Firmware Tab]: System Information - Firmware Information SummaryFansTemperaturesPowerProcessorsMemoryNetworkStorageFirmware Firmware Version Info <table><tr><th>Firmware Name</th><th>Firmware Version</th></tr><tr><td>HP ProLiant System ROM</td><td>02/10/2014</td></tr><tr><td>HP ProLiant System ROM - Backup</td><td>03/01/2013</td></tr><tr><td>HP ProLiant System ROM Bootblock</td><td>03/11/2012</td></tr><tr><td>HP Smart Array P420i Controller</td><td>5.42</td></tr><tr><td>iLO</td><td>1.51 Jun 16 2014</td></tr><tr><td>Power Management Controller Firmware</td><td>3.3</td></tr><tr><td>Power Management Controller Firmware Bootloader</td><td>2.7</td></tr><tr><td>SAS Programmable Logic Device</td><td>Version 0x0C</td></tr><tr><td>Server Platform Services (SPS) Firmware</td><td>2.1.5.28.4</td></tr><tr><td>System Programmable Logic Device</td><td>Version 0x2F</td></tr></table>	System Type	Rack Mount	Model	SUN SERVER X4-2	QPart ID	Q10540	Part Number	33300320+2+1	Serial Number	1507NML0TC	System Identifier	-	System Firmware Version	3.2.4.46	Primary Operating System	Oracle Linux Server release 6.6	Host Primary MAC Address	00:10:e0:70:43:54	ILOM Address	10.250.50.193	ILOM MAC Address	00:10:E0:70:43:58	Firmware Name	Firmware Version	HP ProLiant System ROM	02/10/2014	HP ProLiant System ROM - Backup	03/01/2013	HP ProLiant System ROM Bootblock	03/11/2012	HP Smart Array P420i Controller	5.42	iLO	1.51 Jun 16 2014	Power Management Controller Firmware	3.3	Power Management Controller Firmware Bootloader	2.7	SAS Programmable Logic Device	Version 0x0C	Server Platform Services (SPS) Firmware	2.1.5.28.4	System Programmable Logic Device	Version 0x2F
System Type	Rack Mount																																													
Model	SUN SERVER X4-2																																													
QPart ID	Q10540																																													
Part Number	33300320+2+1																																													
Serial Number	1507NML0TC																																													
System Identifier	-																																													
System Firmware Version	3.2.4.46																																													
Primary Operating System	Oracle Linux Server release 6.6																																													
Host Primary MAC Address	00:10:e0:70:43:54																																													
ILOM Address	10.250.50.193																																													
ILOM MAC Address	00:10:E0:70:43:58																																													
Firmware Name	Firmware Version																																													
HP ProLiant System ROM	02/10/2014																																													
HP ProLiant System ROM - Backup	03/01/2013																																													
HP ProLiant System ROM Bootblock	03/11/2012																																													
HP Smart Array P420i Controller	5.42																																													
iLO	1.51 Jun 16 2014																																													
Power Management Controller Firmware	3.3																																													
Power Management Controller Firmware Bootloader	2.7																																													
SAS Programmable Logic Device	Version 0x0C																																													
Server Platform Services (SPS) Firmware	2.1.5.28.4																																													
System Programmable Logic Device	Version 0x2F																																													
2	RMS Server: Upgrade Firmware	Follow the appropriate Appendix procedure for the corresponding hardware type: • HP DL 380 Gen 8/9 RMS: Appendix B.1: HP DL 380 Server • Oracle Rack Mount Servers: Appendix B.2:																																												

4.2 Install and Configure TVOE on First RMS (PMAC Host)

This section describes the process of installing TVOE on the first rack mount server. Throughout this section, the first RMS server refers to the server that shall host the PMAC VM.

Note: [Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/HP DL380 GEN 9]: Before starting Procedure 3, follow **Appendix Q.1: Non-HA Lab Node Pre-IPM Procedures** to create vgguests logical volume with RAID10 spanning across multiple HDDs.

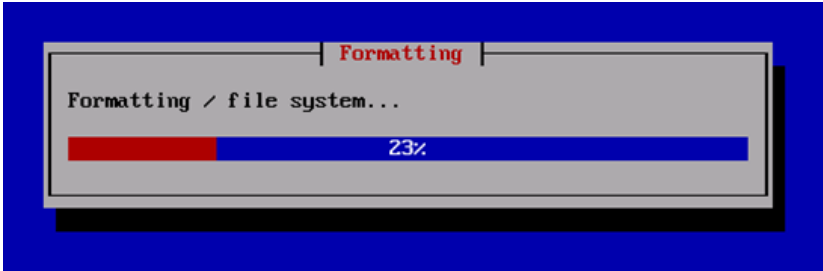
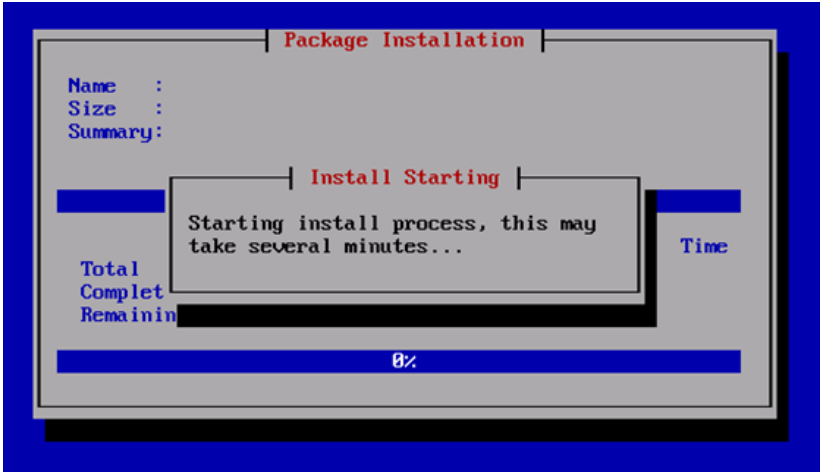
Procedure 3. Install and Configure TVOE on First RMS (PMAC Host)

S T E P #		This procedure explains the steps needed to install TVOE on the first RMS Server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	Connect to the First RMS Server	Connect to the Server using a VGA Display and USB Keyboard, or via the iLO interface using IE. Note: Appendix D: TVOE iLO/iLOM GUI Access and Appendix E: Changing the TVOE iLO/iLOM Address explains how to access the rack mount server iLO and change the address if necessary.
2 ☐	RMS Server : Insert TVOE Media into Server	Insert the OS IPM media (CD/DVD or USB) into the CD/DVD tray/USB slot of the rack mount server. Refer to Appendix N: Creating a Bootable USB Drive on Linux N for creating a bootable USB Alternatively ISO can be mounted using Virtual media as well. Refer to Appendix F: Attaching an ISO Image to a Server using the iLO or iLOM.
3 ☐	Power Cycle Server	Power cycle the server: - For HP rack mount servers, hold the power button in until the button turns amber, then release. Wait 5 seconds, then press the power button and release it again to power on the system. - For Oracle rack mount servers, hold the power button in until the “OK” LED turns off, and starts a slow blink. Wait 5 seconds and press the power button and release it again to power on the system. In a second or 2 the “OK” LED will start to blink faster as the system powers up.
4 ☐	Select Boot Method	For some servers you must select a boot method so that the server does not boot directly from the hard drive. - For HP rack mount servers, hit F11 when prompted to bring up the boot menu and select the appropriate boot method. - For Oracle rack mount servers, hit F8 when prompted to bring up the Boot Pop Up Menu then select the appropriate boot method
5 ☐	RMS Server : Begin IPM Process	Once the Server reboots, it will reboot from the TVOE media and a boot prompt shall be displayed:

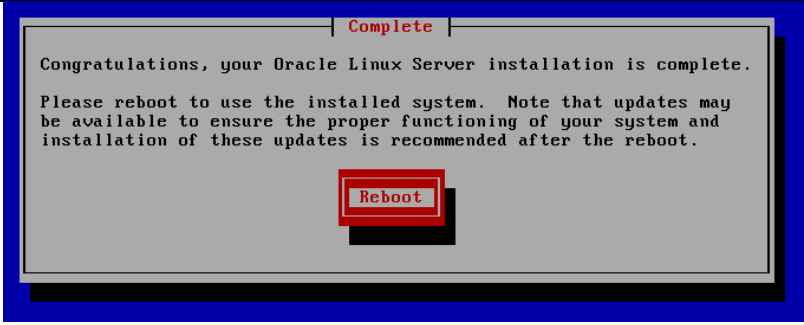
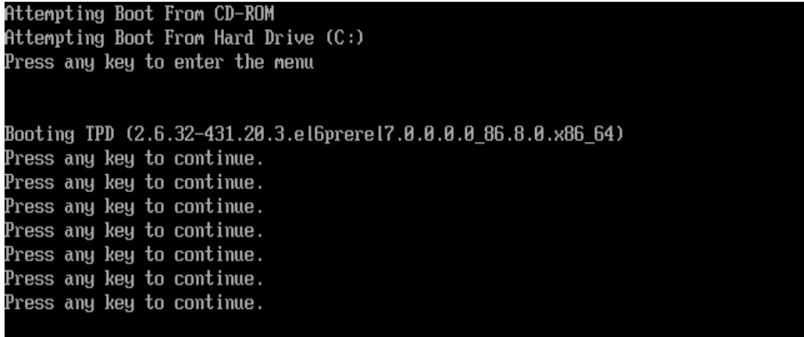
Procedure 3. Install and Configure TVOE on First RMS (PMAC Host)

		<pre> Copyright (C) 2003, 2014, Oracle and/or its affiliates. All rights reserved. Welcome to Tekelec Platform Distribution! Release: 7.0.0.0_06.11.0 Arch: x86_64 For a detailed description of all the supported commands and their options, please refer to the Initial Platform Manufacture document for this release. In addition to linux & rescue TPD provides the following kickstart profiles: [TPD : TPDnoraaid : TPDblade : TPDcompact : HDD] Commonly used options are: [console=<console_option>[,<console_option>]] [primaryConsole=<console_option>] [rdate=<server_ip>] [scrub] [reserved=<size1>[,<sizeN>]] [diskconfig=HWRAID[,force]] [drives=<device>[,device]] [guestArchive] To install using a monitor and a local keyboard, add console=tty0 boot: _ </pre> IPM the server using the following command: <pre>TPDnoraaid diskconfig=HWRAID,force console=tty0</pre> HP DL 380 Gen9 Only (equiped with 10GB FlexLOM): <pre>TPDnoraaid diskconfig=HWRAID,force console=tty0 control_if=eth05,eth06</pre> For Non-HA Lab node (Oracle X5-2/Netra X5-2/X6-2), execute the following command: <pre>TPDnoraaid drives=<Volume ID recorded in procedure Q.1.1-Q.1.3> console=tty0</pre> For Non-HA Lab node (HP DL380 Gen9 equiped with 10GB FlexLOM), execute the following command: <pre>TPDnoraaid drives=<Volume ID recorded in procedure S.1/S.2> console=tty0 control_if=eth05,eth06</pre>
6 ☐	RMS Server : Monitor the IPM Installation	The IPM process takes about 30 minutes, you will see several messages and screens in the process. The following screens will be displayed:

Procedure 3. Install and Configure TVOE on First RMS (PMAC Host)

		<pre> please refer to the Initial Platform Manufacture document for this release. In addition to linux & rescue TPD provides the following kickstart profiles: [TPD : TPDnoraide : TPDblade : TPDbladeraide : TPDnocons : I1200sol : HDD] Commonly used options are: [console=<console_option>[,<console_option>]] [rdate=<server_ip>] [scrub] [reserved=<size1>[,<sizeN>]] [diskconfig=HPC6[,<force>]] [drives=<device>[,<device>]] To install using a monitor and a local keyboard, add console=tty0 boot: TPD Loading vmlinuz..... Loading initrd.img..... Ready. </pre>  	
7 ☐	RMS Server : Install Complete- Reboot	Once the IPM is complete, you will be prompted to press Enter as shown below. Remove the disk from the drive or unmount the TPD image from the iLO and press Enter to reboot the server.	

Procedure 3. Install and Configure TVOE on First RMS (PMAC Host)

		 After a few minutes and multiple reboots, the the server boot sequence will start and eventually display that it is booting the new IPM load.  Note: A successful IPM platform installation process results in a user login prompt.
8 ☐	For NEBS and non NEBS deployment (Oracle Netra X5-2/X6-2 Server only)	For NEBS and non NEBS deployment execute below steps (Oracle Netra X5-2/X6-2 Server only): • For NEBS deployment configuration execute A.2.3.2 • For non-NEBS deployment configuration execute A.2.3.3

Procedure 4. First RMS Configuration

S T E P #	This procedure will configure the First TVOE/Management Server Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

Procedure 4. First RMS Configuration

1 ☐	Determine Bridge Names and Interfaces	Determine the bridge interfaces to be used on the TVOE server and fill in the appropriate values in the table below. If NetBackup is to be used, determine the bridge interface to be used for the NetBackup network and fill in the <TVOE_NetBackup_Bridge_Interface> value. <table border="1"> <thead> <tr> <th>Guest Interface Alias</th> <th>TVOE Bridge Name</th> <th>TVOE Bridge Interface</th> </tr> </thead> <tbody> <tr> <td>control</td> <td>control</td> <td> Fill in the appropriate value (default is bond0): <TVOE_Control_Bridge_Interface> </td> </tr> <tr> <td>management</td> <td>management</td> <td> Fill in the appropriate value: <TVOE_Management_Bridge_Interface> </td> </tr> <tr> <td>xmi</td> <td>xmi</td> <td> Fill in the appropriate value: <TVOE_XMI_Bridge_Interface> </td> </tr> <tr> <td>imi</td> <td>Imi</td> <td> Fill in the appropriate value: <TVOE_IMI_Bridge_Interface> </td> </tr> <tr> <td>Int (iDIH Only)</td> <td>Int</td> <td> Fill in the appropriate value: <TVOE_INT_Bridge_Interface> </td> </tr> <tr> <td>xsi1-16</td> <td>xsi1-16</td> <td> Fill in the appropriate value: xsi1: xsi2: xsi3: xsi4: xsi5: xsi6: xsi7: xsi8: xsi9: xsi10: xsi11: xsi12: xsi13: xsi14: xsi15: xsi16: <TVOE_XSI1-16_Bridge_Interface> </td> </tr> <tr> <td>replication</td> <td>replication</td> <td> Fill in the appropriate value: <TVOE_REPLICATION_Bridge_Interface> </td> </tr> <tr> <td>NetBackup (if applicable)</td> <td>NetBackup</td> <td> Fill in the appropriate value: <TVOE_NetBackup_Bridge_Interface> </td> </tr> </tbody> </table>	Guest Interface Alias	TVOE Bridge Name	TVOE Bridge Interface	control	control	Fill in the appropriate value (default is bond0): <TVOE_Control_Bridge_Interface>	management	management	Fill in the appropriate value: <TVOE_Management_Bridge_Interface>	xmi	xmi	Fill in the appropriate value: <TVOE_XMI_Bridge_Interface>	imi	Imi	Fill in the appropriate value: <TVOE_IMI_Bridge_Interface>	Int (iDIH Only)	Int	Fill in the appropriate value: <TVOE_INT_Bridge_Interface>	xsi1-16	xsi1-16	Fill in the appropriate value: xsi1: xsi2: xsi3: xsi4: xsi5: xsi6: xsi7: xsi8: xsi9: xsi10: xsi11: xsi12: xsi13: xsi14: xsi15: xsi16: <TVOE_XSI1-16_Bridge_Interface>	replication	replication	Fill in the appropriate value: <TVOE_REPLICATION_Bridge_Interface>	NetBackup (if applicable)	NetBackup	Fill in the appropriate value: <TVOE_NetBackup_Bridge_Interface>
Guest Interface Alias	TVOE Bridge Name	TVOE Bridge Interface																											
control	control	Fill in the appropriate value (default is bond0): <TVOE_Control_Bridge_Interface>																											
management	management	Fill in the appropriate value: <TVOE_Management_Bridge_Interface>																											
xmi	xmi	Fill in the appropriate value: <TVOE_XMI_Bridge_Interface>																											
imi	Imi	Fill in the appropriate value: <TVOE_IMI_Bridge_Interface>																											
Int (iDIH Only)	Int	Fill in the appropriate value: <TVOE_INT_Bridge_Interface>																											
xsi1-16	xsi1-16	Fill in the appropriate value: xsi1: xsi2: xsi3: xsi4: xsi5: xsi6: xsi7: xsi8: xsi9: xsi10: xsi11: xsi12: xsi13: xsi14: xsi15: xsi16: <TVOE_XSI1-16_Bridge_Interface>																											
replication	replication	Fill in the appropriate value: <TVOE_REPLICATION_Bridge_Interface>																											
NetBackup (if applicable)	NetBackup	Fill in the appropriate value: <TVOE_NetBackup_Bridge_Interface>																											

Procedure 4. First RMS Configuration

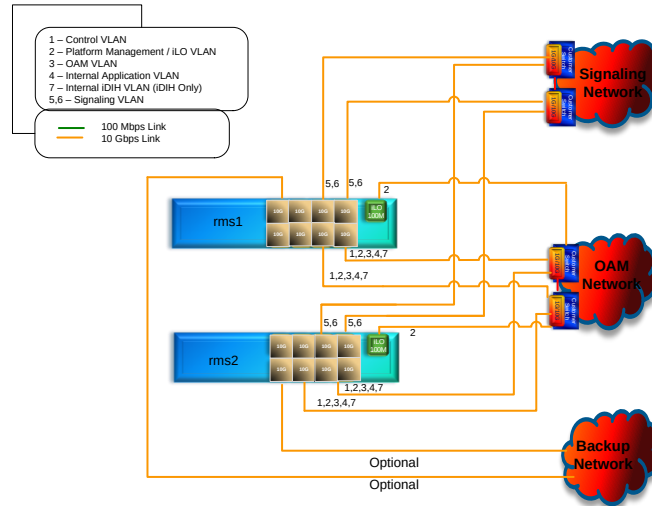
2 ☐	1st RMS iLO/iLOM: Login and Launch the Integrated Remote Console	Log in to iLO/iLOM, follow Appendix D: TVOE iLO/iLOM GUI Access for instructions on how to access the iLO/iLOM GUI. <code>https://<management_server_iLO_ip></code>
3 ☐	1st RMS iLO/iLOM: Create the Management Network	Create the Management network, execute the following command: Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure. <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Management_Bridge_Interface> --onboot=yes Interface bond0.2 added</pre> <pre>\$sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=management --bootproto=none --onboot=yes --address=<Management_Server_TVOE_IP> --netmask=<Management_Server_TVOE_Netmask/prefix> --bridgeInterfaces=<TVOE_Management_Bridge_Interface> Bridge management added!</pre>
4 ☐	1st RMS iLO/iLOM: Configure Default Route	Configure the default route by executing the following commands: <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=default --device=management --gateway=<Management_Gateway_IP_Address> Route to management added</pre>

Procedure 4. First RMS Configuration

5

**1st RMS
iLO/iLOM:
TVOE Bond1
Configuration
(Segregated
Signaling)**


If your rack mount server solution is designed where the signaling traffic is segregated from the rest of the DSR OAM related networks and located on separate NICs, execute this step. If your OAM related networks will share the same physical NICs (non-segregated), skip this step.



Create Bond1 interface:

Note: Refer to **Section 3.4** for network interface references for the configuration step below.

```
$ sudo /usr/TKLC/plat/bin/netAdm add --device=bond1 --onboot=yes
```

```
$ sudo /usr/TKLC/plat/bin/netAdm set --device=<ethernet_interface_3> --type=Ethernet --master=bond1 --slave=yes --onboot=yes
```

Expected Output:

```
/sys/class/net/bond1/bonding/primary has 0 lines, nothing to do.
```

```
Interface <ethernet_interface_3> updated
```

```
$ sudo /usr/TKLC/plat/bin/netAdm set --device=<ethernet_interface_4> --type=Ethernet --master=bond1 --slave=yes --onboot=yes
```

Expected Output:

```
/sys/class/net/bond1/bonding/primary has 0 lines, nothing to do.
```

```
Interface <ethernet_interface_4> updated
```

Procedure 4. First RMS Configuration

6 ☐	1st RMS iLO/iLOM: Set Ethernet Interface Ring Buffer Sizes	The following commands will increase the ring buffer sizes on Ethernet Interfaces: Note: Refer to Section 3.4 for network interface server reference table <pre> \$ sudo netAdm set --device=<ethernet_interface_1> -- ringBufferRx=4096 --ringBufferTx=4096 \$ sudo netAdm set --device=<ethernet_interface_2> -- ringBufferRx=4096 --ringBufferTx=4096 If step 5 was executed, execute the following commands: \$ sudo netAdm set --device=<ethernet_interface_3> -- ringBufferRx=4096 --ringBufferTx=4096 \$ sudo netAdm set --device=<ethernet_interface_4> -- ringBufferRx=4096 --ringBufferTx=4096 </pre>

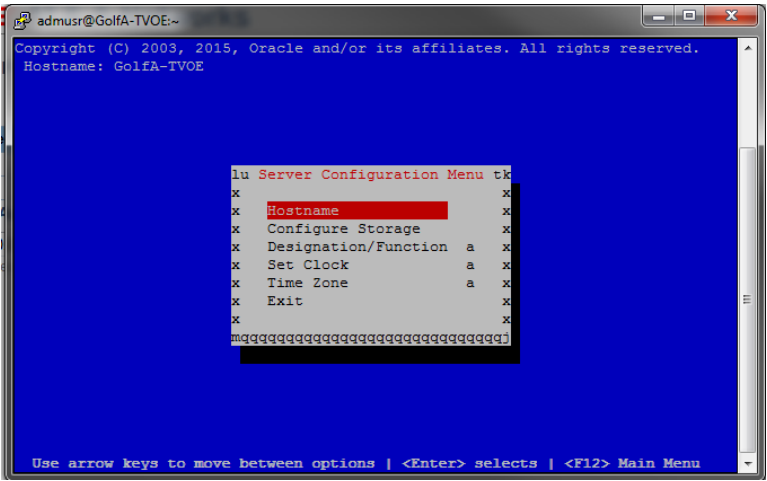
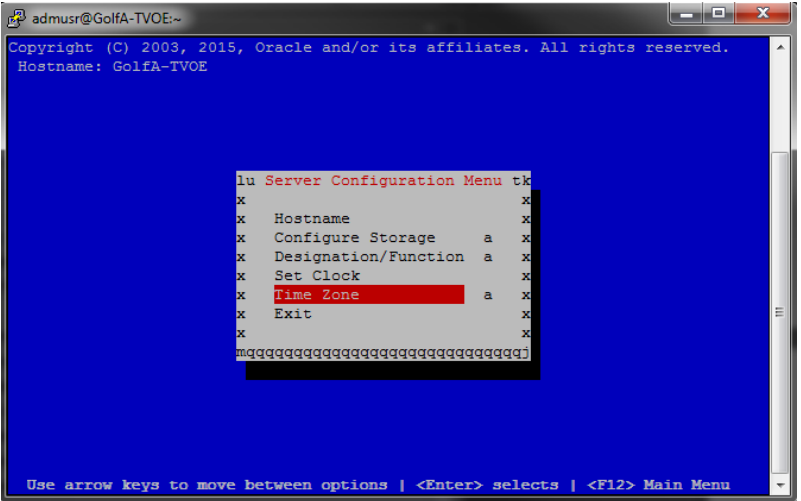
Procedure 4. First RMS Configuration

7 ☐	1st RMS iLO/iLOM: Add the NetBackup Network-Option 1 (Optional)	If NetBackup is to be used, execute this step, otherwise skip to Step 12. Select only this option or the following options listed in steps 8 or 9. NetBackup is a tool that allows the customer to take remote backups of the system. Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured. Note: The example below illustrates a TVOE Management Server configuration with the NetBackup feature enabled. The NetBackup network is configured with a non-default MTU size. Note: The MTU size must be consistent between a network bridge, device, or bond, and associated VLANs. Create NetBackup bridge using a bond containing an untagged interface <pre> \$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_NetBackup_Bridge_Interface> --onboot=yes --type=Bonding --mode=active-backup -- miimon=100 --MTU=<NetBackup_MTU_size> Interface <TVOE_NetBackup_Bridge_Interface> added \$ sudo /usr/TKLC/plat/bin/netAdm set --device=<ethernet_interface_4> --type=Ethernet --master=<TVOE_NetBackup_Bridge_Interface> --slave=yes --onboot=yes Interface <ethernet_interface_4> updated \$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge> --onboot=yes -- bootproto=none --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface> --address=<TVOE_NetBackup_IP> --netmask=<TVOE_NetBackup_Netmask/Prefix> </pre>
8 ☐	1st RMS iLO/iLOM: Add the NetBackup Network-Option 2 (Optional)	If NetBackup is to be used, Select only this option or options in Steps 7 or 9 Create NetBackup bridge using an untagged native interface: <pre> \$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge> --onboot=yes -- bootproto=none --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<Ethernet_Interface_4> --address=<TVOE_NetBackup_IP> --netmask=<TVOE_NetBackup_Netmask/Prefix> </pre>

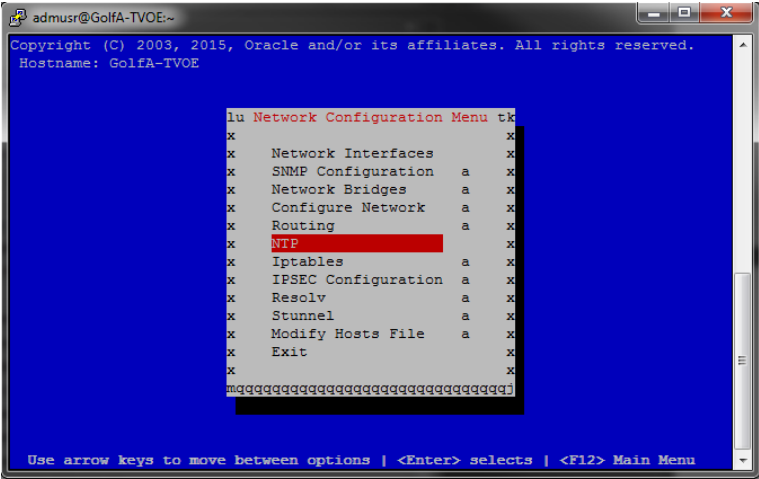
Procedure 4. First RMS Configuration

9 ☐	1st RMS iLO/iLOM: Add the NetBackup Network-Option 3 (Optional)	If NetBackup is to be used, Select only this option or options in 7 or 8 Create NetBackup bridge using a tagged device: <pre> \$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_NetBackup_Bridge_Interface> --onboot=yes Interface <TVOE_NetBackup_Bridge_Interface> added \$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge> --onboot=yes --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface> --address=<TVOE_NetBackup_IP> --netmask=<TVOE_NetBackup_Netmask/Prefix> </pre>
10 ☐	1st RMS iLO/iLOM: Configure Networking for NetBackup Interface (Optional)	Note: If you have configured NetBackup in the previous steps, execute this step; otherwise skip this step. <pre> \$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=NetBackup --address=<TVOE_NetBackup_Network_ID> --netmask=<TVOE_NetBackup_NetMask/Prefix> --gateway=<TVOE_NetBackup_Gateway_IP_Address> </pre>
11 ☐	1st RMS iLO/iLOM: Restart the network interfaces	Restart the network interfaces, execute the following command: <pre> \$ sudo service network restart </pre>

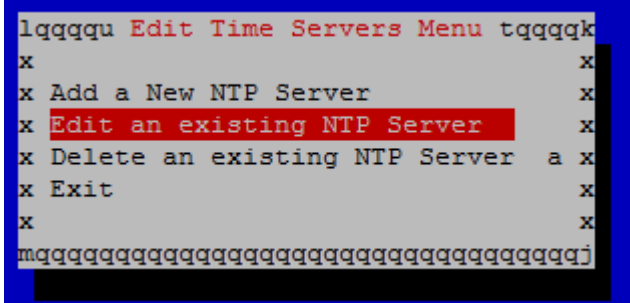
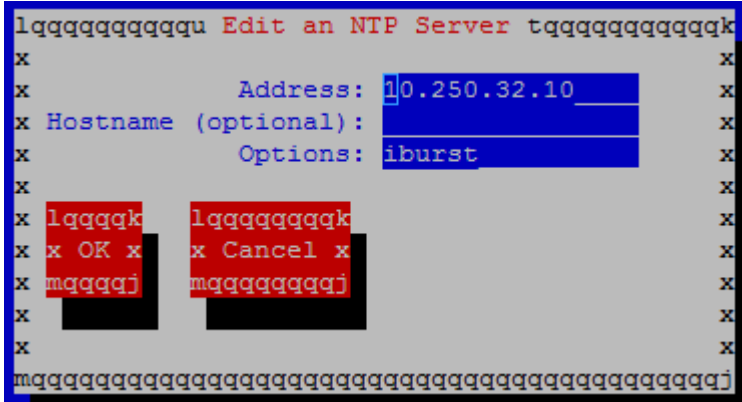
Procedure 4. First RMS Configuration

12 ☐	1st RMS iLO/iLOM: Set Hostname	Set the server hostname by running the following: <pre>\$ sudo su - platcfg</pre> Navigate to Server Configuration -> Hostname ->Edit.  Set TVOE Management Server hostname Press OK. Navigate out of Hostname
13 ☐	1st RMS iLO/iLOM: Set the Time Zone and/or Hardware Clock	Navigate to Server Configuration -> Time Zone.  Select Edit. Set the time zone and/or hardware clock to "UTC" (or appropriate time zone value) Press OK. Navigate out of Server Configuration

Procedure 4. First RMS Configuration

14	RMS iLO/iLOM: Configure NTP	Navigate to Network Configuration ->NTP. 

Procedure 4. First RMS Configuration

15 ☐	TVOE Server: Configure NTP – Edit an NTP Server.	1. Edit NTP Server. The NTP Server to edit Menu window is displayed.  2. Select appropriate NTP server & Edit the details  3. Enter Appropriate data, and select OK Exit platcfg.

Procedure 4. First RMS Configuration

16

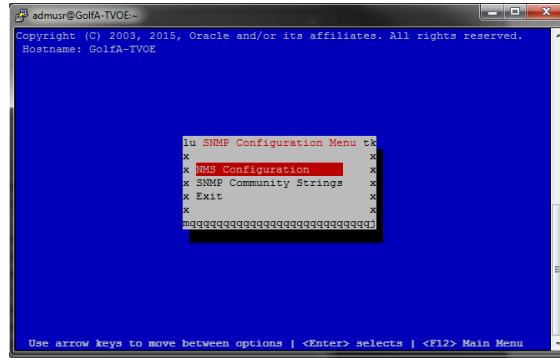
**1st RMS
iLO/iLOM:
Set SNMP**

Set SNMP by running the following:

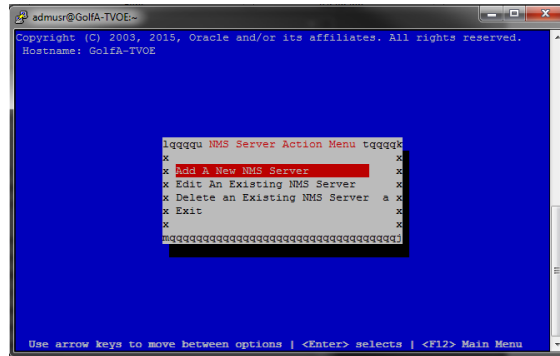
```
$ sudo su - platcfg
```

Note: Refer **Appendix H: SNMP Configuration** to understand the preferred SNMP configuration

Navigate to **Network Configuration -> SNMP Configuration -> NMS Configuration**.

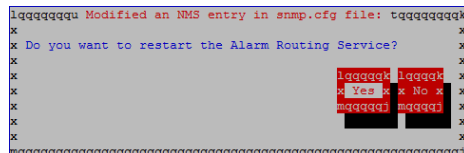


Select **Edit** and then choose **Add a New NMS Server**. The **Add an NMS Server** page will be displayed.



Complete the form by entering NMS server IP, Port (*default port is 162*) and community string provided by the customer about the SNMP trap destination.

Select **OK** to finalize the configuration. The **NMS Server Action Menu** will now be displayed. Select **Exit**. The following dialogue will then be presented.



Select **Yes** and then wait a few seconds while the Alarm Routing Service is restarted. At that time the **SNMP Configuration** menu will be presented.

Exit platcfg.

Procedure 4. First RMS Configuration

17 ☐	1st RMS iLO/iLOM: Restart	Execute the following command to restart the server: <code>\$ sudo init 6</code>
18 ☐	1st RMS iLO/iLOM: Verify Ring Buffer Settings	Verify the ring buffer sizes have been configured correctly (from Step 6) by executing the following command for each Ethernet interface configured above: <code>\$ ethtool -g <eth interfaces configured above></code> Example shown below: [admsr@FJ-TVOE-2 ~]\$ ethtool -g eth01 Ring parameters for eth01: Pre-set maximums: RX: 4096 RX Mini: 0 RX Jumbo: 0 TX: 4096 Current hardware settings: RX: 4096 RX Mini: 0 RX Jumbo: 0 TX: 4096

Procedure 4. First RMS Configuration

19 ☐	1st RMS iLO/iLOM: Configure NetBackup-Part 1 (Optional)	Execute this step if the NetBackup feature is enabled for this system, otherwise skip this step. Configure the appropriate NetBackup client on the PMAC TVOE host. Open firewall ports for NetBackup using the following commands: <pre>\$ sudo ln -s /usr/TKLC/plat/share/NetBackup/60NetBackup.ipt /usr/TKLC/plat/etc/iptables/</pre> <pre>\$ sudo /usr/TKLC/plat/bin/iptablesAdm reconfig</pre> Enable platcfg to show the NetBackup Menu Items by executing the following commands: <pre>\$ sudo platcfgadm --show NBConfig; \$ sudo platcfgadm --show NBInit; \$ sudo platcfgadm --show NBDeInit; \$ sudo platcfgadm --show NBInstall; \$ sudo platcfgadm --show NBVerifyEnv; \$ sudo platcfgadm --show NBVerify;</pre> Create LV and file system for NetBackup client software on the vgguests volume group: <pre>\$sudo /usr/TKLC/plat/sbin/storageMgr /tmp/nb.lvm</pre> This will create the LV, format it with a filesystem, and mount it under /usr/opencv/. Example output is shown below: <pre>Called with options: /tmp/nb.lvm VG vgguests already exists. Creating lv NetBackup_lv. Volume NetBackup_lv will be created. Success: Volume NetBackup_lv was created. Creating filesystem, this may take a while. Updating fstab for lv NetBackup_lv. Configuring existing lv NetBackup_lv. The LV for NetBackup has been created!</pre>

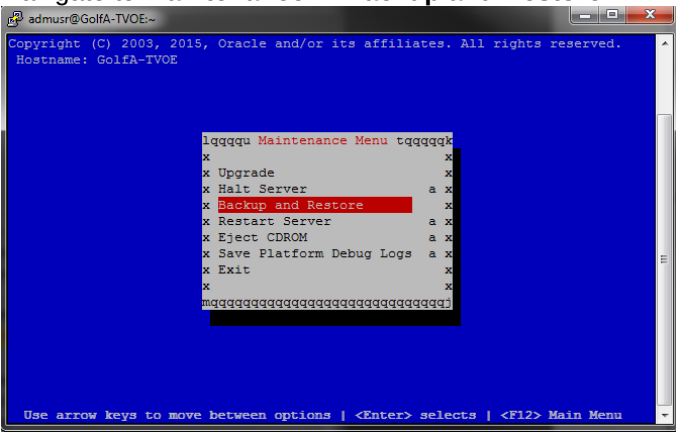
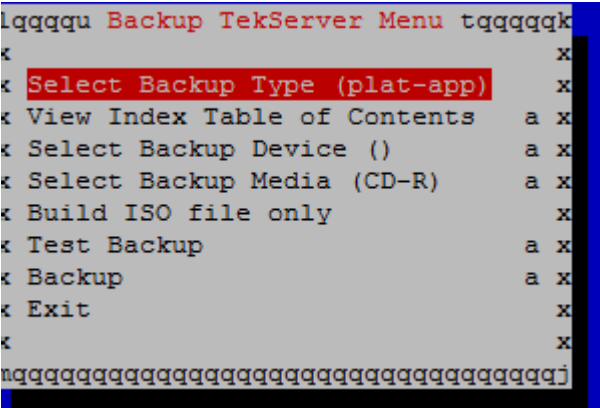
Procedure 4. First RMS Configuration

20 ☐	1st RMS iLO/iLOM: Configure NetBackup-Part 2 (Optional)	Install the NetBackup client software: Refer to Appendix I: Application NetBackup Client Installation Procedures for instructions how to install the NetBackup client. Note: Skip any steps relating to copying NetBackup "notify" scripts to /usr/opensv/NetBackup/bin. The TVOE NetBackup notify scripts are taken care of in the next step. Create soft links for TVOE specific NetBackup notify scripts. <pre>\$sudo ln -s /usr/TKLC/plat/sbin/bpstart_notify /usr/opensv/NetBackup/bin/bpstart_notify</pre> <pre>\$sudo ln -s /usr/TKLC/plat/sbin/bpend_notify /usr/opensv/NetBackup/bin/bpend_notify</pre> Note: Once the NetBackup Client is installed on TVOE, the NetBackup Master should be configured to back up the following files from the TVOE host: • /var/TKLC/bkp/*.iso
21 ☐	1st RMS iLO/iLOM: Setup syscheck	'syscheck' must be configured to monitor bonded interfaces. Replace "bondedInterfaces" with "bond0" or "bond0,bond1" if segregated networks are used: <pre>\$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES --val=<bondedInterfaces></pre> <pre>\$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --enable</pre>
22 ☐	1st RMS iLO/iLOM: Verify syscheck	Verify syscheck: <pre>\$ sudo /usr/TKLC/plat/bin/syscheck net ipbond -v</pre> Expected output should look similar to below: <pre>Running modules in class net... ipbond: Bonded interface bond0 is OK OK</pre> LOG LOCATION: /var/TKLC/log/syscheck/fail log

Procedure 4. First RMS Configuration

23 ☐	1st RMS iLO/iLOM: Verify Server Health	Execute the following: <pre>\$ alarmMgr --alarmStatus</pre> This command should return no output on a healthy system. If any alarms are reported, contact Appendix U: My Oracle Support (MOS)

Procedure 4. First RMS Configuration

24 ☐	1st RMS iLO/iLOM: Perform a TVOE backup using TPD platcfg utility	Execute the following: <pre>\$ sudo su - platcfg</pre> Navigate to Maintenance -> Backup and Restore  Select Backup Platform (CD/DVD) Note: If no cdrom device is found by TPD, you will receive an error dialog with the message: "No disk device available. This is normal on systems without a cdrom device." Press Enter to continue. Select Build ISO file only, and press Enter to continue. Exit from TPD platcfg utility.  The TVOE backup can be found in the "/var/TKLC/bkp/" directory, and is prefixed by the server hostname. An example of a TVOE backup ISO follows: /var/TKLC/bkp/RMS503u14-plat-app-201210301505.iso Move the TVOE backup to a customer provided backup server for safe keeping.

4.3 Install PMAC

Note: [Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only]: Follow procedure **Appendix Q.2: Non-HA Lab Node PMAC Deployment** instead of procedure 5 for PMAC deployment.

Procedure 5. PMAC Deployment

S T E P #	This procedure will deploy PMAC on the TVOE Host Prerequisite: First RMS Network Configuration (PMAC Host) has been completed. Needed material: - PMAC Media on USB Drive or ISO Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PMAC's TVOE iLO/iLOM: Login and Launch the Integrated Remote Console Log in to iLO/iLOM; follow Appendix D: TVOE iLO/iLOM GUI Access for instructions on how to access the iLO/iLOM GUI. <code>https://<management_server_iLO_ip></code>

Procedure 5. PMAC Deployment

2 ☐	PMAC's TVOE iLO/iLOM: Mount the PMAC Media to the TVOE Server	Use one of the following 2 options to mount the PMAC Media: <u>Option 1:</u> If using a USB media, insert the PMAC USB into a USB port and execute the following to mount the ISO: <pre>\$ ls /media/*/*.iso /media/sddl/872-2586-101-6.2.0_62.17.0-PM&C-x86_64.iso</pre> Use the output of the previous command to populate the next command <pre>\$ sudo mount -o loop /media/sddl/872-2586-101-6.2.0_62.17.0-PM&C-x86_64.iso /mnt/upgrade</pre> <u>Option 2:</u> If using an ISO image, run the following to mount it: <pre>\$ sudo mount -o loop ISO_FILENAME.iso /mnt/upgrade</pre> Next Validate the PMAC media by executing the following commands: <pre>\$ cd /mnt/upgrade/upgrade \$.validate/validate_cd</pre> <pre>Validating cdrom... UMVT Validate Utility v2.2.2, (c)Tekelec, June 2012 Validating <device or ISO> Date&Time: 2012-10-25 10:07:01 Volume ID: tklc_872-2441-106_Rev_A_62.17.0 Part Number: 872-2441-106_Rev_A Version: 62.17.0 Disc Label: PM&C Disc description: PM&C The media validation is complete, the result is: PASS CDROM is Valid</pre> Note: If the media validation fails, the media is not valid and should not be used.

Procedure 5. PMAC Deployment

3 ☐	PMAC's TVOE iLO/iLOM: Deploy PMAC	Using the pmac-deploy script, deploy the PMAC instance using the configuration captured during the site survey. <pre>\$ cd /mnt/upgrade/upgrade</pre> If deploying PMAC without NetBackup feature, run the following command: <pre>\$ sudo ./pmac-deploy --guest=<PMAC_Name> --hostname=<PMAC_Name> --controlBridge=<TVOE_Control_Bridge> --controlIP=<PMAC_Control_ip_address> --controlNM=<PMAC_Control_netmask> --managementBridge=<PMAC_Management_Bridge> --managementIP=<PMAC_Management_ip_address> --managementNM=<PMAC_Management_netmask/prefix> --routeGW=<PMAC_Management_gateway_address> --ntpserver=<TVOE_Management_server_ip_address> --isoimagesVolSizeGB=20</pre> If deploying PMAC with NetBackup feature, run the following command: <pre>\$ sudo ./pmac-deploy --guest=<PMAC_Name> --hostname=<PMAC_Name> --controlBridge=<TVOE_Control_Bridge> --controlIP=<PMAC_Control_ip_address> --controlNM=<PMAC_Control_netmask> --managementBridge=<PMAC_Management_Bridge> --managementIP=<PMAC_Management_ip_address> --managementNM=<PMAC_Management_netmask/prefix> --routeGW=<PMAC_Management_gateway_address> --ntpserver=<TVOE_Management_server_ip_address> --NetBackupVol --bridge=<TVOE_NetBackup_Bridge> --nic=NetBackup --isoimagesVolSizeGB=20</pre> The PMAC will deploy and boot. The management and control network will come up based on the settings that were provided to the pmac-deploy script. Note: This step takes between 5 and 10 minutes.
4 ☐	PMAC's TVOE iLO/iLOM: Unmount the Media	The media should auto-unmount, if it does not, unmount the media using the following command: <pre>\$ cd / \$ sudo /bin/umount /mnt/upgrade</pre> Remove the media from the drive.

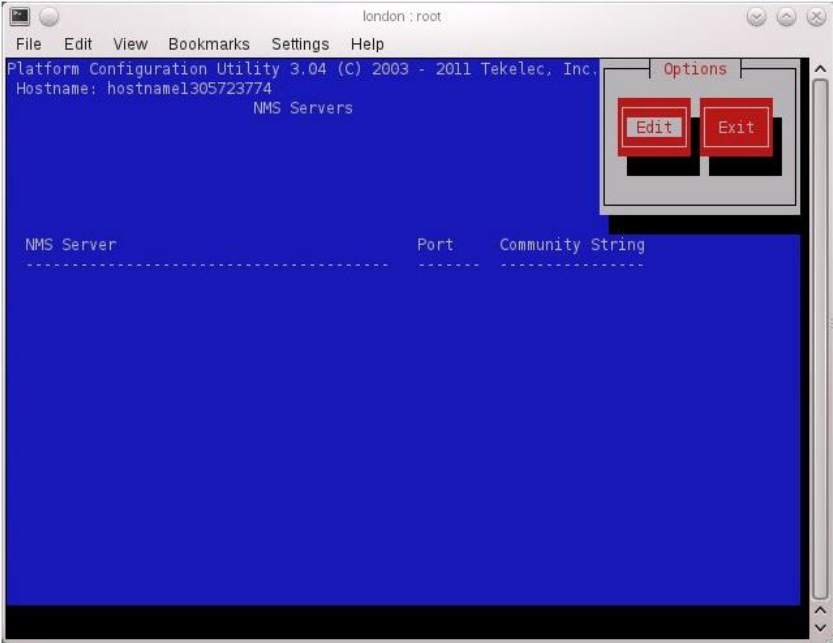
Procedure 5. PMAC Deployment

5 ☐	PMAC's TVOE iLO/iLOM: SSH into the Management Server	Using an SSH client such as putty, ssh to the TVOE host as admusr. Login using virsh, and wait until you see the login prompt : <pre>\$ sudo /usr/bin/virsh list</pre> <pre>Id Name State ----- 2 PM&C running</pre> <pre>\$ sudo /usr/bin/virsh console <PM&C></pre> [Output Removed] <pre>Starting ntdMgr: [OK] Starting atd: [OK] 'TPD Up' notification(s) already sent: [OK] upstart: Starting tpdProvd... upstart: tpdProvd started. CentOS release 6.2 (Final) Kernel 2.6.32-220.17.1.el6prere16.0.0_80.14.0.x86_64 on an x86_64 PM&Cdev7 login:</pre>
6 ☐	Virtual PMAC: Verify the PMAC is configured correctly on first boot	Establish an SSH session to the PMAC, login as admusr. Run the following command (there should be no output): <pre>\$ sudo /bin/ls /usr/TKLC/plat/etc/deployment.d/</pre>
7 ☐	PMAC's TVOE iLO/iLOM: Error doing verification, if error is outputted	If an error was made use the following command to delete the PMAC Guest and then re-deploy the guest again: <pre>\$ sudo guestMgr --remove <PMAC_Name></pre>

Procedure 5. PMAC Deployment

8 ☐	Virtual PMAC: Set the PMAC time zone	Determine the Time Zone to be used for the PMAC Note: Valid time zones can be found in Appendix J: List of Frequently used Time Zones Run <pre>\$ sudo set_pmac_tz.pl <time zone></pre> Example: <pre>\$ sudo set_pmac_tz.pl America/New_York</pre> Verify that the time zone has been updated: <pre>\$ sudo date</pre>

Procedure 5. PMAC Deployment

9 ☐	Virtual PMAC: Set SNMP	Set SNMP by running the following: <pre>\$ sudo su - platcfg</pre> Navigate to Network Configuration -> SNMP Configuration -> NMS Configuration.  Select Edit and then choose Add a New NMS Server. The 'Add an NMS Server' page will be displayed. Complete the form by entering in all information about the SNMP trap destination. Select OK to finalize the configuration. The 'NMS Server Action Menu' will now be displayed. Select Exit. The following dialogue will then be presented. Note: Refer to Appendix H: SNMP Configuration for SNMP Configuration information. Select Yes and then wait a few seconds while the Alarm Routing Service is restarted. At that time the SNMP Configuration Menu will be presented. Exit platcfg.
10 ☐	Virtual PMAC: Reboot the server	Reboot the server by running: <pre>\$ sudo init 6</pre>

4.4 Initialize the PMAC Application

Procedure 6. Initialize the PMAC

S T E P #	Use this procedure to gather and prepare configuration files that are required to proceed with the DSR installation. Needed material: - DSR USB or ISO Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PMAC's TVOE iLO/iLOM: SSH into the Management Server Using an SSH client such as putty, ssh to the TVOE host as admusr. Login using virsh, and wait until you see the login prompt : <pre>\$ sudo /usr/bin/virsh list Id Name State ----- 1 PM&C running</pre> <pre>\$ sudo /usr/bin/virsh console <PM&C> [Output Removed] Starting ntdMgr: [OK] Starting atd: [OK] 'TPD Up' notification(s) already sent: [OK] upstart: Starting tpdProvd... upstart: tpdProvd started. CentOS release 6.2 (Final) Kernel 2.6.32-220.17.1.el6prere16.0.0_80.14.0.x86_64 on an x86_64 PM&Cdev7 login:</pre>

Procedure 6. Initialize the PMAC

2 ☐	Virtual PMAC: Initialize the PMAC Application	Initialize the PMAC Application; run the following commands: <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm applyProfile -- fileName=TVOE</pre> Profile successfully applied. <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm getPmacFeatureState</pre> PMAC Feature State = InProgress <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm finishProfileConfig</pre> Initialization has been started as a background task
3 ☐	Virtual PMAC: Initialize the PMAC Application Note: Initialization typically takes about 1 minute.	Wait for the background task to successfully complete. The command will show "IN_PROGRESS" for a short time. Run the following command until a "COMPLETE" or "FAILED" response is seen similar to the following: <pre>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</pre> <pre>1: Initialize PMAC COMPLETE - PMAC initialized Step 2: of 2 Started: 2012-07-13 08:23:55 running: 29 sinceUpdate: 47 taskRecordNum: 2 Server Identity: Physical Blade Location: Blade Enclosure: Blade Enclosure Bay: Guest VM Location: Host IP: Guest Name: TPD IP: Rack Mount Server: IP: Name:</pre> Note: Some expected networking alarms may be present

Procedure 6. Initialize the PMAC

4 ☐	Virtual PMAC: Initialize the PMAC Application	Perform a system health check on the PMAC \$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus This command should return no output on a healthy system. Note: An NTP alarm will be detected if the system switches are not configured \$ sudo /usr/TKLC/smac/bin/sentry status 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.
5 ☐	Virtual PMAC: Verify the PMAC application release	Verify the PMAC application release Verify that the PMAC application Product Release is as expected. Note: If the PMAC application Product Release is not as expected, STOP and contact Appendix U: My Oracle Support (MOS) \$ sudo /usr/TKLC/plat/bin/appRev Install Time: Fri Sep 28 15:54:04 2012 Product Name: PM&C Product Release: 5.0.0_50.10.0 Part Number ISO: 872-2441-905 Part Number USB: 872-2441-105 Base Distro Product: TPD Base Distro Release: 6.0.0_80.22.0 Base Distro ISO: TPD.install-
6 ☐	Virtual PMAC: Logout of the PMAC	Logout of the virsh console Hold ctrl] to logout of the PMAC
7 ☐	Note	If configuring a system with Aggregation switches (<i>HP DL380 Gen 8 Only</i>), continue to procedure 7 . If configuring a system without aggregation switches (<i>Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9</i>), skip to procedure 9 .

4.5 Configure Cisco 4948E-F Aggregation Switches (HP DL380 Gen 8 Servers Only)

4.5.1 Configure netConfig Repository (HP DL380 Gen 8 Servers Only)

This procedure will configure the netConfig repository for all required services and for each switch to be configured. At any time, you can view the contents of the netConfig repository by using one of the following commands:

For switches, use the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices
```

For services, use the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo listServices
```

Users returning to this procedure after initial installation should run the above commands and note any devices and/or services that have already been configured. Duplicate entries cannot be added; if changes to a device repository entry are required, use the editDevice command. If changes to a services repository entry are necessary, you must delete the original entry first and then add the service again.

IPv4 and IPv6

Configuration support using IPv4 or IPv6 addresses through netConfig. Wherever IP addresses are required for networking procedures in **Section 3.1**, IPv4 or IPv6 may be used. Commands such as ping or ssh may also be used in these procedures, where for IPv6 cases may need to be "ping6" or "ssh -6" as needed.

Terminology

The term 'netConfig server' refers to the entity where netConfig is executed. This may be a virtualized or physical environment. 'Management server' may also accurately describe this location but has been historically used to describe the physical environment while 'Virtual PMAC' was used to describe the virtualized netConfig server. Use of the term 'netConfig server' to describe dual scenarios of physical and virtualized environments will allow for future simplification of network configuration procedures.

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within "<>". Fill these worksheets out based on NAPD, and then refer back to these tables for the proper value to insert depending on your system type.

Variable	Value
<management_server_iLO_ip>	
<management_server_mgmt_ip_address>	
<netConfig_server_mgmt_ip_address>	
<switch_backup_user>	admusr
<switch_backup_user_password>	
<serial console type>	u=USB, c=PCIe

For the first aggregation switch (4948, 4948E, or 4948E-F): Fill in the appropriate value for this site.

Variable	Value
<switch_hostname>	
<device_model>	
<console_name>	
<switch_console_password>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<switch_mgmt_ip_address>	
<switch_mgmt_netmask>	
<mgmt_vlanID>	
<control_vlanID>	
<IOS_filename>	
<ip_version>	

For the second aggregation switch (4948, 4948E, or 4948E-F): Fill in the appropriate value for this site.

Variable	Value
<switch_hostname>	
<device_model>	
<console_name>	
<switch_console_password>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<switch_mgmt_ip_address>	
<switch_mgmt_netmask>	
<mgmt_vlanID>	
<control_vlanID>	
<IOS_filename>	
<ip_version>	

Procedure 7. Configure netConfig Repository (HP DL380 Gen 8 Servers Only)

S T E P #	This procedure will configure 4948E-4948E-F switches with an appropriate IOS and configuration specified by Platform Engineering and Application requirements. Prerequisite: This procedure assumes a recently IPM'ed TVOE server with a VM hosting the PMAC application. Needed material: - HP Misc. Firmware USB - HP Solutions Firmware Upgrade Pack, Software Centric Release Notes (Min 2.2.9) [1] - DSR USB or ISO Note: Uplinks must be disconnected from the customer network prior to executing this procedure. One of the steps in this procedure will instruct when to reconnect these uplink cables. Note: The generic XML configuration file referenced in this procedure needs to be updated to match the customer's network. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	1st RMS iLO/iLOM: Login and Launch the Integrated Remote Console Log in to iLO/iLOM; follow Appendix D: TVOE iLO/iLOM GUI Access for instructions on how to access the iLO/iLOM GUI. https://<management_server_iLO_ip> Login as admusr.

Procedure 7. Configure netConfig Repository (HP DL380 Gen 8 Servers Only)

2 ☐	1st RMS iLO/iLOM: Mount Firmware Image	Insert the Misc. Firmware USB media into the USB drive. For this step, be sure to use the correct IOS version specified by the HP Solutions Firmware Upgrade Pack, Software Centric Release Notes (Min 2.2.9) [1] Copy each ISO image called out by the release notes. SSH to the TVOE Host server as admusr using the vsp/Host Console on the TVOE Management Server iLO/iLOM. Make the upgrade media available to the server. Execute the following commands to copy the required files. Note: The <PMAC Management_IP Address> is the one used to deploy PMAC in procedure 5, step 3. Mount the media on the TVOE Host using one of the following commands: If using a USB Drive, run the following to mount it: <pre>\$ sudo /bin/ls /media/*/*.iso</pre> Use the output of the previous command to populate the next command <pre>\$ sudo /bin/mount -o loop /media/sdb1/ <MISC file name> /mnt/upgrade</pre> If the DSR is on an ISO, mount it using the following commands <pre>\$ sudo /bin/mount -o loop <path to DSR ISO> /mnt/upgrade</pre>

Procedure 7. Configure netConfig Repository (HP DL380 Gen 8 Servers Only)

3 ☐	TVOE iLO/iLO: SSH into the Management Server	Using an SSH client such as putty, ssh to the TVOE host as admusr. Login using virsh, and wait until you see the login prompt : <pre>\$ sudo /usr/bin/virsh list</pre> <pre>Id Name State ----- 1 PM&C running</pre> <pre>\$ sudo /usr/bin/virsh console <PM&C></pre> [Output Removed] <pre>Starting ntdMgr: [OK] Starting atd: [OK] 'TPD Up' notification(s) already sent: [OK] upstart: Starting tpdProvd... upstart: tpdProvd started. CentOS release 6.2 (Final) Kernel 2.6.32-220.17.1.el6prere16.0.0_80.14.0.x86_64 on an x86_64 PM&Cdev7 login:</pre>
4 ☐	Virtual PMAC: Copy ISO images into place (this will copy both the 4948E IOS images into place).	<pre>\$ sudo /usr/bin/scp -r admusr@<TVOE_management_ip_address>:/mnt/upgrade/<4948E_ISO_image_filename> /var/TKLC/smac/image/</pre> Logout of PMAC and Re-login to TVOE Host and unmount the ISO Hold ctrl] to logout of the PMAC <pre>\$ sudo umount /mnt/upgrade</pre> Remove the Misc. Firmware media from the drive

Procedure 7. Configure netConfig Repository (HP DL380 Gen 8 Servers Only)

5 ☐	Virtual PMAC: Setup netConfig Repository	Use netConfig to create a repository entry that will use the ssh service. This command will provide the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> shown as the answer must be entered EXACTLY as they are shown here: <pre> \$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=ssh_service Service type? (tftp, ssh, conserver, oa) ssh Service host? <netConfig_server_mgmt_ip_address> Enter an option name <q to cancel>: user Enter the value for user: <switch_backup_user> Enter an option name <q to cancel>: password Enter the value for password: <switch_backup_user_password> Verify Password: <switch_backup_user_password> Enter an option name <q to cancel>: q Add service for ssh_service successful </pre> To ensure that you entered the information correctly, use the following command and inspect the output, which will be similar to the one shown below. <pre> \$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=ssh_service Service Name: ssh_service Type: ssh Host: 10.250.8.4 Options: password: C20F7D639AE7E7 user: admusr </pre>
6 ☐	Virtual PMAC: Configure TFTP service	Use netConfig to create a repository entry that will use the TFTP service. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here. <pre> \$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=tftp_service Service type? (tftp, ssh, conserver, oa) tftp Service host? <netConfig_server_mgmt_ip_address> Enter an option name (q to cancel): dir Enter a value for user dir: /var/TKLC/smac/image/ Enter an option name(q to cancel): q Add service for tftp_service successful </pre>

Procedure 7. Configure netConfig Repository (HP DL380 Gen 8 Servers Only)

7 ☐	Virtual PMAC: Run conserver Setup	Execute the following command to run the conserverSetup: <pre>\$ sudo /usr/TKLC/plat/bin/conserverSetup -<serial console type> -s <management_server_mgmt_ip_address></pre> You will be prompted for the platcfg credentials. An example: <pre>[admusr@vm-pmac1A]\$ sudo /usr/TKLC/plat/bin/conserverSetup -u -s <management_server_mgmt_ip_address></pre> Enter your platcfg username, followed by [ENTER]:platcfg Enter your platcfg password, followed by [ENTER]:<platcfg_password> Checking Platform Revision for local TPD installation... The local machine is running: Product Name: PMAC Base Distro Release: 7.0.0.0.0_86.1.0 Checking Platform Revision for remote TPD installation... The remote machine is running: Product Name: TVOE Base Distro Release: 7.0.0.0.0_86.2.0 Configuring switch 'switch1A_console' console server...Configured. Configuring switch 'switchBA_console' console server...Configured. Configuring iptables for port(s) 782...Configured. Configuring iptables for port(s) 1024:65535...Configured. Configuring console repository service... Repo entry for "console_service" already exists; deleting entry for: Service Name: console_service Type: conserver Host: <management_server_mgmt_ip_address> ...Configured. Slave interfaces for bond0: bond0 interface: eth01 bond0 interface: eth02
8 ☐	Virtual PMAC: Copy the Cisco Firmware to the TFTP Directory	Copy the FW identified by <FW_image> in the aggregation switch variable table <pre>\$ sudo /bin/cp /mnt/upgrade/files/<FW_image> /var/TKLC/smac/image</pre> <pre>\$ sudo /bin/chmod 644 /var/TKLC/smac/image/<FW_image></pre>

Procedure 7. Configure netConfig Repository (HP DL380 Gen 8 Servers Only)

9 ☐	Virtual PMAC: Setup the netConfig Repository with Aggregation Switch Information	Use netConfig to create a repository entry for each switch. The initial command will prompt the user multiple times. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here. Note: The <device_model> can be 4948, 4948E, or 4948E-F depending on the model of the device. If you do not know, stop now and contact Appendix U: My Oracle Support (MOS) <pre> sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials Device Vendor? Cisco Device Model? <device_model> What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <switch_mgmt_ip_address><mask> Is the management interface a port or a vlan? [vlan]: [Enter] What is the VLAN ID of the management VLAN? [2]: [mgmt_vlanID] What is the name of the management VLAN? [management]: [Enter] What switchport connects to the management server? [GE40]: [Enter] What is the switchport mode (access trunk) for the management server port? [trunk]: [Enter] What are the allowed vlans for the management server port? [1,2]: <control_vlanID>, <mgmt_vlanID> Enter the name of the firmware file [cat4500e-entservicesk9-mz.122- 54.XO.bin]: <IOS_filename> Firmware file to be used in upgrade: <IOS_filename> Enter the name of the upgrade file transfer service: tftp_service File transfer service to be used in upgrade: tftp_service Should the init oob adapter be added (y/n)? y Adding consoleInit protocol for <switch_hostname> using oob... What is the name of the service used for OOB access? console_service What is the name of the console for OOB access? <console name> What is the platform access username? <switch_platform_username> What is the device console password? <switch_console_password> UG006482 Revision B, April 2015 70 Software Installation Procedures Verify password: <switch_console_password> What is the platform user password? <switch_platform_password> Verify password: <switch_platform_password> What is the device privileged mode password? <switch_enable_password> Verify password: <switch_enable_password> Should the live network adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using network... Network device access already set: <switch_mgmt_ip_address> Should the live oob adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using oob... OOB device access already set: console_service Device named <switch_hostname> successfully added. </pre>

Procedure 7. Configure netConfig Repository (HP DL380 Gen 8 Servers Only)

10 ☐	Virtual PMAC: Verification	To check that you entered the information correctly, use the following command: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname></pre> The output should be similar to the one shown: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname> Device: <switch_hostname> Vendor: Cisco Model: <device_model> FW Ver: 0 FW Filename: <IOS_image> FW Service: tftp_service Initialization Management Options mgmtIP: <switch_mgmt_ip_address> mgmtInt: vlan mgmtVlan: <mgmt_vlanID> mgmtVlanName: management interface: GE40 mode: trunk allowedVlans: <control_vlanID>, <mgmt_vlanID> Access: Network: <switch_mgmt_ip_address> Access: OOB: Service: console_service Console: <console_name> Init Protocol Configured Live Protocol Configured</pre>
11 ☐	Virtual PMAC: Repeat For Second 4948.	Repeat Steps 9-10 for the second Cisco 4948.

4.5.2 Configure Cisco 4948E-F Aggregation Switches (HP DL380 Gen 8 Servers Only)

This procedure will configure the 4948E-F switches with the appropriate IOS and configuration from a single management server and virtual PMAC.

Procedure Reference Tables:

Steps within this procedure may refer to variable data indicated by text within "<>". Refer to this table for the proper value to insert depending on your system type.

Variable	Value
<switch_platform_username>	
<switch_platform_password>	
<switch_console_password>	
<switch_enable_password>	
<management_server_mgmt_ip_address>	
<pmac_mgmt_ip_address>	
<switch_mgmtVLAN_id>	
<switch1A_mgmtVLAN_ip_address>	
<switch_mgmt_netmask>	
<mgmt Vlan_subnet id>	
<netmask>	
<switch1B_mgmtVLAN_ip_address>	
<switch_Internal_VLANS_list>	
<management_server_mgmtInterface>	
<management_server_iLO_ip>	
<customer_supplied_ntp_server_address>	

Variable	Value
<platcfg_password>	Initial password as provided by Oracle
<management_server_mgmtInterface>	Value gathered from NAPD
<switch_backup_user>	admusr
<switch_backup_user_password>	

Procedure 8. Configure Cisco 4948E-F Aggregation Switches-netConfig (HP DL 380 Servers Only)

S T E P #	This procedure will configure the 4948E-F switches with the appropriate IOS and configuration from a single management server and virtual PMAC. Needed material: - HP Misc. Firmware USB - HP Solutions Firmware Upgrade Pack, Software Centric Release Notes (Min 2.2.9) [1] - Template XML files from the DSR media Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	Virtual PMAC: Verify IOS image is on the system Verify the IOS image is on the system. If the appropriate image does not exist, copy the image to the PMAC. <pre>\$ /bin/ls -i /var/TKLC/smac/image/<IOS_image_file></pre>
2 ☐	Virtual PMAC: Modify PMAC Feature to allow TFTP Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow TFTP traffic: <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT --enable=1 \$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures</pre> Note: Ignore the sentry restart instructions Note: This may take up to 60 seconds to complete.
3 ☐	Virtual PMAC TVOE HOST: Manipulate host server physical interfaces. Exit from the virtual PMAC console, by entering < ctrl-] > and you will be returned to the server prompt. Ensure that the interface of the server connected to switch1A is the only interface up and obtain the IP address of the management server management interface by performing the following commands: <pre>\$ sudo /sbin/ifup <ethernet_interface_1> \$ sudo /sbin/ifdown <ethernet_interface_2> \$ sudo /sbin/ip addr show <management_server_mgmtInterface> grep inet</pre> Note: The command output should contain the IP address of variable <management_server_Mgmt_ip_address>

Procedure 8. Configure Cisco 4948E-F Aggregation Switches-netConfig (HP DL 380 Servers Only)

4 ☐	Virtual PMAC: Determine if switch1A PROM upgrade is required	Determine if switch1A PROM upgrade is required. Note: ROM & PROM are intended to have the same meaning for this procedure Connect serially to switch1A by issuing the following command. <pre>\$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg switch1A_console Enter platcfg@pmac5000101's password: <platcfg_password> [Enter ``^Ec?' for help] Press Enter Switch> show version include ROM ROM: 12.2(31r)SGA1 System returned to ROM by reload</pre> Note: If the console command fails, contact Appendix U: My Oracle Support (MOS) Note the IOS image & ROM version for comparison in a following step. Exit from the console by entering <ctrl-e><c><.> and you will be returned to the server prompt. Check the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix K: Upgrade Cisco 4948 PROM to upgrade the PROM for switch1A.

Procedure 8. Configure Cisco 4948E-F Aggregation Switches-netConfig (HP DL 380 Servers Only)

5 ☐	Virtual PMAC: Modify configure xml file with information needed to initialize the switch.	Extract the configuration files from the zip file copied in procedure 6 <pre>\$ cd /usr/TKLC/smac/etc \$ sudo unzip DSR_NetConfig_Templates.zip</pre> Note: This will create a directory called “DSR_NetConfig_Templates” which contains all the necessary configuration files. Copy the following files using the following commands <pre>\$ sudo chmod 644 DSR_NetConfig_Templates/ \$ sudo cp -a DSR_NetConfig_Templates/init/Aggregation/*.xml /usr/TKLC/smac/etc \$ sudo cp -a DSR_NetConfig_Templates /config/DSR_RMS_Productization/4948E-F_L3_configure.xml /usr/TKLC/smac/etc</pre> Note: Update the 4948E init and configure xml files to match your network parameters. Values to be modified by the user will be notated in this step by a preceding dollar sign. So a value that has <some_variable_name> will need to be modified, removing the dollar sign and the less than, greater than sign. <pre>\$ sudo vi /usr/TKLC/smac/etc/switch1A_4948_E_E-F_cClass_template_init.xml \$ sudo vi /usr/TKLC/smac/etc/switch1B_4948_E_E-F_cClass_template_init.xml \$ sudo vi /usr/TKLC/smac/etc/4948E-F_L3_configure.xml</pre>

Procedure 8. Configure Cisco 4948E-F Aggregation Switches-netConfig (HP DL 380 Servers Only)

6 ☐	Virtual PMAC: Initialize Switch1A	Initialize switch1A by issuing the following command: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch1A_4948_4948E_init.xml</pre> Processing file: /usr/TKLC/smac/etc/switch1A_4948_4948E_init.xml Note: This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Appendix U: My Oracle Support (MOS). A successful completion of netConfig will return the user to the prompt. Use netConfig to get the hostname of the switch, to verify that the switch was initialized properly, and to verify that netConfig can connect to the switch. <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getHostname</pre> Hostname: switch1A \$ Note: If this command fails, stop this procedure and contact Appendix U: My Oracle Support (MOS) Exit the PMAC with the escape character is <ctrl-]>
7 ☐	Virtual PMAC TVOE HOST: Manipulate host server physical interfaces.	Exit from the virtual PMAC console, by entering < ctrl-] > and you will be returned to the server prompt. Ensure that the interface of the server connected to switch1B is the only interface up and obtain the IP address of the management server management interface by performing the following commands: <pre>\$ sudo /sbin/ifup <ethernet_interface_2> \$ sudo /sbin/ifdown <ethernet_interface_1></pre>

Procedure 8. Configure Cisco 4948E-F Aggregation Switches-netConfig (HP DL 380 Servers Only)

8 ☐	TVOE iLO/iLO: SSH into the Management Server	Log back into the PMAC. Login using virsh, and wait until you see the login prompt : <pre>\$ sudo /usr/bin/virsh list</pre> <pre>Id Name State ----- 1 myTPD running 2 PM&C running</pre> <pre>\$ sudo /usr/bin/virsh console <PM&C></pre> [Output Removed] <pre>Starting ntdMgr: [OK] Starting atd: [OK] 'TPD Up' notification(s) already sent: [OK] upstart: Starting tpdProvd... upstart: tpdProvd started. CentOS release 6.2 (Final) Kernel 2.6.32-220.17.1.el6prere16.0.0_80.14.0.x86_64 on an x86_64 PM&Cdev7 login:</pre>
9 ☐	Virtual PMAC: Initialize switch1B	Initialize switch1B by issuing the following command: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch1B_4948_4948E_init.xml</pre> <pre>Processing file: /usr/TKLC/smac/etc/switch1B_4948_4948E_init.xml \$</pre> Note: This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Appendix U: My Oracle Support (MOS) A successful completion of netConfig will return the user to the prompt. Use netConfig to get the hostname of the switch, to verify that the switch was initialized properly, and to verify that netConfig can connect to the switch. <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- device=switch1B getHostname</pre> <pre>Hostname: switch1B \$</pre> Note: If this command fails, stop this procedure and contact Appendix U: My Oracle Support (MOS)

Procedure 8. Configure Cisco 4948E-F Aggregation Switches-netConfig (HP DL 380 Servers Only)

10 ☐	Virtual PMAC: Modify PMAC Feature to disable TFTP	Disable the DEVICE.NETWORK.NETBOOT feature. <pre>\$ sudo /usr/TKLC/smac/bin/PM&Cadm editFeature --featureName=DEVICE.NETWORK.NETBOOT --enable=0 \$ sudo /usr/TKLC/smac/bin/PM&Cadm resetFeatures</pre> Note: Ignore the sentry restart instructions Note: This may take up to 60 seconds to complete.
11 ☐	Virtual PMAC: Configure the switches	Configure both switches by issuing the following command: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/4948_4948E_configure.xml Processing file: /usr/TKLC/smac/etc/4948_4948E_configure.xml</pre> Note: This step takes about 2-3 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Appendix U: My Oracle Support (MOS).
12 ☐	TVOE Management Server: Enable Interfaces on TVOE Host	Exit from the virtual PMAC console, by entering <ctrl-]> and you will be returned to the server prompt. Ensure that the interfaces of the server connected to switch1A and switch1B are up by performing the following commands: <pre>\$ sudo /sbin/ifup <ethernet_interface_1> \$ sudo /sbin/ifup <ethernet_interface_2></pre>

Procedure 8. Configure Cisco 4948E-F Aggregation Switches-netConfig (HP DL 380 Servers Only)

13 ☐	TVOE iLO/iLO: SSH into the Management Server	Log back into the PMAC. Login using virsh, and wait until you see the login prompt : <pre>\$ sudo /usr/bin/virsh list</pre> <pre>Id Name State ----- 1 myTPD running 2 PM&C running</pre> <pre>\$ sudo /usr/bin/virsh console <PM&C></pre> [Output Removed] <pre>Starting ntdMgr: [OK] Starting atd: [OK] 'TPD Up' notification(s) already sent: [OK] upstart: Starting tpdProvd... upstart: tpdProvd started. CentOS release 6.2 (Final) Kernel 2.6.32-220.17.1.el6prere16.0.0_80.14.0.x86_64 on an x86_64 PM&Cdev7 login:</pre>
14 ☐	Virtual PMAC: Verify switch configuration	Ping each of the interfaces to verify switch configuration <pre>\$ /bin/ping <switch1A_mgmtVLANIP> \$ /bin/ping <switch1B_mgmtVLANIP></pre>
15 ☐	Cabinet: Connect Uplinks of Switch1A	Attach switch1A customer uplink cables. Refer to the NAPD for which ports are uplink ports. Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.
16 ☐	Virtual PMAC: Verify access to customer network	Verify connectivity to the customer network by issuing the following command <pre>\$ /bin/ping <customer_supplied_ntp_server_address></pre>
17 ☐	Cabinet: Connect Uplinks of Switch1B	Attach switch1B customer uplink cables and detach switch1A customer uplink cables. Refer to the NAPD for which ports are uplink ports. Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.

Procedure 8. Configure Cisco 4948E-F Aggregation Switches-netConfig (HP DL 380 Servers Only)

18 ☐	Virtual PMAC: Verify access to customer network	Verify connectivity to the customer network by issuing the following command \$ /bin/ping <customer_supplied_ntp_server_address>
19 ☐	Virtual PMAC: Re-attach uplinks of switch1A	Re-attach switch1A customer uplink cables. Refer to the NAPD for which ports are uplink ports. Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active
20 ☐	TVOE Management Server: Restore the TVOE host back to its original state	Exit from the virtual PMAC console, by entering <ctrl-]> and you will be returned to the server prompt. Restore the server networking back to original state: \$ sudo /sbin/service network restart

4.6 Configure PMAC Server (NetBackup Only)

Procedure 9. Configure the PMAC Server (NetBackup Only)

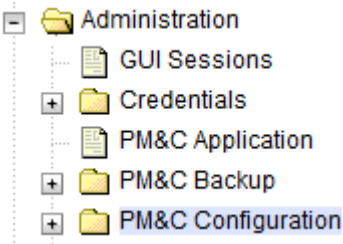
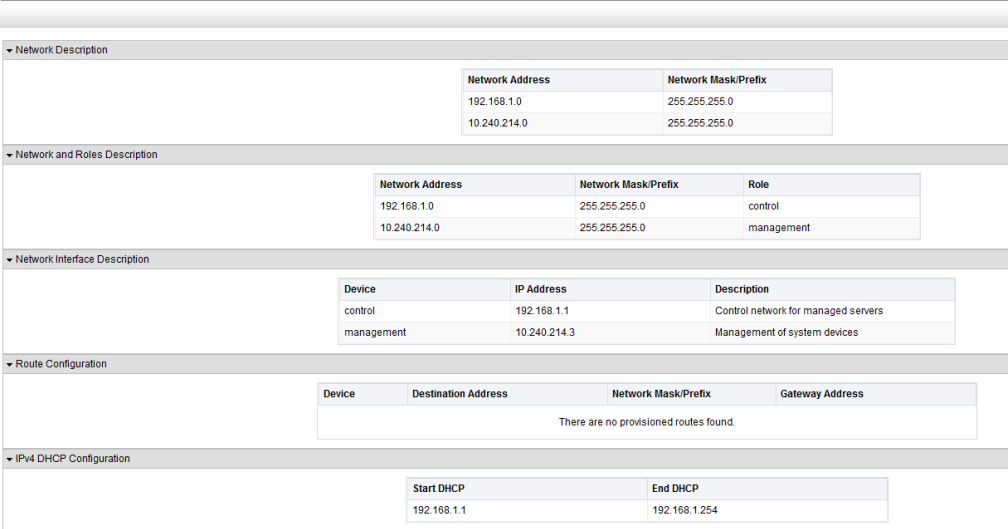
S T E P #	This procedure will provide PMAC configuration for NetBackup using the web interface. Note: The installer must be knowledgeable of the network. If you make a mistake, click Cancel and try again. The finish step may take longer time because it reconfigures the network and attempts to connect may fail. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PMAC GUI: Login Open web browser and navigate to the PMAC GUI, Login as guiadmin user: <code>https://<pmac_network_ip></code> 

Procedure 9. Configure the PMAC Server (NetBackup Only)

2

PMAC GUI:
Configure
Optional
Features

Procedure 9. Configure the PMAC Server (NetBackup Only)

3 ☐	PMAC GUI: Settings summary	Go to In the Main Menu -> Administration -> PM&C Configuration  The following summary screen will be displayed. This will provide a summary of PMAC configuration IPv4 Example Shown: Main Menu: Administration -> PM&C Configuration -> PM&C Network Configuration  Network Description <table border="1"> <thead> <tr> <th>Network Address</th> <th>Network Mask/Prefix</th> </tr> </thead> <tbody> <tr> <td>192.168.1.0</td> <td>255.255.255.0</td> </tr> <tr> <td>10.240.214.0</td> <td>255.255.255.0</td> </tr> </tbody> </table> Network and Roles Description <table border="1"> <thead> <tr> <th>Network Address</th> <th>Network Mask/Prefix</th> <th>Role</th> </tr> </thead> <tbody> <tr> <td>192.168.1.0</td> <td>255.255.255.0</td> <td>control</td> </tr> <tr> <td>10.240.214.0</td> <td>255.255.255.0</td> <td>management</td> </tr> </tbody> </table> Network Interface Description <table border="1"> <thead> <tr> <th>Device</th> <th>IP Address</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>control</td> <td>192.168.1.1</td> <td>Control network for managed servers</td> </tr> <tr> <td>management</td> <td>10.240.214.3</td> <td>Management of system devices</td> </tr> </tbody> </table> Route Configuration <table border="1"> <thead> <tr> <th>Device</th> <th>Destination Address</th> <th>Network Mask/Prefix</th> <th>Gateway Address</th> </tr> </thead> <tbody> <tr> <td colspan="4">There are no provisioned routes found.</td> </tr> </tbody> </table> IPv4 DHCP Configuration <table border="1"> <thead> <tr> <th>Start DHCP</th> <th>End DHCP</th> </tr> </thead> <tbody> <tr> <td>192.168.1.1</td> <td>192.168.1.254</td> </tr> </tbody> </table>	Network Address	Network Mask/Prefix	192.168.1.0	255.255.255.0	10.240.214.0	255.255.255.0	Network Address	Network Mask/Prefix	Role	192.168.1.0	255.255.255.0	control	10.240.214.0	255.255.255.0	management	Device	IP Address	Description	control	192.168.1.1	Control network for managed servers	management	10.240.214.3	Management of system devices	Device	Destination Address	Network Mask/Prefix	Gateway Address	There are no provisioned routes found.				Start DHCP	End DHCP	192.168.1.1	192.168.1.254
Network Address	Network Mask/Prefix																																					
192.168.1.0	255.255.255.0																																					
10.240.214.0	255.255.255.0																																					
Network Address	Network Mask/Prefix	Role																																				
192.168.1.0	255.255.255.0	control																																				
10.240.214.0	255.255.255.0	management																																				
Device	IP Address	Description																																				
control	192.168.1.1	Control network for managed servers																																				
management	10.240.214.3	Management of system devices																																				
Device	Destination Address	Network Mask/Prefix	Gateway Address																																			
There are no provisioned routes found.																																						
Start DHCP	End DHCP																																					
192.168.1.1	192.168.1.254																																					

Procedure 9. Configure the PMAC Server (NetBackup Only)

4 ☐	PMAC Command Line: Perform a system healthcheck	Execute the following commands: <pre>\$ alarmMgr --alarmStatus</pre> This command should return no output on a healthy system. <pre>\$ sudo sentry status</pre> All Processes should be running, displaying output similar to the following: <pre>[admusr@5010441PMAC ~]\$ sudo sentry status sending status command... PM&C Sentry Status ----- sentryd started: Thu Sep 15 15:02:57 2016 Current activity mode: ACTIVE Process PID Status StartTS NumR ----- smacTalk 10695 running Thu Sep 15 15:02:57 2016 1 smacMon 10705 running Thu Sep 15 15:02:57 2016 1 hpiPortAudit 10730 running Thu Sep 15 15:02:57 2016 1 snmpEventHandler 10757 running Thu Sep 15 15:02:57 2016 1 Wed Jan 4 12:21:35 2017 Command Complete.</pre>
5 ☐	PMAC Command Line: Install NetBackup (Optional)	- If the NetBackup client installation will rely on the TPD “nbAutoInstall” process to configure the PMAC NetBackup client perform the following at the PMAC Command Line, otherwise continue to sub bullet 2 below. <pre>\$ sudo mkdir -p /usr/opensv/NetBackup/bin/ \$ sudo ln -s /usr/TKLC/smac/sbin/bpstart_notify /usr/opensv/NetBackup/bin/ \$ sudo ln -s /usr/TKLC/smac/sbin/bpend_notify /usr/opensv/NetBackup/bin/</pre> Use TPD platcfg utility to add the NetBackup Server’s alias and IP to the “/etc/hosts” file. - Refer to [14], procedure “PM&C NetBackup Client Installation and Configuration” for instructions on installing the NetBackup client on the TVOE Management Server.

Procedure 9. Configure the PMAC Server (NetBackup Only)

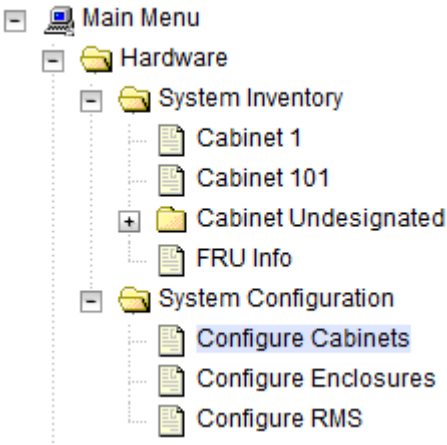
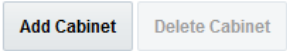
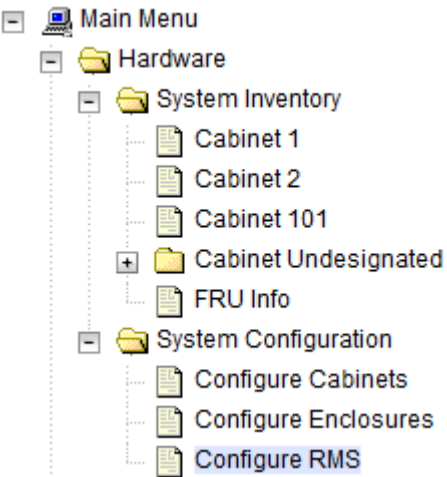
6 ☐	PMAC Command Line: Perform a backup	Perform PMAC application backup using the following command: <pre>\$ sudo pmacadm backup</pre> <pre>PM&C backup been successfully initiated as task ID 7</pre> <pre>[usradm@pmacDev3 ~]\$</pre> Note: The "pmacadm backup" command uses a naming convention which includes a date/time stamp in the file name (Example file name: backupPmac_20111025_100251.pef). In the example provided, the backup file name indicates that it was created on 10/25/2011 at 10:02:51 am server time. Next Verify that the backup was successful using the following command: <pre>\$ sudo pmaccli getBgTasks</pre> <pre>2: Backup PMAC COMPLETE - PMAC Backup successful</pre> <pre>Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4</pre> <pre>sinceUpdate: 2 taskRecordNum:</pre> Once the backup has been verified that it was successful, copy the backup file to a remote location. The backup file is located under /var/TKLC/smac/backup.

4.7 Add Rack Mount Server to PMAC

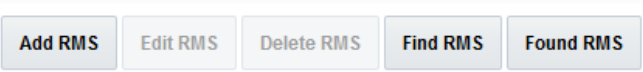
Procedure 10. Add RMS to the PMAC system Inventory

S T E P #	This procedure will add Rack Mount Servers to the PMAC system inventory. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PMAC GUI: Login Open web browser and navigate to the PMAC GUI, Login as guiadmin user: <code>https://<pmac_network_ip></code> 

Procedure 10. Add RMS to the PMAC system Inventory

2 ☐	PMAC GUI: Configure Cabinets	Navigate to Main Menu -> Hardware -> System Configuration -> Configure Cabinets.  Press the Add Cabinet Button  Enter the Cabinet ID, and press the Add Cabinet button: Cabinet ID (required): 1 <i>Cabinet ID must be from 1 to 654.</i> 
3 ☐	PMAC GUI: Configure RMS	Navigate to Main Menu -> Hardware -> System Configuration -> Configure RMS 

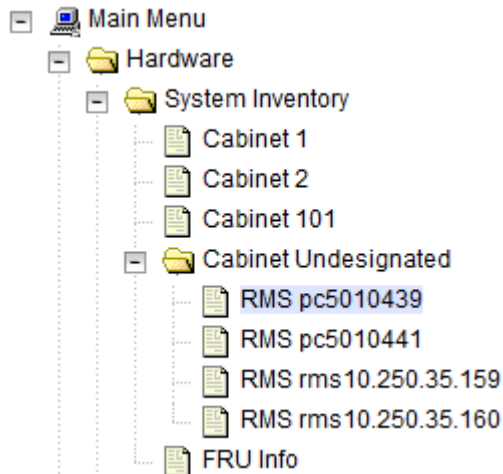
Procedure 10. Add RMS to the PMAC system Inventory

4 ☐	PMAC GUI: Add RMS	On the Configure RMS panel, click the Add RMS button. 
5 ☐	PMAC GUI: Enter information	Enter the IP Address of the rack mount server management port (iLO/iLOM) and username/password of the iLO/iLOM. All the other fields are optional. Then click on the Add RMS button. Main Menu: Hardware -> System Configuration -> Configure RMS [Add RMS]  Note: The PMAC contains default credentials for the rack mount server management port (not to be confused with OS or Application credentials), however if you know the default credentials will not work then enter the valid credentials for the rack mount server management port.
6 ☐	PMAC GUI: Repeat for Additional Rack Mount Servers	Repeat Steps 3-5 for additional Rack Mount Servers.

Procedure 10. Add RMS to the PMAC system Inventory

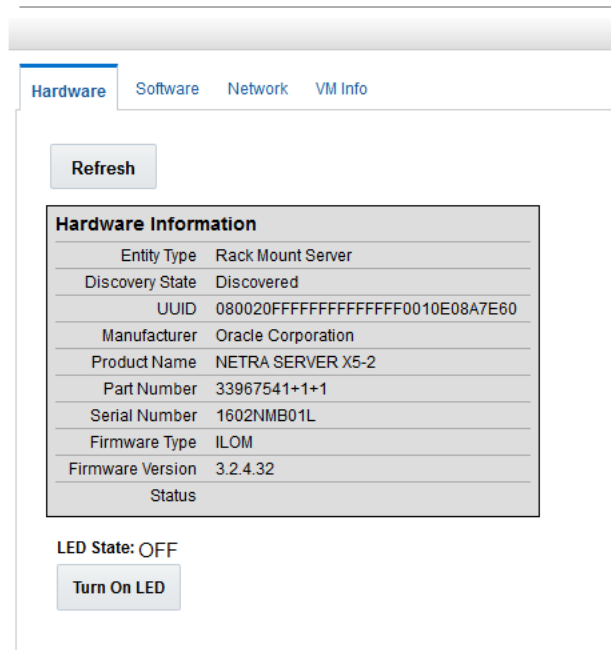
- 7 **PMAC**
☐ **GUI:** Verify RMS discovered

Navigate to **Main Menu -> Hardware -> System Inventory -> Cabinet xxx -> RMS yyy**. Where **xxx** is the cabinet id selected when adding RMS (or "Undesignated") and **yyy** is the name of the RMS.



The RMS inventory page is displayed.

Main Menu: Hardware -> System Inventory -> Cabinet



Periodically refresh the hardware information using the double arrow to the right of the title **"Hardware Information"** until the **"Discovery state"** changes from **"Undiscovered"** to **"Discovered"**.

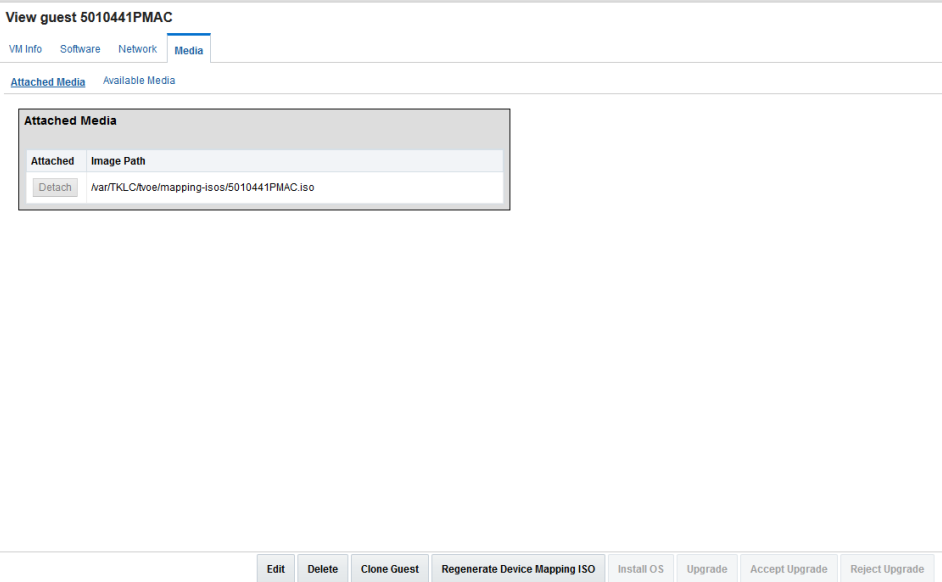
Note: If **"Status"** displays an error, contact Appendix U: My Oracle Support (MOS)

4.8 Install TVOE on Additional Rack Mount Servers

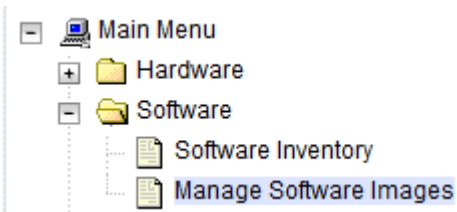
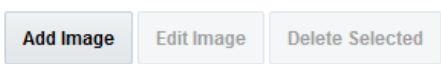
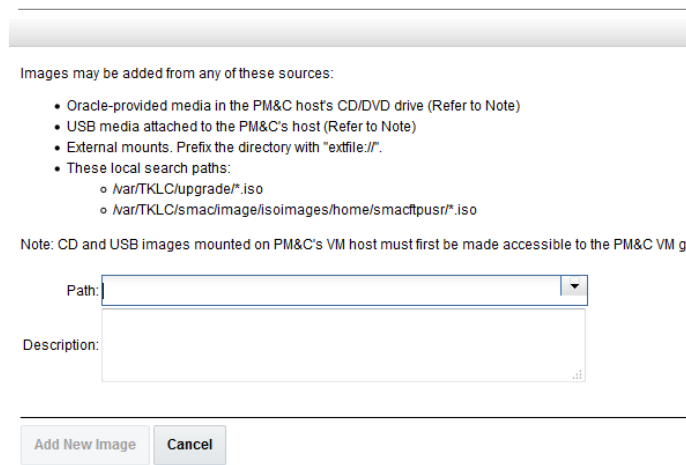
Procedure 11. Install TVOE on Additional Rack Mount Servers

S T E P #	This procedure will install the TVOE operating system on additional Mounted Servers. Prerequisite: PMAC (virtualized) has been installed on the First RMS Server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PMAC GUI: Login Open web browser and navigate to the PMAC GUI, Login as guiadmin user: <code>https://<pmac_network_ip></code>  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.

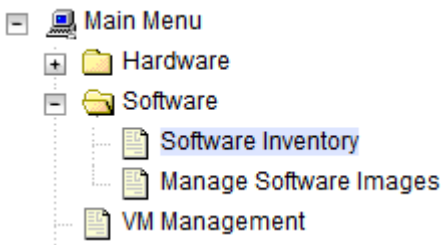
Procedure 11. Install TVOE on Additional Rack Mount Servers

2 ☐	PMAC's TVOE : Load TVOE ISO	Add the TVOE ISO image to the PMAC, this can be done in one of two ways: 1. Attach the USB device containing the ISO image to a USB port. • Login to the PMAC GUI if not already done so (Step 1) • In the "VM Management" list, select the PMAC guest. On the resulting "View VM Guest" page, select the Media tab. • Under the Media tab, find the ISO image in the "Available Media" list, and click its Attach button. After a pause, the image will appear in the "Attached Media" list.  2. Using a TVOE 64 bit ISO file Use sftp to transfer the ISO image to the PMAC server in the /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as pmacftpusr user: <pre># cd into the directory where your ISO image is located on the TVOE Host (not on the PMAC server)</pre> <pre># Using sftp, connect to the PMAC management server</pre> <pre>> sftp pmacftpusr@<PM&C_management_network_ip> > put <image>.iso</pre> <pre># After the image transfer is 100% complete, close the connection</pre> <pre>> quit</pre>

Procedure 11. Install TVOE on Additional Rack Mount Servers

3 ☐	PMAC GUI: Add TVOE image	Navigate to Main Menu -> Software -> Manage Software Images  Press Add Image button. Use the drop down to select the image.  If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://..."). These devices are assigned in numerical order as CD and USB images become available on the TVOE Management Server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the ISO image of interest is normally present on the second device, "device://dev/sr1". If one or more CD or USB-based images were already present on the TVOE Management Server before you started this procedure, choose a correspondingly higher device number. If in Step 2 the image was transferred to PMAC via sftp it will appear in the list as a local file "/var/TKLC/...". Main Menu: Software -> Manage Software Images [Add Image]  Select the appropriate path and Press Add New Image button. You may check the progress using the Task Monitoring link. Observe the green bar indicating success. Once the green bar is displayed, remove the TVOE Media from the optical drive of the TVOE Management Server.

Procedure 11. Install TVOE on Additional Rack Mount Servers

4 ☐	PMAC GUI: Select RMS Servers for TVOE OS install	Navigate to Software -> Software Inventory.  Select the RMS servers you want to IPM. If you want to install the same OS image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows will be highlighted in green. Main Menu: Software -> Software Inventory <table border="1"> <thead> <tr> <th>Identity</th> <th>IP Address</th> <th>Hostname</th> <th>Platform Name</th> <th>Platform Version</th> <th>Application Name</th> <th>Application Version</th> <th>Designation</th> <th>Function</th> </tr> </thead> <tbody> <tr> <td>RMS: pc5010439</td> <td>192.168.1.32</td> <td>hostname7237c8296d11</td> <td>TPD (x86_64)</td> <td>7.2.0.0.0-88.18.0</td> <td>TVOE</td> <td>3.2.0.0.0_88.18.0</td> <td></td> <td></td> </tr> </tbody> </table> Click on Install OS Selection active -- periodic display updates paused Install OS Upgrade Accept Upgrade Reject Upgrade Transfer ISO Image Map Device Aliases Rediscover	Identity	IP Address	Hostname	Platform Name	Platform Version	Application Name	Application Version	Designation	Function	RMS: pc5010439	192.168.1.32	hostname7237c8296d11	TPD (x86_64)	7.2.0.0.0-88.18.0	TVOE	3.2.0.0.0_88.18.0		
Identity	IP Address	Hostname	Platform Name	Platform Version	Application Name	Application Version	Designation	Function												
RMS: pc5010439	192.168.1.32	hostname7237c8296d11	TPD (x86_64)	7.2.0.0.0-88.18.0	TVOE	3.2.0.0.0_88.18.0														

Procedure 11. Install TVOE on Additional Rack Mount Servers

5

PMAC GUI:

Initiate OS Install on RMS Server(s)

The left side of this screen shows the servers to be affected by this OS installation. From the list of available bootable images on the right side of the screen, select one OS image to install to all of the selected servers.

Software Install - Select Image

Tasks*

Targets

Entity	Status
RMS: pc5010439	

Select Image

Image Name	Type	Architecture	Description
TPD Install-7.0.3.0.0_86.43.0-OracleLinux6.7-x86_64	Bootable	x86_64	
TPD Install-7.2.0.0.0_88.18.0-OracleLinux6.7-x86_64	Bootable	x86_64	
TVOE-3.0.3.0.0_86.43.0-x86_64	Bootable	x86_64	
TVOE-3.2.0.0.0_88.18.0-x86_64	Bootable	x86_64	

HP DL380 Gen9 with 10GB FlexLOM, enter the following in the **Supply Software Install Arguments (Optional)** field:

Supply Software Install Arguments (Optional)

control_if=eth05,eth06

Click on **Start Software Install**, a confirmation window will pop up, click on **Ok** to proceed with the install.

Start Software Install

Back

Select OK to begin the installation

You have selected to install a bootable OS iso on the selected targets.

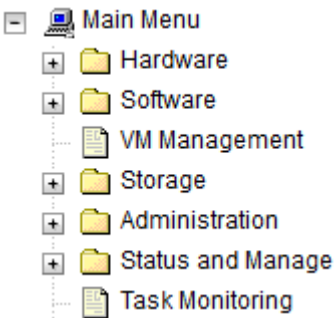
The following targets already have an Application:
RMS: pc5010439 ==> TVOE

Are you sure you want to install TVOE-3.2.0.0.0_88.18.0-x86_64 on all entities in the Targets list?

OK

Cancel

Procedure 11. Install TVOE on Additional Rack Mount Servers

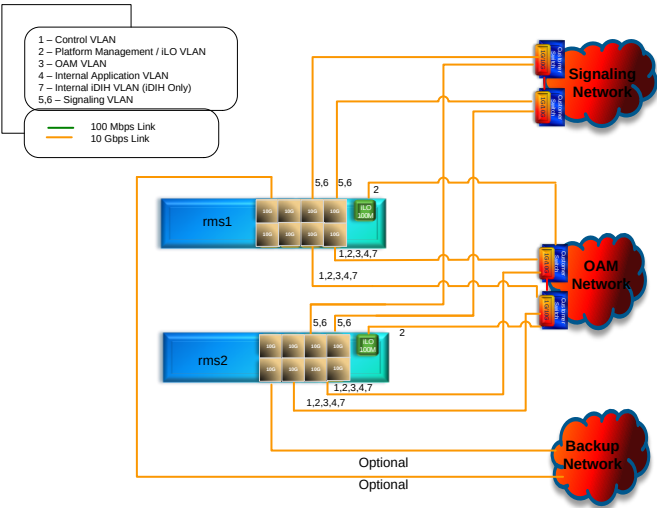
6	PMAC GUI: Monitor OS Install	Navigate to Main Menu -> Task Monitoring to monitor the progress of the TVOE Installation background task. A separate task will appear for each server affected.  Main Menu: Task Monitoring Filter* <table border="1"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>State</th> <th>Task Output</th> <th>Running Time</th> <th>Start Time</th> <th>Progress</th> </tr> </thead> <tbody> <tr> <td>622</td> <td>Install OS</td> <td>RMS: pc5010439</td> <td>Installing packages from ISO</td> <td>IN_PROGRESS</td> <td>N/A</td> <td>0:04:19</td> <td>2016-06-07 14:10:05</td> <td>71%</td> </tr> </tbody> </table> When the installation is complete, the task will change to green and the Progress bar will indicate "100%". Main Menu: Task Monitoring Filter* <table border="1"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>State</th> <th>Task Output</th> <th>Running Time</th> <th>Start Time</th> <th>Progress</th> </tr> </thead> <tbody> <tr> <td>622</td> <td>Install OS</td> <td>RMS: pc5010439</td> <td>Done: TVOE-3.2.0.0.0_88.18.0-x86_64</td> <td>COMPLETE</td> <td>N/A</td> <td>0:28:42</td> <td>2016-06-07 14:10:05</td> <td>100%</td> </tr> </tbody> </table>	ID	Task	Target	Status	State	Task Output	Running Time	Start Time	Progress	622	Install OS	RMS: pc5010439	Installing packages from ISO	IN_PROGRESS	N/A	0:04:19	2016-06-07 14:10:05	71%	ID	Task	Target	Status	State	Task Output	Running Time	Start Time	Progress	622	Install OS	RMS: pc5010439	Done: TVOE-3.2.0.0.0_88.18.0-x86_64	COMPLETE	N/A	0:28:42	2016-06-07 14:10:05	100%
ID	Task	Target	Status	State	Task Output	Running Time	Start Time	Progress																														
622	Install OS	RMS: pc5010439	Installing packages from ISO	IN_PROGRESS	N/A	0:04:19	2016-06-07 14:10:05	71%																														
ID	Task	Target	Status	State	Task Output	Running Time	Start Time	Progress																														
622	Install OS	RMS: pc5010439	Done: TVOE-3.2.0.0.0_88.18.0-x86_64	COMPLETE	N/A	0:28:42	2016-06-07 14:10:05	100%																														

4.9 Configure TVOE on Additional Rack Mount Servers

Procedure 12. Configure TVOE on Additional Rack Mount Servers

S T E P #	This procedure will configure TVOE on all remaining RMS Servers. Prerequisite: RMS Server has been IPM'ed with TVOE OS Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Determine Bridge Names and Interfaces	Determine the network bridge names by referring to procedure 4, step 1. The entries in this table should match the table that was filled out for the first rack mount server.
2 ☐	RMS iLO/iLOM: Login and Launch the Integrated Remote Console	Log in to iLO/iLOM; follow Appendix D: TVOE iLO/iLOM GUI Access for instructions on how to access the iLO/iLOM GUI. <code>https://<management_server_iLO_ip></code>
3 ☐	RMS iLO/iLOM: Create the Management Network	Create the Management network, execute the following command: Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure. <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Management_Bridge_Interface> --onboot=yes Interface bond0.2 added</pre> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=management --bootproto=none --onboot=yes --address=<Management_Server_TVOE_IP> --netmask=<Management_Server_TVOE_Netmask> --bridgeInterfaces=<TVOE_Management_Bridge_Interface> Bridge management added!</pre>

Procedure 12. Configure TVOE on Additional Rack Mount Servers

4 ☐	RMS iLO/iLOM: Create the Management Network Route	<pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=default --device=management -- gateway=<Management_Gateway_IP_Address></pre> Route to management added
5 ☐	RMS iLO/iLOM: TVOE Bond1 Configuration (Segregated Signaling)	If the OAM networks and signaling networks share the same bond (non-segregated), skip this step.  Create Bond1 interface: Note: Refer to Section 3.4 for network interface references for the configuration step below. <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=bond1 --onboot=yes \$ sudo /usr/TKLC/plat/bin/netAdm set -- device=<ethernet_interface_3> --type=Ethernet -- master=bond1 --slave=yes --onboot=yes \$ sudo /usr/TKLC/plat/bin/netAdm set -- device=<ethernet_interface_4> --type=Ethernet -- master=bond1 --slave=yes --onboot=yes</pre>

Procedure 12. Configure TVOE on Additional Rack Mount Servers

6 ☐	RMS iLO/iLOM: Set Ethernet Interface Ring Buffer Sizes	The following commands will increase the ring buffer sizes on 10Gbps Ethernet Interfaces: Note: Refer to Section 3.4 for network interface server reference table <pre> \$ sudo netAdm set --device=<ethernet_interface_1> --ringBufferRx=4096 --ringBufferTx=4096 \$ sudo netAdm set --device=<ethernet_interface_2> --ringBufferRx=4096 --ringBufferTx=4096 If step 6 was executed, execute the following commands: \$ sudo netAdm set --device=<ethernet_interface_3> --ringBufferRx=4096 --ringBufferTx=4096 \$ sudo netAdm set --device=<ethernet_interface_4> --ringBufferRx=4096 --ringBufferTx=4096 </pre>

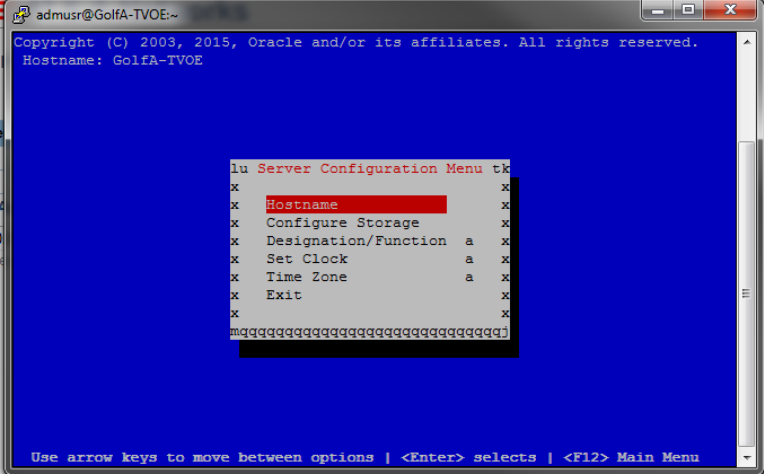
Procedure 12. Configure TVOE on Additional Rack Mount Servers

7 ☐	RMS iLO/iLOM: Add the NetBackup Network-Option 1 (Optional)	If NetBackup is to be used, execute this step, otherwise skip to Step 11. Select only this option or the following options listed in steps 8 or 9. Before selecting the configuration option, first read the description in each step to determine which configuration is applicable to your installation and network. NetBackup is a tool that allows the customer to take remote backups of the system. Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured. Note: The example below illustrates a TVOE Management Server configuration with the NetBackup feature enabled. The NetBackup network is configured with a non-default MTU size. Note: The MTU size must be consistent between a network bridge, device, or bond, and associated VLANs. <u>Create NetBackup bridge using a bond containing an untagged interface</u> <pre> \$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_NetBackup_Bridge_Interface> --onboot=yes --type=Bonding --mode=active-backup --miimon=100 --MTU=<NetBackup_MTU_size> Interface <TVOE_NetBackup_Bridge_Interface> added \$ sudo /usr/TKLC/plat/bin/netAdm set --device=<ethernet_interface_4> --type=Ethernet --master=<TVOE_NetBackup_Bridge_Interface> --slave=yes --onboot=yes Interface <ethernet_interface_4> updated \$ sudo /usr/TKLC/plat/bin/netAdm add -type=Bridge --name=<TVOE_NetBackup_Bridge> --onboot=yes - bootproto=none --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface> --address=<TVOE_NetBackup_IP> --netmask=<TVOE_NetBackup_Netmask> </pre>

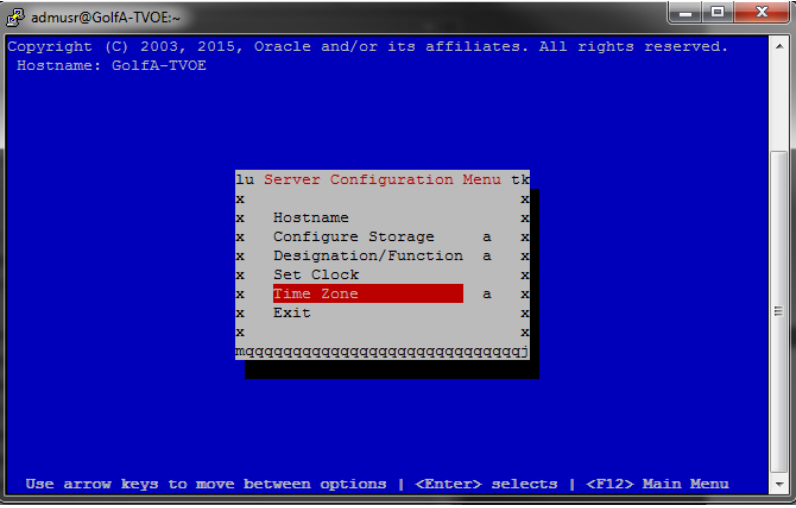
Procedure 12. Configure TVOE on Additional Rack Mount Servers

8 ☐	RMS iLO/iLOM: Add the NetBackup Network-Option 2 (Optional)	Select only this option or options in Steps 7 or 9 <u>Create NetBackup bridge using an untagged native interface:</u> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add -type=Bridge --name=<TVOE_NetBackup_Bridge> --onboot=yes - bootproto=none -MTU=<NetBackup_MTU_size> --bridgeInterfaces=<Ethernet_Interface_4> --address=<TVOE_NetBackup_IP> --netmask=<TVOE_NetBackup_Netmask></pre>
9 ☐	RMS iLO/iLOM: Add the NetBackup Network-Option 3 (Optional)	Select only this option or options in 7 or 8 <u>Create NetBackup bridge using a tagged device:</u> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_NetBackup_Bridge_Interface> --onboot=yes Interface <TVOE_NetBackup_Bridge_Interface> added \$ sudo /usr/TKLC/plat/bin/netAdm add -type=Bridge --name=<TVOE_NetBackup_Bridge> --onboot=yes --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface> --address=<TVOE_NetBackup_IP> --netmask=<TVOE_NetBackup_Netmask></pre>
10 ☐	RMS iLO/iLOM: Restart the network interfaces	Restart the network interfaces, execute the following command: <pre>\$ sudo service network restart</pre>

Procedure 12. Configure TVOE on Additional Rack Mount Servers

11 ☐	RMS iLO/iLOM: Set Hostname	Set the server hostname by running the following: <pre>\$ sudo su - platcfg</pre> Navigate to Server Configuration -> Hostname ->Edit.  Set TVOE Management Server hostname Press OK. Navigate out of Hostname

Procedure 12. Configure TVOE on Additional Rack Mount Servers

12 ☐	RMS iLO/iLOM: Set the Time Zone and/or Hardware Clock	Navigate to Server Configuration -> Time Zone.  Select Edit. Set the time zone and/or hardware clock to <i>“UTC”</i> (or appropriate time zone value) Press OK. Navigate out of Server Configuration

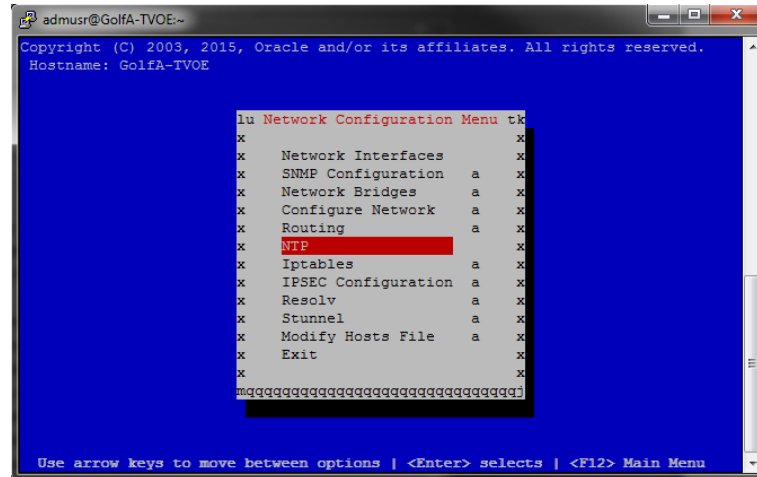
Procedure 12. Configure TVOE on Additional Rack Mount Servers

13

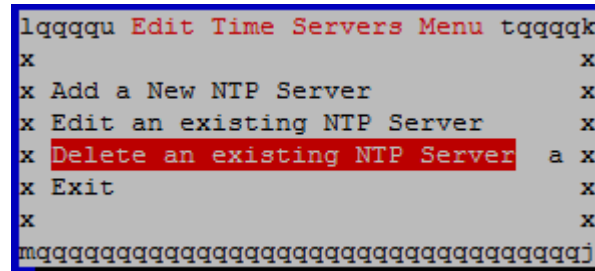
RMS
iLO/iLOM:
 Delete PMAC
 VM as NTP
 Source on
 RMS

Note: fdconfig script will populate the NTP configuration.

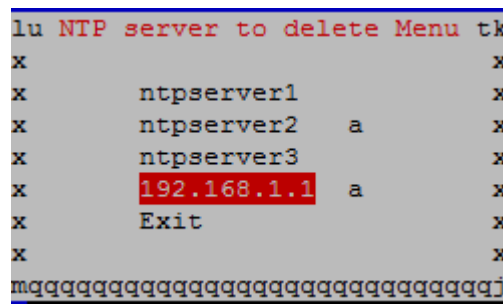
Navigate to **Network Configuration ->NTP**.



Select **Delete an existing NTP Server**

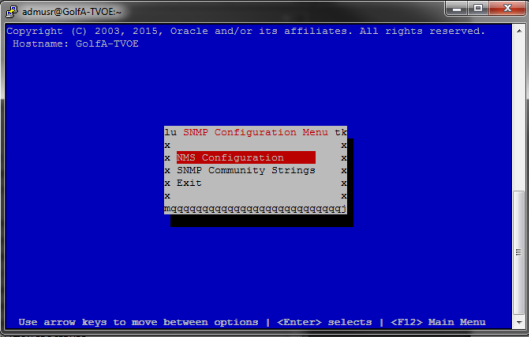
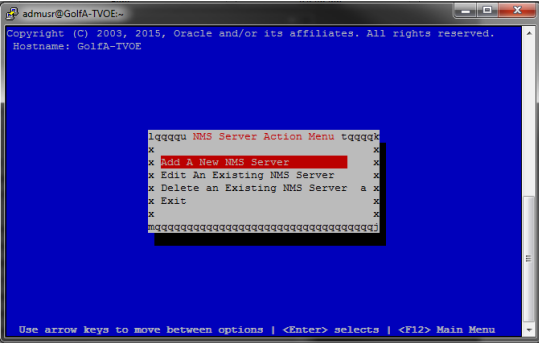
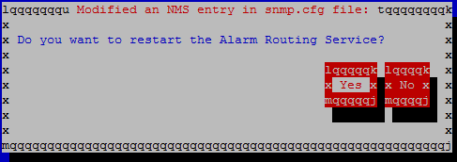


Select the PMAC VM Control IP, Click **[Enter]**



You will be returned to the **NTP Menu**

Procedure 12. Configure TVOE on Additional Rack Mount Servers

14 ☐	RMS iLO/iLOM: Set SNMP	Note: Refer to Appendix H: SNMP Configuration to understand the preferred SNMP configuration Navigate to Network Configuration -> SNMP Configuration -> NMS Configuration.  Select Edit and then choose Add a New NMS Server. The Add an NMS Server page will be displayed.  Complete the form by entering NMS server IP, Port (<i>default port is 162</i>) and community string provided by the customer about the SNMP trap destination. Select OK to finalize the configuration. The NMS Server Action Menu will now be displayed. Select Exit. The following dialogue will then be presented.  Select Yes and then wait a few seconds while the Alarm Routing Service is restarted. At that time the SNMP Configuration menu will be presented. Exit platcfg.

Procedure 12. Configure TVOE on Additional Rack Mount Servers

15 ☐	RMS iLO/iLOM: Restart Server	Execute the following command to restart the server: \$ sudo init 6
16 ☐	1st RMS iLO/iLOM: Verify Ring Buffer Settings	Verify the ring buffer sizes have been configured correctly (from Step 6) by executing the following command for each Ethernet interface configured above: \$ ethtool -g <eth interfaces configured above> Example shown below: <pre style="background-color: #2e3436; color: #eeeeec; padding: 10px;">[admusr@FJ-TVOE-2 ~]\$ ethtool -g eth01 Ring parameters for eth01: Pre-set maximums: RX: 4096 RX Mini: 0 RX Jumbo: 0 TX: 4096 Current hardware settings: RX: 4096 RX Mini: 0 RX Jumbo: 0 TX: 4096</pre>

Procedure 12. Configure TVOE on Additional Rack Mount Servers

17 ☐	RMS iLO/iLOM: Configure NetBackup- Part 1 (Optional)	Execute this step if the NetBackup feature is enabled for this system, otherwise skip this step. Configure the appropriate NetBackup client on the PMAC TVOE host. Open firewall ports for NetBackup using the following commands: <pre>\$ sudo ln -s /usr/TKLC/plat/share/NetBackup/60NetBackup.ipt /usr/TKLC/plat/etc/iptables/ \$ sudo /usr/TKLC/plat/bin/iptablesAdm reconfig</pre> Enable platcfg to show the NetBackup Menu Items by executing the following commands: <pre>\$ sudo platcfgadm -show NBConfig; \$ sudo platcfgadm -show NBInit; \$ sudo platcfgadm -show NBDeInit; \$ sudo platcfgadm -show NBInstall; \$ sudo platcfgadm -show NBVerifyEnv; \$ sudo platcfgadm -show NBVerify;</pre> Create LV and file system for NetBackup client software on the vgguests volume group: <pre>\$sudo /usr/TKLC/plat/sbin/storageMgr /tmp/nb.lvm</pre> This will create the LV, format it with a filesystem, and mount it under /usr/opencv/. Example output is shown below: <pre>Called with options: /tmp/nb.lvm VG vgguests already exists. Creating lv NetBackup_lv. Volume NetBackup_lv will be created. Success: Volume NetBackup_lv was created. Creating filesystem, this may take a while. Updating fstab for lv NetBackup_lv. Configuring existing lv NetBackup_lv. The LV for NetBackup has been created!</pre>

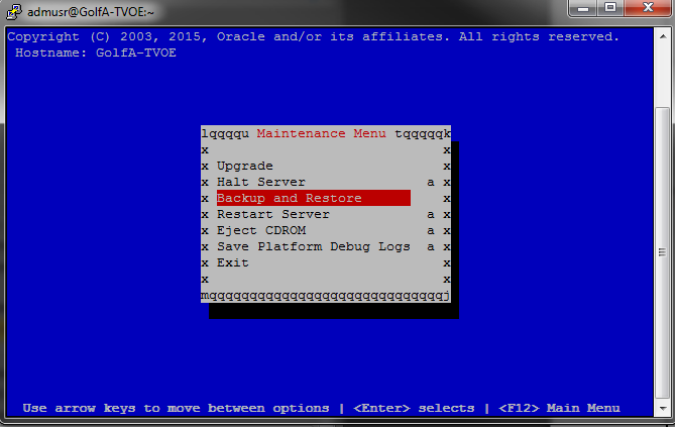
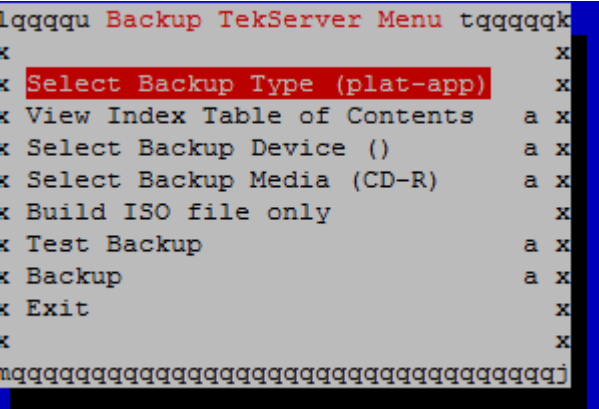
Procedure 12. Configure TVOE on Additional Rack Mount Servers

18 ☐	RMS iLO/iLOM: Configure NetBackup-Part 2 (Optional)	Install the NetBackup client software: Refer to Appendix I: Application NetBackup Client Installation Procedures on instructions how to install the NetBackup client. Note: Skip any steps relating to copying NetBackup “notify” scripts to /usr/opensv/NetBackup/bin. The TVOE NetBackup notify scripts are taken care of in the next step. Create softlinks for TVOE specific NetBackup notify scripts. <pre>\$sudo ln -s /usr/TKLC/plat/sbin/bpstart_notify /usr/opensv/NetBackup/bin/bpstart_notify \$sudo ln -s /usr/TKLC/plat/sbin/bpend_notify /usr/opensv/NetBackup/bin/bpend_notify</pre> Note: Once the NetBackup Client is installed on TVOE, the NetBackup Master should be configured to back up the following files form the TVOE host: • /var/TKLC/bkp/*.iso
19 ☐	RMS iLO/iLOM: Setup syscheck	Syscheck must be configured to monitor bonded interfaces. Replace “bondedInterfaces” with “bond0” or “bond0,bond1” if segregated networks are used: <pre>\$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond -set --var=DEVICES -val=<bondedInterfaces> \$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond -enable</pre>
20 ☐	RMS iLO/iLOM: Verify syscheck	Verify syscheck: <pre>\$ sudo /usr/TKLC/plat/bin/syscheck net ipbond -v</pre> Expected output should look similar to below: <pre>Running modules in class net... ipbond: Bonded interface bond0 is OK OK LOG LOCATION: /var/TKLC/log/syscheck/fail log</pre>

Procedure 12. Configure TVOE on Additional Rack Mount Servers

21 ☐	RMS iLO/iLOM: Verify Server Health	Execute the following: <pre>\$ alarmMgr --alarmStatus</pre> This command should return no output on a healthy system. If any alarms are reported, contact Appendix U: My Oracle Support (MOS)

Procedure 12. Configure TVOE on Additional Rack Mount Servers

22 ☐	RMS iLO/iLOM: Perform a TVOE backup using TPD platcfg utility	Execute the following: <pre>\$ sudo su - platcfg</pre> Navigate to Maintenance -> Backup and Restore  Select Backup Platform (CD/DVD) Note: If no cdrom device is found by TPD, you will receive an error dialog with the message: "No disk device available. This is normal on systems without a cdrom device." Press Enter to continue. Select Build ISO file only, and press Enter to continue. Exit from TPD platcfg utility.  The TVOE backup can be found in the "/var/TKLC/bkp/" directory, and is prefixed by the server hostname. An example of a TVOE backup ISO follows: /var/TKLC/bkp/RMS503u14-plat-app-201210301505.iso Move the TVOE backup to a customer provided backup server for safe keeping.

Procedure 12. Configure TVOE on Additional Rack Mount Servers

23 ☐	Additional RMS: Repeat	Repeat this procedure for additional Rack Mount Servers.

4.10 Determine VM Placement and Socket Pinning

Note: Skip this section if deploying a Non-HA Lab Node of DL380 Gen system

In order to maximize performance efficiency, customers who are deploying DSR **on Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps)** servers may obtain the DSR VM placement and CPU pinning information document. This recommended document can be obtained from an Oracle representative for implementation. If the DSR VM placement and CPU pinning information is NOT available, the customer may use [16] (VM Placement and CPU Socket Pinning Tool)

Note: VM placement and CPU pinning will need to be determined for all components of the DSR installation (PMAC, IDIH, DSR, and SDS)

Note: HP DL380 Gen9 equipped with onboard 1Gbps NICs should follow Appendix S: VM placement in HP DL380 Gen8/Gen9 (Onboard 1Gbps NICs) and CPU Pinning in HP DL380 Gen9 (Onboard 1Gbps NICs) for VM placement/Pinning.

4.11 Deploy Redundant PMAC (Optional)

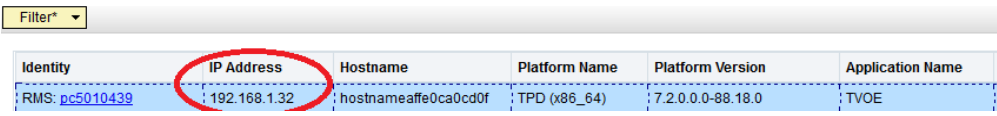
This procedure is optional and required only if the redundant PMAC Server feature is to be deployed. This procedure will provide the instructions for deploying a redundant PMAC, as well as creating the first backup from the primary PMAC.

Note: [Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9]: Skip this Section

Procedure 13. Installing a Redundant PMAC

S T E P #	This procedure is optional and required only if the redundant PMAC Server feature is to be deployed. This procedure will provide steps for deploying a redundant PMAC, as well as creating the first backup from the primary PMAC. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Primary PMAC: Establish SSH Session	Establish an SSH session to the primary PMAC, login as admusr .

Procedure 13. Installing a Redundant PMAC

2 ☐	Primary PMAC: Exchange SSH keys between the Primary PMAC and the Redundant PMAC's TVOE Host	Use the PMAC GUI to determine the Control Network IP address of the redundant PMAC's TVOE host server. From the PMAC GUI, navigate to Main Menu -> Software -> Software Inventory. Main Menu: Software -> Software Inventory  Note the IP address for the redundant PMAC's TVOE Host server. Login to the PMAC terminal as the admusr. From a terminal window connection on the PMAC as the admusr user, exchange SSH keys for admusr between the primary PMAC and the redundant PMAC's TVOE Host server using the keyexchange utility, using the Control network IP address for the redundant PMAC's TVOE Host server. When prompted for the password, enter the password for the admusr user of the redundant PMAC's TVOE Host server. <pre>\$ keyexchange admusr@<redundant PMAC's TVOE Host server control IP></pre>
3 ☐	Primary PMAC: Export the PMAC ISO image to the Redundant PMAC's TVOE Host	Execute the following command to export the PMAC ISO image to the redundant PMAC's TVOE host Server: <pre>\$ sudo /usr/sbin/exportfs <redundant PMAC TVOE Host Control IP>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name></pre>
4 ☐	Primary PMAC: SSH to the Redundant PMAC's TVOE Host	Establish an SSH session to the redundant PMAC's TVOE host server, login as admusr: <pre>\$ sudo ssh admusr@<redundant PMAC's TVOE Host server control IP></pre>
5 ☐	Redundant PMAC's TVOE Host: Mount the PMAC media	Mount the PMAC upgrade media from the primary PMAC server: <pre>\$ sudo /bin/mount <primary_pmac_control_IP>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name> /mnt/upgrade</pre>

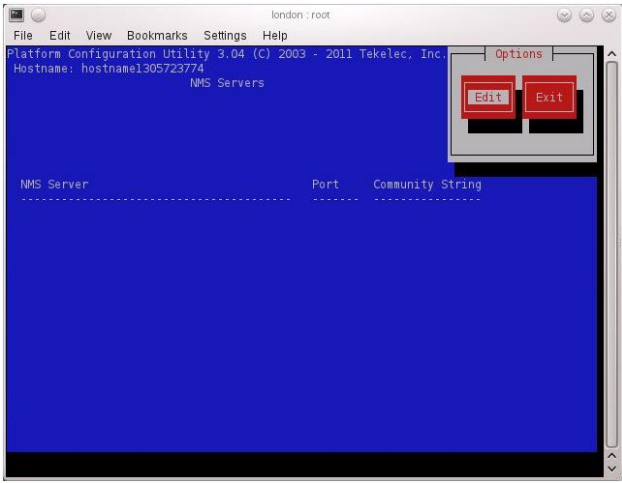
Procedure 13. Installing a Redundant PMAC

6 ☐	Redundant PMAC's TVOE Host: Deploy PMAC	Using the pmac-deploy script; deploy the PMAC instance using the configuration detailed by the completed NAPD. All configuration options (<i>NetBackup</i> or <i>isoimagesVolSizeGB</i>) should match the configuration of the primary PMAC. Reference Procedure (step 3) For this example, deploy a PMAC without NetBackup feature: <pre> \$ cd /mnt/upgrade/upgrade \$ sudo ./pmac-deploy -guest=<Redundant_PMAC_Name> --hostname=<Redundant_PMAC_Name> --controlBridge=<TVOE_Control_Bridge> --controlIP=<Redundant_PMAC_Control_ip_address> --controlNM=<PMAC_Control_netmask> --managementBridge=<PMAC_Management_Bridge> --managementIP=<Redundant_PMAC_Management_ip_address> --managementNM=<PMAC_Management_netmask_or_prefix> --routeGW=<PMAC_Management_gateway_address> --ntpserver=<Redundant_TVOE_Management_server_ip_address> </pre> The PMAC will deploy and boot. The management and control network will come up based on the settings that were provided to the pmac-deploy script.
7 ☐	Redundant PMAC's TVOE Host: Unmount Media	Unmount the media by executing the following command: <pre> \$ cd / \$ sudo /bin/umount /mnt/upgrade </pre>

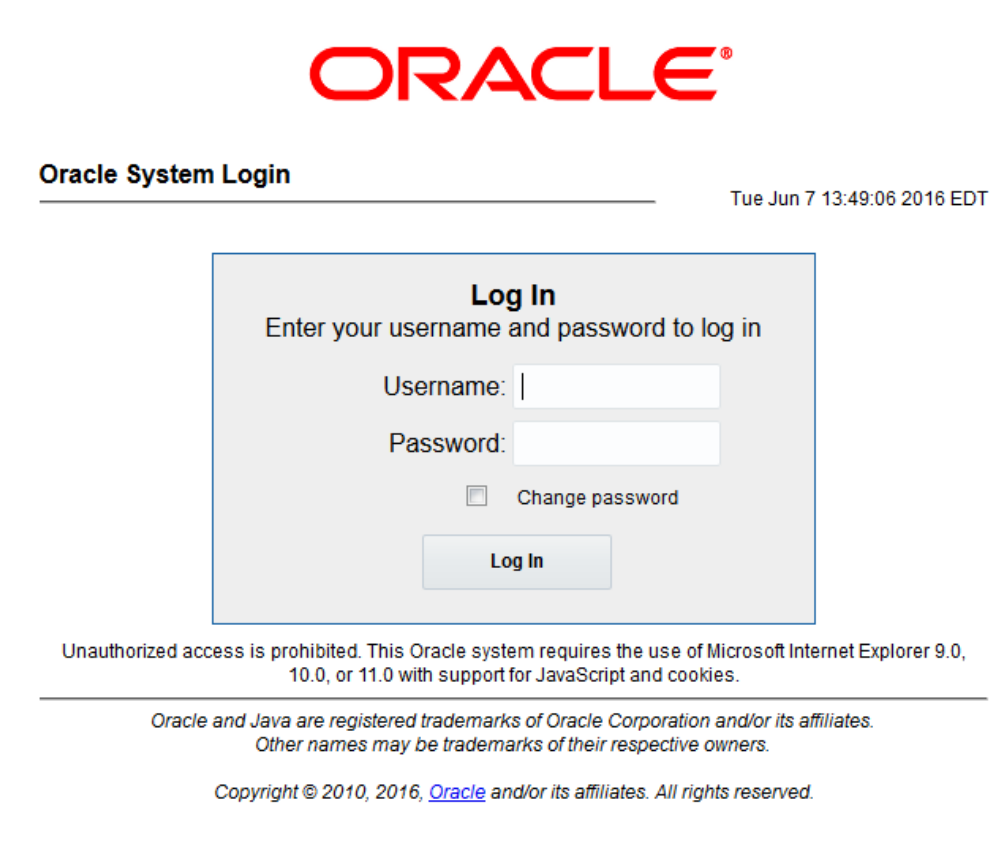
Procedure 13. Installing a Redundant PMAC

8 ☐	Redundant PMAC's TVOE Host: SSH into the Redundant PMAC Server	Using an SSH client such as putty, ssh to the TVOE host as admusr. Login using virsh, and wait until you see the login prompt : <pre>\$ sudo /usr/bin/virsh list</pre> <table border="1"> <thead> <tr> <th>Id</th> <th>Name</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>myTPD</td> <td>running</td> </tr> <tr> <td>2</td> <td>PM&C</td> <td>running</td> </tr> <tr> <td>3</td> <td>Redundant PM&C</td> <td>running</td> </tr> </tbody> </table> <pre>\$ sudo /usr/bin/virsh console <Redundant PM&C></pre> [Output Removed] <pre>Starting ntdMgr: [OK] Starting atd: [OK] 'TPD Up' notification(s) already sent: [OK] upstart: Starting tpdProvd... upstart: tpdProvd started. CentOS release 6.2 (Final) Kernel 2.6.32-220.17.1.el6prere16.0.0_80.14.0.x86_64 on an x86_64 PM&Cdev7 login:</pre>	Id	Name	State	1	myTPD	running	2	PM&C	running	3	Redundant PM&C	running
Id	Name	State												
1	myTPD	running												
2	PM&C	running												
3	Redundant PM&C	running												
9 ☐	Redundant PMAC: Verify the Redundant PMAC is configured correctly on first boot	Establish an SSH session to the redundant PMAC, login as admusr. Run the following command (there should be no output): <pre>\$ sudo /bin/ls /usr/TKLC/plat/etc/deployment.d/</pre>												
10 ☐	Redundant PMAC's TVOE Host: Error doing verification, if error is outputted	If an error was made use the following command to delete the redundant PMAC Guest and then re-deploy the guest again: <pre>\$ sudo guestMgr -remove < Redundant PMAC_Name></pre>												

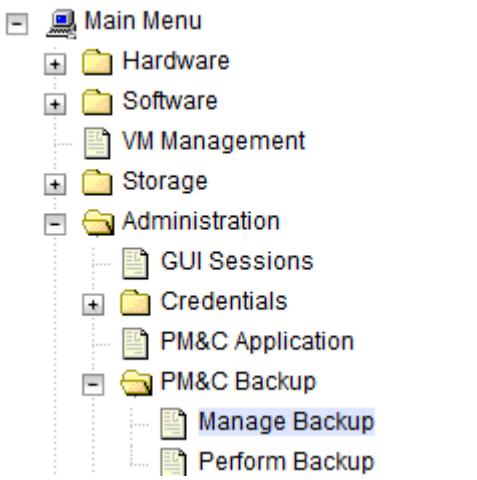
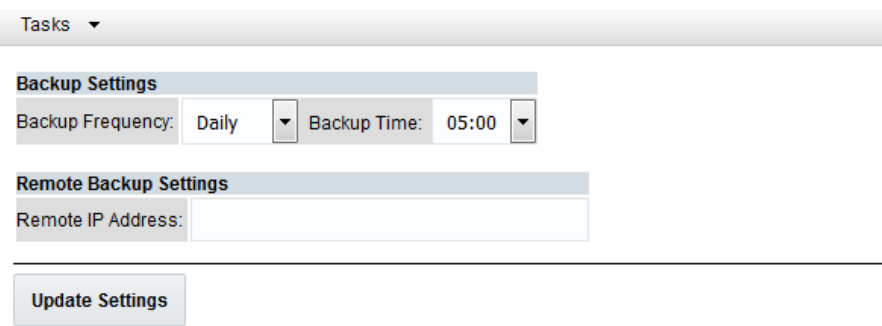
Procedure 13. Installing a Redundant PMAC

11 ☐	Redundant PMAC: Set the PMAC time zone	Determine the Time Zone to be used for the redundant PMAC Note: Valid time zones can be found in Appendix J: List of Frequently used Time Zones Run <pre>\$ sudo set_pmac_tz.pl <time zone></pre> Example: <pre>\$ sudo set_pmac_tz.pl America/New_York</pre> Verify that the time zone has been updated: <pre>\$ sudo date</pre>
12 ☐	Redundant PMAC: Set SNMP	Set SNMP by running the following: <pre>\$ sudo su - platcfg</pre> Navigate to Network Configuration -> SNMP Configuration -> NMS Configuration.  Select Edit and then choose Add a New NMS Server. The 'Add an NMS Server' page will be displayed. Complete the form by entering in all information about the SNMP trap destination. Select OK to finalize the configuration. The 'NMS Server Action Menu' will now be displayed. Select Exit. The following dialogue will then be presented. Select Yes and then wait a few seconds while the Alarm Routing Service is restarted. At that time the SNMP Configuration Menu will be presented. Exit platcfg.

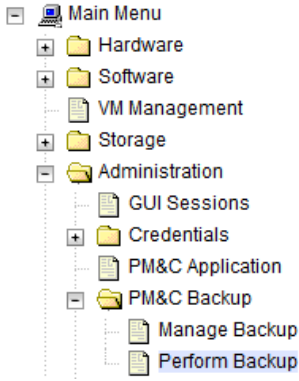
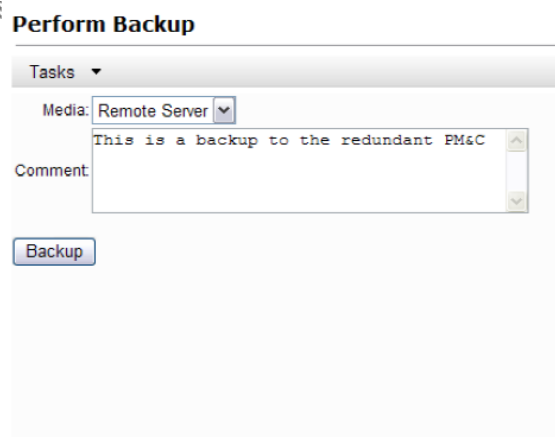
Procedure 13. Installing a Redundant PMAC

13 ☐	Redundant PMAC: Reboot the server	Reboot the server by running: \$ sudo init 6
14 ☐	PMAC GUI: Login	Open web browser and navigate to the PMAC GUI, Login as guiadmin user: https://<pmac_network_ip> 

Procedure 13. Installing a Redundant PMAC

15 ☐	PMAC GUI: Configure Backups	Navigate to Main Menu -> Administration -> PM&C Backup -> Manage Backup  Configure the primary PMAC to send backups to the redundant PMAC: On the Remote IP Address field, enter the management IP of the redundant PMAC server. Main Menu: Administration -> PM&C Backup -> Manage Backup 

Procedure 13. Installing a Redundant PMAC

16 ☐	PMAC GUI: Perform Initial Backup	Navigate to Main Menu -> Administration -> PM&C Backup -> Perform Backup  Select the <i>Remote Server</i> from the drop down Media Box, enter any desired comment and click Backup  Verify the Backup was successful by clicking on the Task Monitoring Link to monitor the Backup PMAC status. Note: This backup function copies existing PMAC backup files and all of the images added to the PMAC image repository from the primary PMAC server to the redundant PMAC Server.
17 ☐	Primary PMAC: Un-Export the PMAC ISO image	Execute the following command to Un-export the PMAC ISO image to the redundant PMAC's TVOE host Server: <pre>\$ sudo /usr/sbin/exportfs -u <redundant PMAC TVOE Host Control IP>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name></pre>

4.12 Virtual Machine/Network Fast Deployment

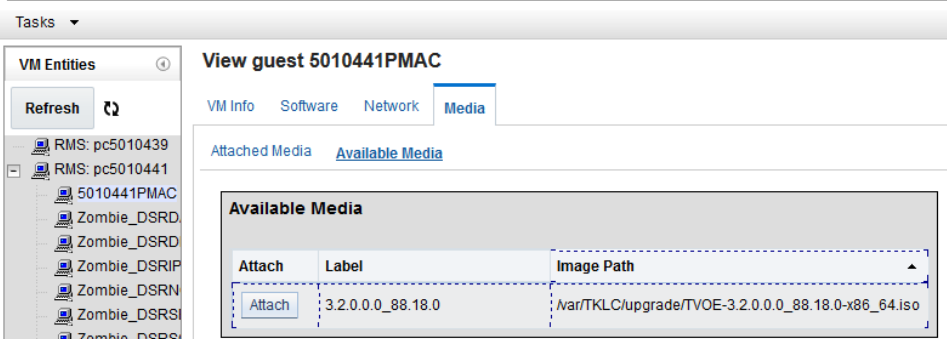
Procedure 14. Load DSR, SDS, and TPD ISOs to the PMAC Server

S T E P #	This procedure will load the DSR, SDS, and TPD ISOs into the PMAC Server. Note: If deploying IDIH, the IDIH ISOs can also be loaded here as well. Needed material: - Application Media Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	PMAC's TVOE: Load Application ISO	Add the TPD ISO image to the PMAC, this can be done in one of three ways: 1. Insert the CD containing the TPD image into the removable media drive. 2. Attach the USB device containing the ISO image to a USB port. 3. Copy the Application ISO file to the PMAC server into the “/var/TKLC/smac/image/isoimages/home/smacftpusr/” directory as pmacftpusr user: cd into the directory where your ISO image is located on the TVOE Host (not on the PMAC server) Using sftp, connect to the PMAC server <pre>\$ sftp pmacftpusr@<pmac_management_network_ip> \$ put <image>.iso</pre> After the image transfer is 100% complete, close the connection: <pre>\$ quit</pre>

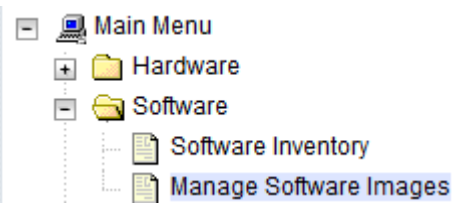
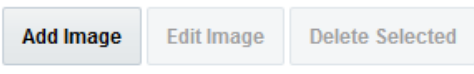
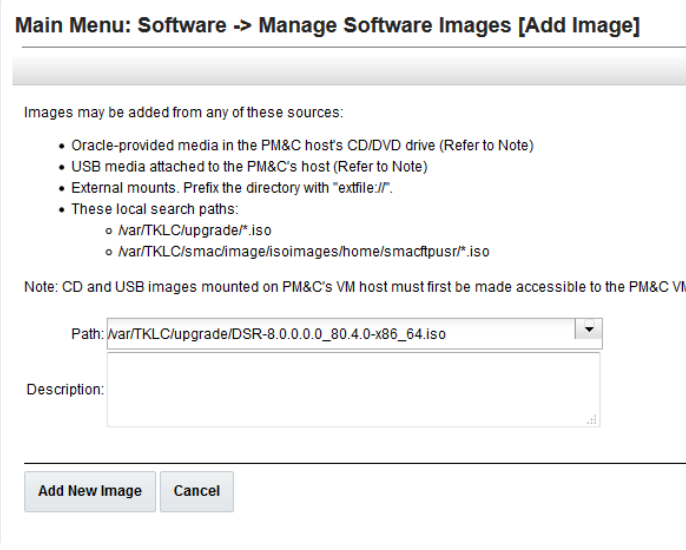
Procedure 14. Load DSR, SDS, and TPD ISOs to the PMAC Server

2 ☐	PMAC GUI: Login	Open web browser and navigate to the PMAC GUI, Login as guiadmin user: <code>https://<pmac_network_ip></code>

Procedure 14. Load DSR, SDS, and TPD ISOs to the PMAC Server

3 ☐	PMAC GUI: Attach the software Image to the PMAC Guest	If in Step 1 the ISO image was transferred directly to the PMAC guest via sftp, skip the rest of this step and continue with step 4. If the image is on a CD or USB device, continue with this step. In the PMAC GUI, navigate to Main Menu -> VM Management. In the “VM Entities” list, select the PMAC guest. On the resulting “View VM Guest” page, select the Media tab. Under the Media tab, find the ISO image in the “Available Media” list, and click its Attach button. After a pause, the image will appear in the “Attached Media” list. Main Menu: VM Management  The screenshot displays the PMAC GUI interface. On the left, the 'VM Entities' list shows a tree structure with 'RMS: pc5010439' and 'RMS: pc5010441' expanded, revealing '5010441PMAC' and several 'Zombie_DSRD' entries. The main panel is titled 'View guest 5010441PMAC' and has tabs for 'VM Info', 'Software', 'Network', and 'Media'. The 'Media' tab is active, showing 'Attached Media' and 'Available Media' sections. The 'Available Media' section contains a table with the following data: <table border="1"> <thead> <tr> <th>Attach</th> <th>Label</th> <th>Image Path</th> </tr> </thead> <tbody> <tr> <td> Attach </td> <td>3.2.0.0.0_88.18.0</td> <td>/var/TKLC/upgrade/TVOE-3.2.0.0.0_88.18.0-x86_64.iso</td> </tr> </tbody> </table>	Attach	Label	Image Path	Attach	3.2.0.0.0_88.18.0	/var/TKLC/upgrade/TVOE-3.2.0.0.0_88.18.0-x86_64.iso
Attach	Label	Image Path						
Attach	3.2.0.0.0_88.18.0	/var/TKLC/upgrade/TVOE-3.2.0.0.0_88.18.0-x86_64.iso						

Procedure 14. Load DSR, SDS, and TPD ISOs to the PMAC Server

4 ☐	PMAC GUI : Add TPD Image	Navigate to Main Menu -> Software -> Manage Software Images  Press Add Image button. Use the drop down to select the image.  If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://..."). These devices are assigned in numerical order as CD and USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the ISO image of interest is normally present on the second device, "device://dev/sr1". If one or more CD or USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number. If in Step 1 the image was transferred to PMAC via sftp it will appear in the list as a local file "/var/TKLC/...".  Select the appropriate path and Press Add New Image button. You may check the progress using the Task Monitoring link. Observe the green bar indicating success. Once the green bar is displayed, remove the TPD Media from the optical drive of the management server.

Procedure 14. Load DSR, SDS, and TPD ISOs to the PMAC Server

5 ☐	PMAC GUI: Load DSR ISO	If the DSR ISO hasn't been loaded onto the PMAC already, repeat steps 1 through 4 to load it using the DSR media or ISO.
6 ☐	PMAC GUI: Load SDS ISO	If the SDS ISO hasn't been loaded onto the PMAC already, repeat steps 1 through 4 to load it using the SDS media or ISO.

Procedure 15. Execute VM/Network Fast Deployment

STEP #	This procedure will provide the steps needed to create network bond interfaces and bridges, set TVOE host NTP servers, and create virtual machines. Prerequisite: TVOE has been installed and configured on the target RMS. Prerequisite: DSR iso has been loaded onto the PMAC. Note: Refer to Section 4.10 for VM placement Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	PMAC: Login	Establish an SSH session to the PMAC server, login as admusr .
2 ☐	PMAC: Transfer Script and Supporting Files	Copy script and supporting files from the DSR iso: <pre>\$ sudo rsync -avz --exclude cpuset.py --exclude irq tune.sh --exclude tuned_tv oe.tar /usr/TKLC/smac/html/TPD/<DSR ISO loaded previous procedure>/upgrade/overlay/RMS/ /usr/TKLC/smac/etc/RMS/</pre> Change permissions: <pre>\$ sudo chmod 777 /usr/TKLC/smac/etc/RMS/*</pre>

Procedure 15. Execute VM/Network Fast Deployment

3 □	PMAC: Edit/Update Configuration File	Change directory: <pre>\$ cd /usr/TKLC/smac/etc/RMS/</pre> Edit/Update the configuration file (<i>rms.cfg</i>) Read all notes shown below before editing the file. Note: Comment out configuration items that are not needed. Note: It is recommended that a separate configuration file be created for EACH rack mount server being deployed. Note: Cabinet ID in the config file needs to match the cabinet added in procedure 10. The following items are mandatory: • siteName • tpdIso • dsrIso (if DSR VMs are being configured) • sdsIso (if SDS VMs are being configured) • NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured) • XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured) • XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured) • DSRNOAM1XMIIPADDRESS (if DSRNOAM1 is being configured) • DSRNOAM2XMIIPADDRESS (if DSRNOAM2 is being configured) • DSRDRNOAM1XMIIPADDRESS (if DSRDRNOAM1 is being configured) • DSRDRNOAM2XMIIPADDRESS (if DSRDRNOAM2 is being configured) • SDSNOAM1XMIIPADDRESS (if SDSNOAM1 is being configured) • SDSNOAM2XMIIPADDRESS (if SDSNOAM2 is being configured) • SDSDRNOAM1XMIIPADDRESS (if SDSDRNOAM1 is being configured) • SDSDRNOAM2XMIIPADDRESS (if SDSDRNOAM2 is being configured) Note: Refer to Appendix R: VM Automation Profile Values for DSR and SDS profile values with the configuration file. Note: Comment out SDS and DSR profile items if cooresponding products are not used. Note: [Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9]: Refer to Appendix Q.3: Non-HA Lab Node VM Automation Profile Values for DSR and SDS profile values with the configuration file. Note: The VM names should not be modified in the .cfg file. The names are fixed and will be prefixed in the siteName. Note: The VM locations should not be changed from their 'RMSx' format. Each RMS should correspond with a separate Rack Mount Server. Note: The network bond interfaces are not to be changed from their 'bondx.x' format. If bond1 was previously created for segregated signaling, update the bond interface to reflect the base bond interface (i.e bond0.x or bond1.x) To receive the iso names for 'tpdIso', 'dsrIso', and 'sdsIso', execute the following command: <pre>\$ ls /var/TKLC/smac/image/repository</pre> Note: DO NOT append '.iso' to the image name.
DSR-8.0/8.1		115 February 2018

Procedure 15. Execute VM/Network Fast Deployment

4 ☐	PMAC: Rename/ Transfer config file	It is recommended that each of the above created configuration files be renamed/copied to <hostname>.cfg and transferred to an external server for disaster recovery purposes.

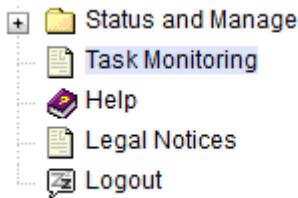
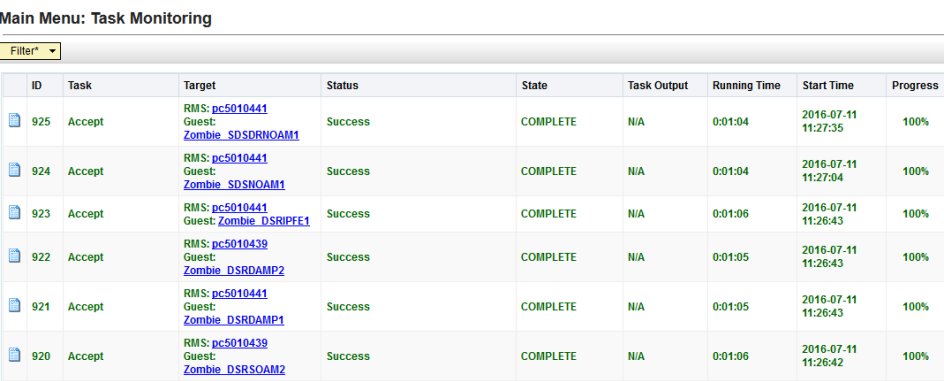
Procedure 15. Execute VM/Network Fast Deployment

5 □	PMAC: Execute the config.sh script	Execute config.sh with the config file defined above: Note: If the below command is executed on multiple cfg files, it will overwrite the existing xml file. It is recommended to rename the xml file before running the below command again. <pre>\$ sudo ./config.sh <config file> Sample Output: [admusr@5010441PMAC RMS]\$ sudo ./config.sh rms.cfg Validating cfg file... Successful validation of cfg file. Added Cabinet 101 to Fast Deployment File. Added Zombie_TVOE1 to Fast Deployment File. Added Zombie_TVOE2 to Fast Deployment File. Added xmi(bond0.4) to Fast Deployment File. Added imi(bond0.3) to Fast Deployment File. Added rep(bond1.10) to Fast Deployment File. Added xsi1(bond1.6) to Fast Deployment File. Added xsi2(bond1.7) to Fast Deployment File. Added xsi3(bond1.8) to Fast Deployment File. Added xsi4(bond1.9) to Fast Deployment File. Added xsi5(bond1.11) to Fast Deployment File. Added xsi6(bond1.12) to Fast Deployment File. Added xsi7(bond1.13) to Fast Deployment File. Added xsi8(bond1.14) to Fast Deployment File. Added xsi9(bond1.15) to Fast Deployment File. Added xsi10(bond1.16) to Fast Deployment File. Added xsi11(bond1.17) to Fast Deployment File. Added xsi12(bond1.18) to Fast Deployment File. Added xsi13(bond1.19) to Fast Deployment File. Added xsi14(bond1.20) to Fast Deployment File. Added xsi15(bond1.21) to Fast Deployment File. Added xsi16(bond1.22) to Fast Deployment File. Added Zombie_DSRNOAM1 to Fast Deployment File. Added Zombie_DSRNOAM2 to Fast Deployment File. Added Zombie_DSRDRNOAM1 to Fast Deployment File. Added Zombie_DSRDRNOAM2 to Fast Deployment File. Added Zombie_SDSNOAM1 to Fast Deployment File. Added Zombie_SDSNOAM2 to Fast Deployment File. Added Zombie_SDSRNOAM1 to Fast Deployment File. Added Zombie_SDSRNOAM2 to Fast Deployment File. Added Zombie_DSRSOAM1 to Fast Deployment File. Added Zombie_DSRSOAM2 to Fast Deployment File. Added Zombie_SDSOAM1 to Fast Deployment File. Added Zombie_SDSOAM2 to Fast Deployment File. Added Zombie_DSRDAMP1 to Fast Deployment File. Added Zombie_DSRDAMP2 to Fast Deployment File. Added Zombie_DSRIPFE1 to Fast Deployment File. Added Zombie_DSRIPFE2 to Fast Deployment File. Added Zombie_SSDPSV1 to Fast Deployment File. Added Zombie_SSDPSV2 to Fast Deployment File. Validating Fast Deployment File..... Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml" Configuration file validation successful. Validation complete Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml SUCCESS: OPERATION SUCCESS!! [admusr@5010441PMAC RMS]\$</pre>

Procedure 15. Execute VM/Network Fast Deployment

6 ☐	PMAC: Execute Fast Deployment	With the file generated from the config.sh script, execute the following command to start fast deployment: <pre>\$ screen \$ sudo fdconfig config --file=<fd_config.xml></pre> Note: This is a long duration command. If the screen command was run prior to executing the fdconfig, perform a “<i>screen -dr</i>” to resume the screen session in the event of a terminal timeout etc.

Procedure 15. Execute VM/Network Fast Deployment

7 ☐	PMAC GUI: Monitor the Configuration	If not already done so, establish a GUI session on the PMAC server. Navigate to Main Menu -> Task Monitoring  Monitor the configuration to completion: Main Menu: Task Monitoring  Note: Should a failure occur with fdconfig, logs can be accessed in /var/TKLC/log/fdconfig/fdconfig.log <pre>[admusr@melbourne-pmac-1 fdconfig]\$ sudo fdconfig dumpsteps -- file=deploy_melbourne_20170329T202458_701b.fdcdb Dump Steps in file: "deploy_melbourne_20170329T202458_701b.fdcdb" Here are the steps that were generated ----- begin ----- Dump of DB steps: NUM PHS DLY INFRA ID SVRTYPE CMD ELEMENT PRE STATE TO BGTS COMMAND TEXT ----- 1 1 0 pmac Fast_Deployment 0 21 0 Complete 300 0 Check PM&C is available 2 1 0 pmac Fast_Deployment 0 1 1 1 Skipped 300 0 Add Cabinet 3 1 0 pmac Fast_Deployment 0 3 melbourne_RMS3 1 Skipped 900 0 Add Rms 4 2 0 pmac Fast_Deployment 1 Run Below command to restart the fdconfig after a failure has occurred and has been resolved:</pre> <pre>\$ sudo fdconfig restart -- file=deploy_melbourne_20170329T202458_701b.fdcdb</pre>

Procedure 15. Execute VM/Network Fast Deployment

8 ☐	PMAC: Repeat for each Rack mount server configuration file	Repeat steps 4-7 for each rack mount server/configuration file created from step 3
9 ☐	PMAC Server: Backup FDC file	Create the fdcc directory so that the fdcc file is backed up by PMAC: Issue the following commands: Create the fdcc backup directory: <pre>\$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/fdcc</pre> Change permissions: <pre>\$ sudo chmod 777 /usr/TKLC/smac/etc/fdcc</pre> Copy the fdcc file to the fdcc backup directory: Note: The fdcc file referring here is the rms.cfg file. <pre>\$ sudo cp /usr/TKLC/smac/etc/RMS/<fdcc_file> /usr/TKLC/smac/etc/fdcc/</pre> Note: Rename it to <hostname>.cfg to identify the correct fdcc file during disaster recovery procedure. <pre>\$ sudo mv /usr/TKLC/smac/etc/fdcc/<fdcc_file> /usr/TKLC/smac/etc/fdcc/<hostname.cfg></pre>

4.13 CPU Pinning

Note: Skip this section if deploying a **Non-HA** Lab Node of DL380 Gen system

Note: HP DL380 Gen8 Skip this step

Procedure 16. CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)

S T E P #	This procedure describes steps needed to configure VM CPU socket pinning on each TVOE host to optimize performance. Prerequisite: VM Guests creation has been completed. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Obtain CPU Socket Pinning Information	Obtain CPU socket pinning information by referring to the data gathered in Section 4.10 Note: For HP DL380 Gen9 equipped with 1Gbps NICs, obtain the CPU socket pinning information from Appendix S: VM placement in HP DL380 Gen8/Gen9 (Onboard 1Gbps NICs) and CPU Pinning in HP DL380 Gen9 (Onboard 1Gbps NICs)
2 ☐	TVOE Host: Login	Establish an SSH session to the TVOE host, login as <i>admusr</i>.

Procedure 16. CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)

3 	TVOE Host: Execute the CPU Pinning Script	Execute the following commands to allocate CPU sets for EACH (including the PMAC(s)) VM configured: <pre>\$ cd /var/TKLC/upgrade</pre> Print the current CPU pinning allocations: <pre>\$ sudo ./cpuset.py --show</pre> Expected output: <pre>[admusr@Discovery-TVOE-4 ~]\$ sudo ./cpuset.py --show VM Domain Name vcpus cpuset numa state ----- Discovery-IPFEA2 4 None None running Discovery-DAMP9 12 None None running Discovery-DAMP8 12 None None running Discovery-DAMP12 12 None None running Discovery-DAMP11 12 None None running NUMA node 0 Free CPUs: count = 32 [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53] NUMA node 1 Free CPUs: count = 36 [18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71]</pre> Execute the following to allocate CPU pinning on EACH VM: <pre>\$ sudo ./cpuset.py --set=<VM Name> --numa=<0/1></pre> Example: <pre>[admusr@Discovery-TVOE-4 ~]\$ sudo ./cpuset.py -set=Discovery-IPFEA2 -numa=0 Successful. Domain Discovery-IPFEA2 must be restarted for changes to take affect [admusr@Discovery-TVOE-4 ~]\$ sudo ./cpuset.py --show VM Domain Name vcpus cpuset numa state ----- Discovery-IPFEA2 4 2-3,38-39 0 running Discovery-DAMP9 12 None None running Discovery-DAMP8 12 None None running Discovery-DAMP12 12 None None running Discovery-DAMP11 12 None None running NUMA node 0 Free CPUs: count = 28 [4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53] NUMA node 1 Free CPUs: count = 36 [18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71]</pre> Note: If deploying IDIH, make note of the CPU pinning allocations, as the CPU pinning will be done as part of IDIH configuration (Section 4.16) Note: To clear pinning, execute the following guest on EACH VM as necessary: <pre>\$ sudo ./cpuset.py --clear=<VM NAME></pre> Example: <pre>[admusr@Sterling-TVOE-4 admusr]# sudo ./cpuset.py -clear=Sterling2So-DA-MP4</pre>

Procedure 16. CPU Pinning (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)

4 ☐	TVOE Host: Restart	Restart the TVOE host by executing the following command: \$ sudo init 6
5 ☐	TVOE Host: Verify CPU Pinning	Once the TVOE host is restarted, establish an SSH session to the TVOE Host, login as admusr . Verify the CPU pinning is allocated by executing the following commands: \$ cd /var/TKLC/upgrade Print the current CPU pinning allocations: \$ sudo ./cpuset.py --show Expected output: [admusr@Discovery-TVOE-4 ~]\$ sudo ./cpuset.py -set=Discovery-DAMP8 -cpuset=4-9,40-45 Successful. Domain Discovery-DAMP8 must be restarted for changes to take affect [admusr@Discovery-TVOE-4 ~]\$ sudo ./cpuset.py --show VM Domain Name vcpus cpuset numa state ----- Discovery-IPFEA2 4 2-3,38-39 0 running Discovery-DAMP9 12 18-23,54-59 1 running Discovery-DAMP8 12 4-9,40-45 0 running Discovery-DAMP12 12 None None running Discovery-DAMP11 12 None None running NUMA node 0 Free CPUs: count = 16 [10, 11, 12, 13, 14, 15, 16, 17, 46, 47, 48, 49, 50, 51, 52, 53] NUMA node 1 Free CPUs: count = 24 [24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71]
6 ☐	Repeat for Each TVOE HOST	Repeat this procedure for each TVOE host.

4.14 Application Configuration: DSR

4.14.1 DSR Configuration: NOAMs

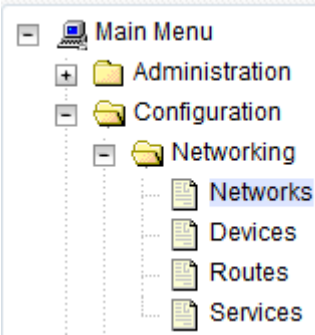
Procedure 17. Configure First NOAM NE and Server

S T E P #	This procedure will provide the steps to configure the First NOAM server. Note: SDS NOAM configuration only applicable on Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	Save the NOAM Network Data to an XML file Using a text editor, create a NOAM Network Element file that describes the networking of the target install environment of your first NOAM server. Select an appropriate file name and save the file to a known location on your computer. A suggested filename format is “Appname_Nename_NetworkElement.XML”, so for example a DSR2 NOAM network element XML file would have a filename “DSR2_NOAM_NetworkElement.xml”. Alternatively, you can update the sample DSR Network Element file. It can be found on the management server at: <pre>/usr/TKLC/smac/html/TPD/<DSR Release>/upgrade/overlay/SAMPLE-NetworkElement.xml</pre> A sample XML file can also be found in Appendix L: Sample Network Element. Note: The following limitations apply when specifying a Network Element name: A 1-32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.

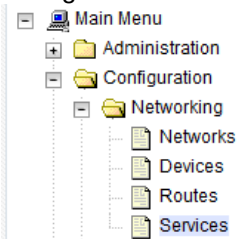
Procedure 17. Configure First NOAM NE and Server

2 ☐	NOAM GUI: Login	Using the xmi IP address defined and configured in the DSR fast deployment configuration file (rms.cfg). Login to the NOAM GUI as the <i>guiadmin</i> user:

Procedure 17. Configure First NOAM NE and Server

5 ☐	Create the NOAM Network Element using the XML File	Navigate to Main Menu->Networking -> Networks  Select the Browse button, and enter the pathname of the NOAM network XML file: To create a new Network Element, upload a valid configuration file: Browse... zombie.xml Upload File Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved. Select the Upload File button to upload the XML file and configure the NOAM Network Element. Once the data has been uploaded, you should see a tab appear with the name of your network element. Click on this tab and you will get a window which describes the individual networks that are now configured: Main Menu: Configuration -> Networking -> Networks info* Global ZombieNOAM ⓘ <table border="1"> <thead> <tr> <th>Network Name</th> <th>Network Type</th> <th>Default</th> <th>Locked</th> <th>Routed</th> <th>VLAN</th> <th>Configured Interfaces</th> <th>Network</th> </tr> </thead> <tbody> <tr> <td>XMI</td> <td>OAM</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>4</td> <td>0</td> <td>10.240.213.0/24</td> </tr> <tr> <td>IMI</td> <td>OAM</td> <td>No</td> <td>Yes</td> <td>No</td> <td>3</td> <td>0</td> <td>169.254.1.0/24</td> </tr> </tbody> </table>	Network Name	Network Type	Default	Locked	Routed	VLAN	Configured Interfaces	Network	XMI	OAM	Yes	Yes	Yes	4	0	10.240.213.0/24	IMI	OAM	No	Yes	No	3	0	169.254.1.0/24
Network Name	Network Type	Default	Locked	Routed	VLAN	Configured Interfaces	Network																			
XMI	OAM	Yes	Yes	Yes	4	0	10.240.213.0/24																			
IMI	OAM	No	Yes	No	3	0	169.254.1.0/24																			

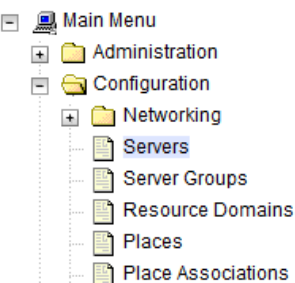
Procedure 17. Configure First NOAM NE and Server

6 ☐	Map Services to Networks	Navigate to Main Menu -> Networking -> Services.  Select the Edit button and set the Services as shown in the table below: <table border="1"> <thead> <tr> <th>Name</th> <th>Intra-NE Network</th> <th>Inter-NE Network</th> </tr> </thead> <tbody> <tr> <td>OAM</td> <td><IMI Network></td> <td><XMI Network></td> </tr> <tr> <td>Replication</td> <td><IMI Network></td> <td><XMI Network></td> </tr> <tr> <td>Signaling</td> <td>Unspecified</td> <td>Unspecified</td> </tr> <tr> <td>HA_Secondary</td> <td>Unspecified</td> <td>Unspecified</td> </tr> <tr> <td>HA_MP_Secondary</td> <td>Unspecified</td> <td>Unspecified</td> </tr> <tr> <td>Replication_MP</td> <td><IMI Network></td> <td>Unspecified</td> </tr> <tr> <td>ComAgent</td> <td><IMI Network></td> <td>Unspecified</td> </tr> </tbody> </table> For example, if your IMI network is named IMI and your XMI network is named XMI, then your services should config should look like the following: <table border="1"> <thead> <tr> <th>Name</th> <th>Intra-NE Network</th> <th>Inter-NE Network</th> </tr> </thead> <tbody> <tr> <td>OAM</td> <td>INTERNALIMI</td> <td>INTERNALXMI</td> </tr> <tr> <td>Replication</td> <td>INTERNALIMI</td> <td>INTERNALXMI</td> </tr> <tr> <td>Signaling</td> <td>Unspecified</td> <td>Unspecified</td> </tr> <tr> <td>HA_Secondary</td> <td>Unspecified</td> <td>Unspecified</td> </tr> <tr> <td>HA_MP_Secondary</td> <td>Unspecified</td> <td>Unspecified</td> </tr> <tr> <td>Replication_MP</td> <td>INTERNALIMI</td> <td>Unspecified</td> </tr> <tr> <td>ComAgent</td> <td>INTERNALIMI</td> <td>Unspecified</td> </tr> </tbody> </table> Select the Ok button to apply the Service-to-Network selections. Click OK at the pop up dialog:	Name	Intra-NE Network	Inter-NE Network	OAM	<IMI Network>	<XMI Network>	Replication	<IMI Network>	<XMI Network>	Signaling	Unspecified	Unspecified	HA_Secondary	Unspecified	Unspecified	HA_MP_Secondary	Unspecified	Unspecified	Replication_MP	<IMI Network>	Unspecified	ComAgent	<IMI Network>	Unspecified	Name	Intra-NE Network	Inter-NE Network	OAM	INTERNALIMI	INTERNALXMI	Replication	INTERNALIMI	INTERNALXMI	Signaling	Unspecified	Unspecified	HA_Secondary	Unspecified	Unspecified	HA_MP_Secondary	Unspecified	Unspecified	Replication_MP	INTERNALIMI	Unspecified	ComAgent	INTERNALIMI	Unspecified
Name	Intra-NE Network	Inter-NE Network																																																
OAM	<IMI Network>	<XMI Network>																																																
Replication	<IMI Network>	<XMI Network>																																																
Signaling	Unspecified	Unspecified																																																
HA_Secondary	Unspecified	Unspecified																																																
HA_MP_Secondary	Unspecified	Unspecified																																																
Replication_MP	<IMI Network>	Unspecified																																																
ComAgent	<IMI Network>	Unspecified																																																
Name	Intra-NE Network	Inter-NE Network																																																
OAM	INTERNALIMI	INTERNALXMI																																																
Replication	INTERNALIMI	INTERNALXMI																																																
Signaling	Unspecified	Unspecified																																																
HA_Secondary	Unspecified	Unspecified																																																
HA_MP_Secondary	Unspecified	Unspecified																																																
Replication_MP	INTERNALIMI	Unspecified																																																
ComAgent	INTERNALIMI	Unspecified																																																

Procedure 17. Configure First NOAM NE and Server

7 ☐	Insert the 1st NOAM server	Navigate to Main Menu -> Configuration -> Servers. Select the Insert button to insert the new NOAM server into servers table. Fill in the fields as follows: Hostname: <Hostname> Role: NETWORK OAM&P System ID: <Site System ID> Hardware Profile: DSR TVOE Guest Network Element Name: [Choose NE from Drop Down Box] Location: <NOAM Server Location> <table border="1"> <tr> <td>Role *</td> <td>NETWORK OAM&P ▼</td> </tr> <tr> <td>System ID</td> <td> </td> </tr> <tr> <td>Hardware Profile</td> <td>DSR TVOE Guest ▼</td> </tr> <tr> <td>Network Element Name *</td> <td>ZombieNOAM ▼</td> </tr> <tr> <td>Location</td> <td>pc5010441</td> </tr> </table> The network interface fields will now become available with selection choices based on the chosen hardware profile and network element Fill in the server IP addresses for the XMI network. Select xmi for the interface. Leave the “VLAN” checkbox unchecked. Fill in the server IP addresses for the IMI network. Select imi for the interface. Leave the “VLAN” checkbox unchecked. <table border="1"> <tr> <td>XMI (10.240.213.0/24)</td> <td> 10.240.213.2 </td> <td>xmi ▼</td> <td>☐ VLAN (4)</td> </tr> <tr> <td>IMI (169.254.1.0/24)</td> <td> 169.254.1.2 </td> <td>imi ▼</td> <td>☐ VLAN (3)</td> </tr> </table> Next, add the following NTP servers: <table border="1"> <thead> <tr> <th>NTP Server</th> <th>Preferred?</th> </tr> </thead> <tbody> <tr> <td><1st-NOAM-TVOE-IP-Address></td> <td>Yes</td> </tr> </tbody> </table> NTP Servers: <table border="1"> <thead> <tr> <th>NTP Server IP Address</th> <th>Prefer</th> <th></th> </tr> </thead> <tbody> <tr> <td> 10.240.214.2 </td> <td>☒</td> <td> Add Remove </td> </tr> </tbody> </table> Select the Ok button when you have completed entering all the server data.	Role *	NETWORK OAM&P ▼	System ID		Hardware Profile	DSR TVOE Guest ▼	Network Element Name *	ZombieNOAM ▼	Location	pc5010441	XMI (10.240.213.0/24)	10.240.213.2	xmi ▼	☐ VLAN (4)	IMI (169.254.1.0/24)	169.254.1.2	imi ▼	☐ VLAN (3)	NTP Server	Preferred?	<1st-NOAM-TVOE-IP-Address>	Yes	NTP Server IP Address	Prefer		10.240.214.2	☒	Add Remove
Role *	NETWORK OAM&P ▼																													
System ID																														
Hardware Profile	DSR TVOE Guest ▼																													
Network Element Name *	ZombieNOAM ▼																													
Location	pc5010441																													
XMI (10.240.213.0/24)	10.240.213.2	xmi ▼	☐ VLAN (4)																											
IMI (169.254.1.0/24)	169.254.1.2	imi ▼	☐ VLAN (3)																											
NTP Server	Preferred?																													
<1st-NOAM-TVOE-IP-Address>	Yes																													
NTP Server IP Address	Prefer																													
10.240.214.2	☒	Add Remove																												

Procedure 17. Configure First NOAM NE and Server

8 ☐	Export the Initial Configuration	Navigate to Main Menu -> Configuration -> Servers.  From the GUI screen, select the NOAM server and then select Export to generate the initial configuration data for that server. 
9 ☐	NOAM iLO: Copy Configuration File to 1 st NOAM Server	Using the xmi IP address defined and configured in the DSR fast deployment configuration file (rms.cfg). Establish an SSH session to the 1st NOAM server, logging in as the admusr user. Copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the 1st NOAM to the /var/tmp directory. The configuration file will have a filename like TKLCConfigData.<hostname>.sh. The following is an example: <pre data-bbox="467 1146 1360 1247">\$ sudo cp /var/TKLC/db/filemgmt/TKLCConfigData.RMS01.sh /var/tmp/TKLCConfigData.sh</pre> Note: The file in /var/tmp/ directory MUST be <i>TKLCConfigData.sh</i>
10 ☐	NOAM iLO: Wait for Configuration to Complete	The automatic configuration daemon will look for the file named <i>“TKLCConfigData.sh”</i> in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server. Wait to be prompted to reboot the server, but DO NOT reboot the server, it will be rebooted later on in this procedure. Note: Ignore the warning about removing the USB key, since no USB key is present.

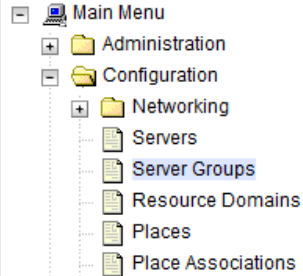
Procedure 17. Configure First NOAM NE and Server

11 ☐	NOAM iLO: Set the Time zone and Reboot the Server	From the command line prompt, execute set_ini_tz.pl. This will set the system time zone. The following command example uses the America/New_York time zone. Replace as appropriate with the time zone you have selected for this installation. For a full list of valid time zones, see Appendix J: List of Frequently used Time Zones. <pre>\$ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York"</pre> <pre>\$ sudo init 6</pre>
12 ☐	1st NOAM Server: Verify Server Health	Execute the following command on the 1st NOAM server and make sure that no errors are returned: <pre>\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

Procedure 18. Configure the NOAM Server Group

S T E P #	This procedure will provide the steps to configure the NOAM server group. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	NOAM GUI: Login Establish a GUI session on the first NOAM server by using the XMI IP address. Open the web browser and enter a URL of < NO1_XMI_IP_Address > Login as the <i>guiadmin</i> user:  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.

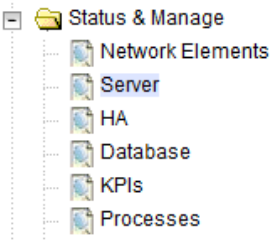
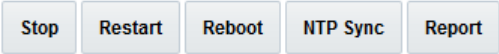
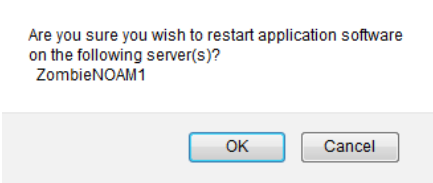
Procedure 18. Configure the NOAM Server Group

2 ☐	NOAM GUI: Enter NOAM Server Group Data	Navigate to Main Menu -> Configuration -> Server Groups  Select Insert and fill the following fields: Insert Edit Delete Report • Server Group Name: <Enter Server Group Name> • Level: A • Parent : None • Function: DSR (Active/Standby Pair) • WAN Replication Connection Count: Use Default Value Adding new server group <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Desc</th> </tr> </thead> <tbody> <tr> <td>Server Group Name *</td> <td> ZombieNOAM </td> <td>Uniqu requir</td> </tr> <tr> <td>Level *</td> <td> A ▼</td> <td>Selec</td> </tr> <tr> <td>Parent *</td> <td> NONE ▼</td> <td>Selec</td> </tr> <tr> <td>Function *</td> <td> DSR (active/standby pair) ▼</td> <td>Selec</td> </tr> <tr> <td>WAN Replication Connection Count</td> <td> 1 </td> <td>Speci</td> </tr> </tbody> </table> Ok Apply Cancel Select OK when all fields are filled in.	Field	Value	Desc	Server Group Name *	ZombieNOAM	Uniqu requir	Level *	A ▼	Selec	Parent *	NONE ▼	Selec	Function *	DSR (active/standby pair) ▼	Selec	WAN Replication Connection Count	1	Speci
Field	Value	Desc																		
Server Group Name *	ZombieNOAM	Uniqu requir																		
Level *	A ▼	Selec																		
Parent *	NONE ▼	Selec																		
Function *	DSR (active/standby pair) ▼	Selec																		
WAN Replication Connection Count	1	Speci																		

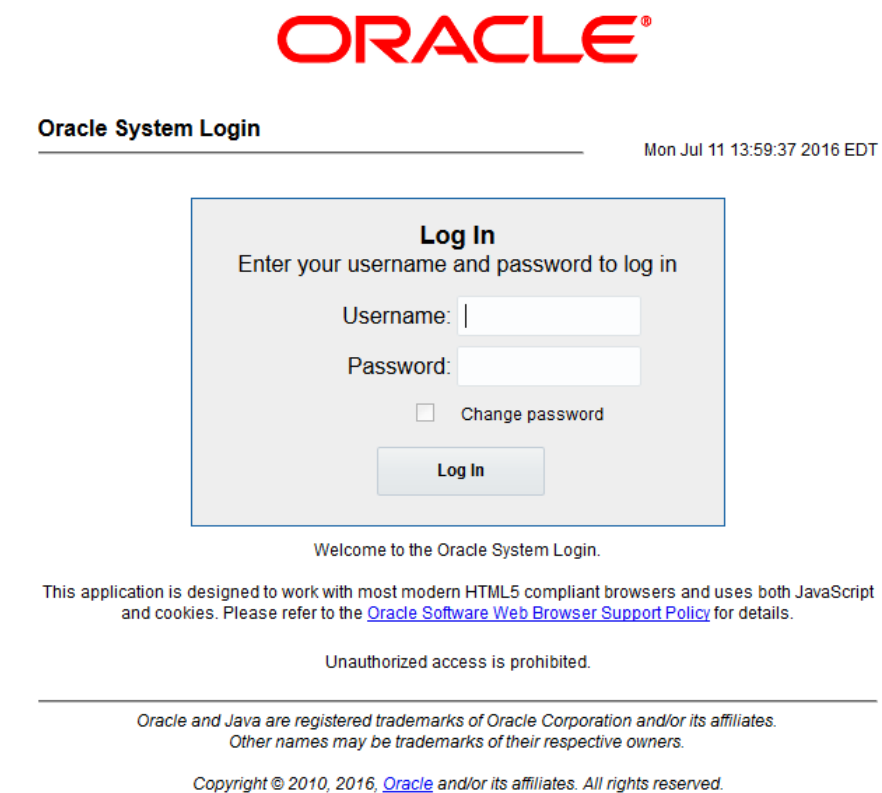
Procedure 18. Configure the NOAM Server Group

3 ☐	NOAM GUI: Edit the NOAM Server Group	From the GUI Main Menu -> Configuration -> Server Groups. Select the new server group, and then select Edit Insert Edit Delete Report Select the Network Element that represents the NOAM. <table border="1" data-bbox="467 546 1208 657"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> </tbody> </table> In the portion of the screen that lists the servers for the server group, find the NOAM server being configured. Click the Include in SG checkbox. Leave other boxes blank. Press OK Ok Apply Cancel	Server	SG Inclusion	Preferred HA Role	ZombieNOAM1	☒ Include in SG	☐ Prefer server as spare
Server	SG Inclusion	Preferred HA Role						
ZombieNOAM1	☒ Include in SG	☐ Prefer server as spare						
4 ☐	NOAM: Verify NOAM server role	From terminal window of the first NOAM server, execute the following command: <pre>\$ha.mystate</pre> Verify that the DbReplication and VIP item under the resourceId column has a value of Active under the role column. You might have to wait a few minutes for it to become in that state. Example: <pre data-bbox="456 1377 1338 1591">[admsr@ZombieNOAM1 ~]\$ ha.mystate resourceId role node DC subResources lastUpdate ----- DbReplication Act/Act A0630.238 * 0 0713:105006.861 VIP Act/Act A0630.238 * 0 0713:105006.862 CacdProcessRes Act/OOS A0630.238 * 0 0713:105006.861 CAPM_HELP_Proc Act/OOS A0630.238 * 0 0713:105006.816 DSROAM_Proc Act/OOS A0630.238 * 0 0713:105011.916 CAPM_PSFS_Proc Act/Act A0630.238 * 0 0713:105012.017</pre>						

Procedure 18. Configure the NOAM Server Group

5 ☐	NOAM GUI: Restart 1 st NOAM Server	From the NOAM GUI. Navigate to Main menu -> Status & Manage -> Server  Select the first NOAM server. Select the Restart button.  Answer OK to the confirmation popup.  Wait for restart to complete.

Procedure 19. Configure the Second NOAM Server

S T E P #	This procedure will provide the steps to configure the Second NOAM server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	NOAM GUI: Login	Establish a GUI session on the first NOAM server by using the XMI IP address. Open the web browser and enter a URL of < NO1_XMI_IP_Address > Login as the guiadmin user: 

Procedure 19. Configure the Second NOAM Server

2 ☐	NOAM GUI: Insert the 2 nd NOAM server	Navigate to Main Menu -> Configuration -> Servers. Fill in the fields as follows: Hostname: <Hostname> Role: NETWORK OAM&P System ID: <Site System ID> Hardware Profile: DSR TVOE Guest Network Element Name: [Choose NE from Drop Down Box] Location: <NOAM Server Location> <table border="1"> <tr> <td>Hostname *</td> <td>ZombieNOAM2</td> </tr> <tr> <td>Role *</td> <td>NETWORK OAM&P ▼</td> </tr> <tr> <td>System ID</td> <td></td> </tr> <tr> <td>Hardware Profile</td> <td>DSR TVOE Guest ▼</td> </tr> <tr> <td>Network Element Name *</td> <td>ZombieNOAM ▼</td> </tr> <tr> <td>Location</td> <td>pc5010439</td> </tr> </table> The network interface fields will now become available with selection choices based on the chosen hardware profile and network element Fill in the server IP addresses for the XMI network. Select xmi for the interface. Leave the “VLAN” checkbox unchecked. Fill in the server IP addresses for the IMI network. Select imi for the interface. Leave the “VLAN” checkbox unchecked. <table border="1"> <tr> <td>XMI (10.240.213.0/24)</td> <td>10.240.213.3</td> <td>xmi ▼</td> <td>☐ VLAN (4)</td> </tr> <tr> <td>IMI (169.254.1.0/24)</td> <td>169.254.1.3</td> <td>imi ▼</td> <td>☐ VLAN (3)</td> </tr> </table> Next, add the following NTP servers: <table border="1"> <thead> <tr> <th>NTP Server</th> <th>Preferred?</th> </tr> </thead> <tbody> <tr> <td><2nd-NOAM-TVOE-IP-Address></td> <td>Yes</td> </tr> </tbody> </table> NTP Servers: <table border="1"> <thead> <tr> <th>NTP Server IP Address</th> <th>Prefer</th> <th></th> </tr> </thead> <tbody> <tr> <td>10.240.214.4</td> <td>☒</td> <td> Add Remove </td> </tr> </tbody> </table> Select the Ok button when you have completed entering all the server data.	Hostname *	ZombieNOAM2	Role *	NETWORK OAM&P ▼	System ID		Hardware Profile	DSR TVOE Guest ▼	Network Element Name *	ZombieNOAM ▼	Location	pc5010439	XMI (10.240.213.0/24)	10.240.213.3	xmi ▼	☐ VLAN (4)	IMI (169.254.1.0/24)	169.254.1.3	imi ▼	☐ VLAN (3)	NTP Server	Preferred?	<2nd-NOAM-TVOE-IP-Address>	Yes	NTP Server IP Address	Prefer		10.240.214.4	☒	Add Remove
Hostname *	ZombieNOAM2																															
Role *	NETWORK OAM&P ▼																															
System ID																																
Hardware Profile	DSR TVOE Guest ▼																															
Network Element Name *	ZombieNOAM ▼																															
Location	pc5010439																															
XMI (10.240.213.0/24)	10.240.213.3	xmi ▼	☐ VLAN (4)																													
IMI (169.254.1.0/24)	169.254.1.3	imi ▼	☐ VLAN (3)																													
NTP Server	Preferred?																															
<2nd-NOAM-TVOE-IP-Address>	Yes																															
NTP Server IP Address	Prefer																															
10.240.214.4	☒	Add Remove																														

Procedure 19. Configure the Second NOAM Server

3 ☐	NOAM GUI: Export the Initial Configuration	Navigate to Main Menu -> Configuration -> Servers. From the GUI screen, select the 2nd NOAM server and then select Export to generate the initial configuration data for that server.
4 ☐	1st NOAM Server: Copy Configuration File to 2 nd NOAM Server	Obtain a terminal session to the 1st NOAM as the admusr user. Execute the following command to configure the 2nd NOAM server: <pre>\$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<NOAM2_Hostname>.sh admusr@<NOAM2_xmi_IP_address>:/var/tmp/TKLCConfigData.sh</pre>
5 ☐	2nd NOAM Server: Verify server configuration and Reboot the Server	Obtain a terminal window connection on the 2nd NOAM. Login as the admusr user. The automatic configuration daemon will look for the file named “TKLCConfigData.sh” in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server. Verify server configuration was called by checking the following file <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> Verify no errors are present and that the following message is displayed: <pre>[SUCCESS] script completed successfully!</pre> Note: The script may return success even when errors are reported in the log file. Go through the entire install.log file to verify no errors are present. Now Reboot the Server: <pre>\$ sudo init 6</pre> Wait for the server to reboot

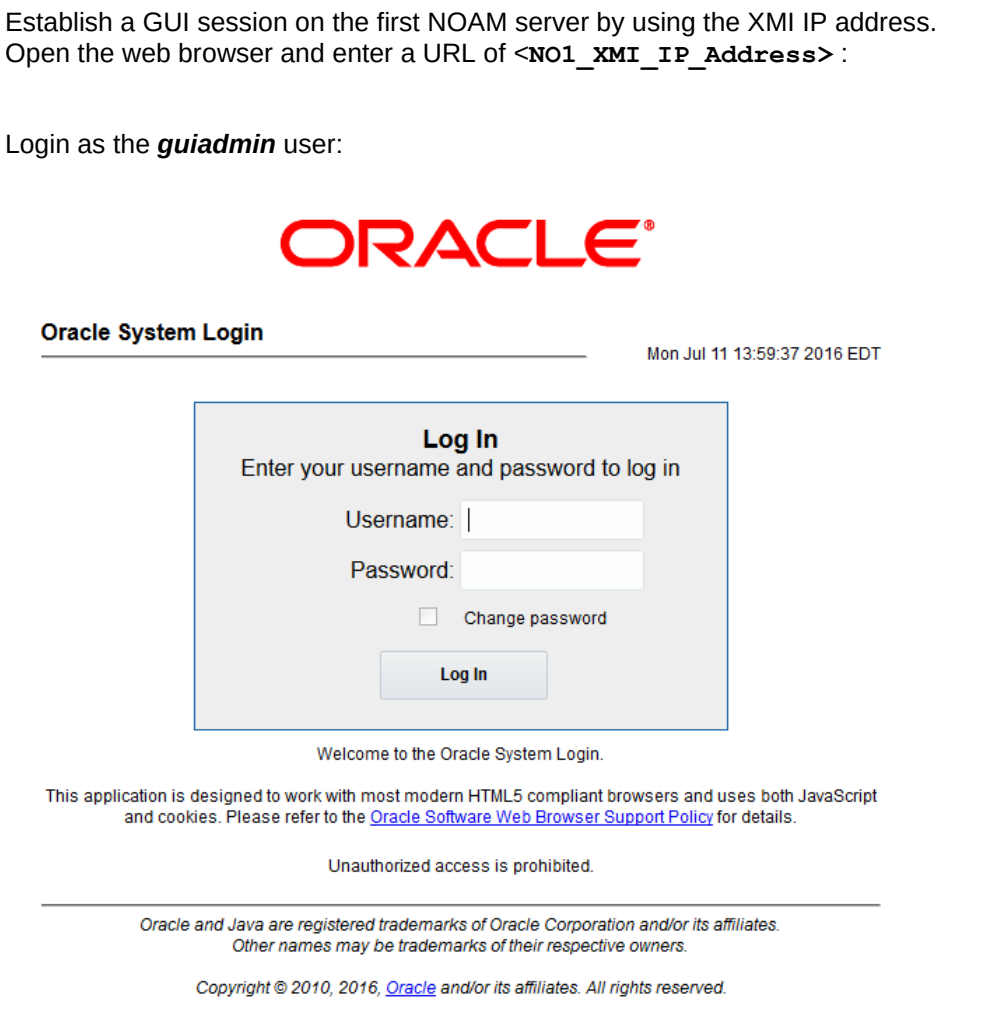
Procedure 19. Configure the Second NOAM Server

6 ☐	2nd NOAM Server: Verify Server Health	Execute the following command on the 2nd NOAM server and make sure that no errors are returned: <pre>\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

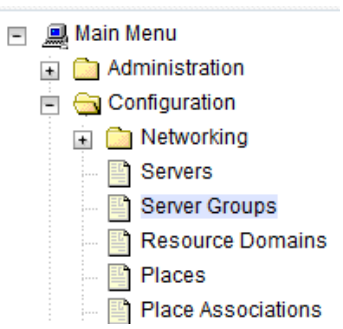
Procedure 20. Complete NOAM Server Group Configuration

STEP #	This procedure will provide the steps to finish configuring the NOAM server group. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

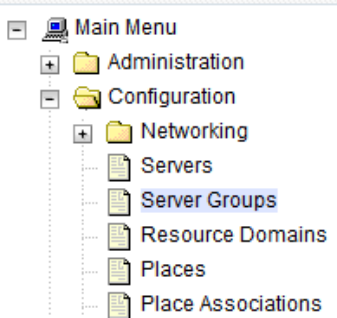
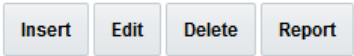
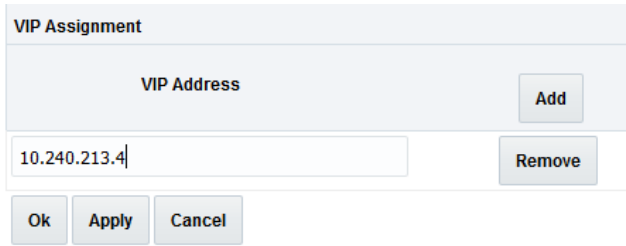
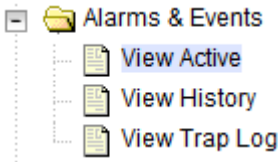
Procedure 20. Complete NOAM Server Group Configuration

1 ☐	NOAM GUI: Login	Establish a GUI session on the first NOAM server by using the XMI IP address. Open the web browser and enter a URL of <NO1_XMI_IP_Address> : Login as the <i>guiadmin</i> user: 

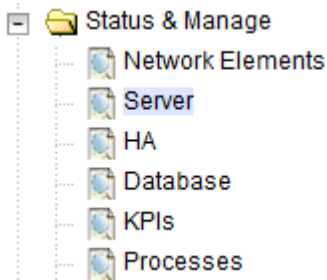
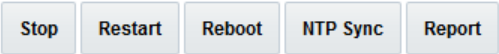
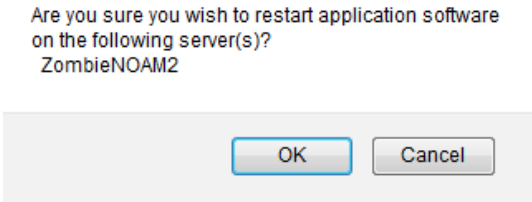
Procedure 20. Complete NOAM Server Group Configuration

2 ☐	NOAM GUI: Edit the NOAM Server Group Data	Navigate to Main Menu-> Configuration-> Server Groups.  Select the NOAM Server group and click on Edit Insert Edit Delete Report Add the 2nd NOAM server to the Server Group by clicking the <i>Include in SG</i> checkbox for the 2nd NOAM server. <table border="1" data-bbox="462 913 1421 1176"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> <tr> <td>ZombieNOAM2</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> </tbody> </table> Click Apply.	Server	SG Inclusion	Preferred HA Role	ZombieNOAM1	☒ Include in SG	☐ Prefer server as spare	ZombieNOAM2	☒ Include in SG	☐ Prefer server as spare
Server	SG Inclusion	Preferred HA Role									
ZombieNOAM1	☒ Include in SG	☐ Prefer server as spare									
ZombieNOAM2	☒ Include in SG	☐ Prefer server as spare									

Procedure 20. Complete NOAM Server Group Configuration

3 ☐	NOAM GUI: Add VIP	Navigate to Main Menu-> Configuration-> Server Groups.  Select the NOAM Server group and click on Edit  Add a NOAM VIP by click on Add. Fill in the VIP Address and press Ok as shown below 
4 ☐	NOAM VIP: Wait for Remote Database Alarm to Clear	Navigate to Main menu->Alarms & Events->View Active  Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding.

Procedure 20. Complete NOAM Server Group Configuration

5 ☐	NOAM GUI: Restart 2 nd NOAM Server	From the NOAM GUI, select the Main menu -> Status & Manage -> Server menu.  Select the 2nd NOAM server. Select the Restart button.  Answer OK to the confirmation popup. 

4.14.2 DSR Configuration: NetBackup Client Installation (Optional)

Procedure 21. Install NetBackup Client (Optional)

S T E P #	This procedure will download and install NetBackup Client software on the server. Location of the bpstart_notify and bpend_notify scripts is required for the execution of this procedure. For Appworks based applications the scripts are located as follows: - /usr/TKLC/appworks/sbin/bpstart_notify - /usr/TKLC/appworks/sbin/bpend_notify Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Install NetBackup Client Software	If a customer has a way of transferring and installing the net Backup client without the aid of TPD tools (push configuration) then use Appendix I.2: NETBACKUP CLIENT INSTALL/UPGRADE WITH NBAUTOINSTALL Note: This is not common. If the answer to the previous question is not known then use Appendix I.1: NetBackup Client Install using PLATCFG
2 ☐	Install NetBackup Client Software	Choose the same method used in step 1 to install NetBackup on the 2nd NOAM.

4.14.3 DSR Configuration: Disaster Recovery NOAM (Optional)

Procedure 22. NOAM Configuration for DR Site (Optional)

S T E P #	This procedure will provide the steps to configure the First DR NOAM server. Prequisites: The following prerequisites are assumed before starting this procedure: • TVOE is configured (Section 4.2) • Site PMAC is installed and deployed (Sections 4.3, 4.4 & 4.6) • Additional Rack Mount Servers installed and configured (Sections 4.7, 4.8, & 4.9) • VM placement, deployment and network has been configured (Sections 4.10, 4.12, 4.13) Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PRIMARY NOAM VIP GUI: Login Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of < NOAM_XMI_VIP_IP_Address >: Login as the <i>guiadmin</i> user:  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 22. NOAM Configuration for DR Site (Optional)

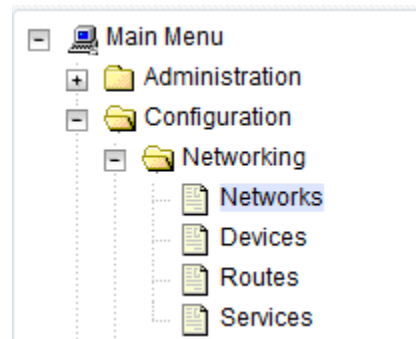
2



PRIMARY NOAM VIP GUI: Insert the DR NOAM Network Element

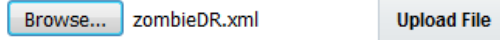
Note: NOAM Network Element file that describes the networking of the target install environment of the NOAM server should be created. Refer procedure 17, step 1 to find how to create this xml file

Navigate to **Main Menu->Networking -> Networks**



Select the **Browse** button, and enter the pathname of the NOAM network XML file:

To create a new Network Element, upload a valid configuration file:



Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.

Select the **Upload File** button to upload the XML file and configure the DR NOAM Network Element.

Once the data has been uploaded, you should see a tab appear with the name of your network element. Click on this tab and you will get a window which describes the individual networks that are now configured:

Main Menu: Configuration -> Networking -> Networks

Info*								
Global ZombieNOAM Ⓢ ZombieDRNOAM Ⓢ								
Network Name	Network Type	Default	Locked	Routed	VLAN	Configured Interfaces	Network	
XMI	OAM	Yes	Yes	Yes	4	0	10.240.213.0/24	
IMI	OAM	No	Yes	No	3	0	169.234.1.0/24	

Procedure 22. NOAM Configuration for DR Site (Optional)

3 ☐	PRIMARY NOAM VIP GUI: Insert the 1st DR-NOAM server	Navigate to Main Menu -> Configuration -> Servers. Fill in the fields as follows: Hostname: <Hostname> Role: NETWORK OAM&P System ID: <Site System ID> Hardware Profile: DSR TVOE Guest Network Element Name: [Choose NE from Drop Down Box] Location: <NOAM Server Location> Adding a new server <table border="1"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Hostname *</td> <td>ZombieDRNOAM1</td> </tr> <tr> <td>Role *</td> <td>NETWORK OAM&P</td> </tr> <tr> <td>System ID</td> <td></td> </tr> <tr> <td>Hardware Profile</td> <td>DSR TVOE Guest</td> </tr> <tr> <td>Network Element Name *</td> <td>ZombieDRNOAM</td> </tr> <tr> <td>Location</td> <td>pc5010441</td> </tr> </tbody> </table> The network interface fields will now become available with selection choices based on the chosen hardware profile and network element Fill in the server IP addresses for the XMI network. Select xmi for the interface. Leave the “VLAN” checkbox unchecked. Fill in the server IP addresses for the IMI network. Select imi for the interface. Leave the “VLAN” checkbox unchecked. <table border="1"> <tbody> <tr> <td>XMI (10.240.213.0/24)</td> <td>10.240.213.5</td> <td>xmi</td> <td>☐ VLAN (4)</td> </tr> <tr> <td>IMI (169.254.1.0/24)</td> <td>169.254.1.5</td> <td>imi</td> <td>☐ VLAN (3)</td> </tr> </tbody> </table> Next, add the following NTP servers: <table border="1"> <thead> <tr> <th>NTP Server</th> <th>Preferred?</th> </tr> </thead> <tbody> <tr> <td><1st-DR-NOAM-TVOE-IP-Address></td> <td>Yes</td> </tr> </tbody> </table> NTP Servers: <table border="1"> <thead> <tr> <th>NTP Server IP Address</th> <th>Prefer</th> <th></th> </tr> </thead> <tbody> <tr> <td>10.240.214.4</td> <td>☒</td> <td>Remove</td> </tr> </tbody> </table> Select the Ok button when you have completed entering all the server data.	Attribute	Value	Hostname *	ZombieDRNOAM1	Role *	NETWORK OAM&P	System ID		Hardware Profile	DSR TVOE Guest	Network Element Name *	ZombieDRNOAM	Location	pc5010441	XMI (10.240.213.0/24)	10.240.213.5	xmi	☐ VLAN (4)	IMI (169.254.1.0/24)	169.254.1.5	imi	☐ VLAN (3)	NTP Server	Preferred?	<1st-DR-NOAM-TVOE-IP-Address>	Yes	NTP Server IP Address	Prefer		10.240.214.4	☒	Remove
Attribute	Value																																	
Hostname *	ZombieDRNOAM1																																	
Role *	NETWORK OAM&P																																	
System ID																																		
Hardware Profile	DSR TVOE Guest																																	
Network Element Name *	ZombieDRNOAM																																	
Location	pc5010441																																	
XMI (10.240.213.0/24)	10.240.213.5	xmi	☐ VLAN (4)																															
IMI (169.254.1.0/24)	169.254.1.5	imi	☐ VLAN (3)																															
NTP Server	Preferred?																																	
<1st-DR-NOAM-TVOE-IP-Address>	Yes																																	
NTP Server IP Address	Prefer																																	
10.240.214.4	☒	Remove																																

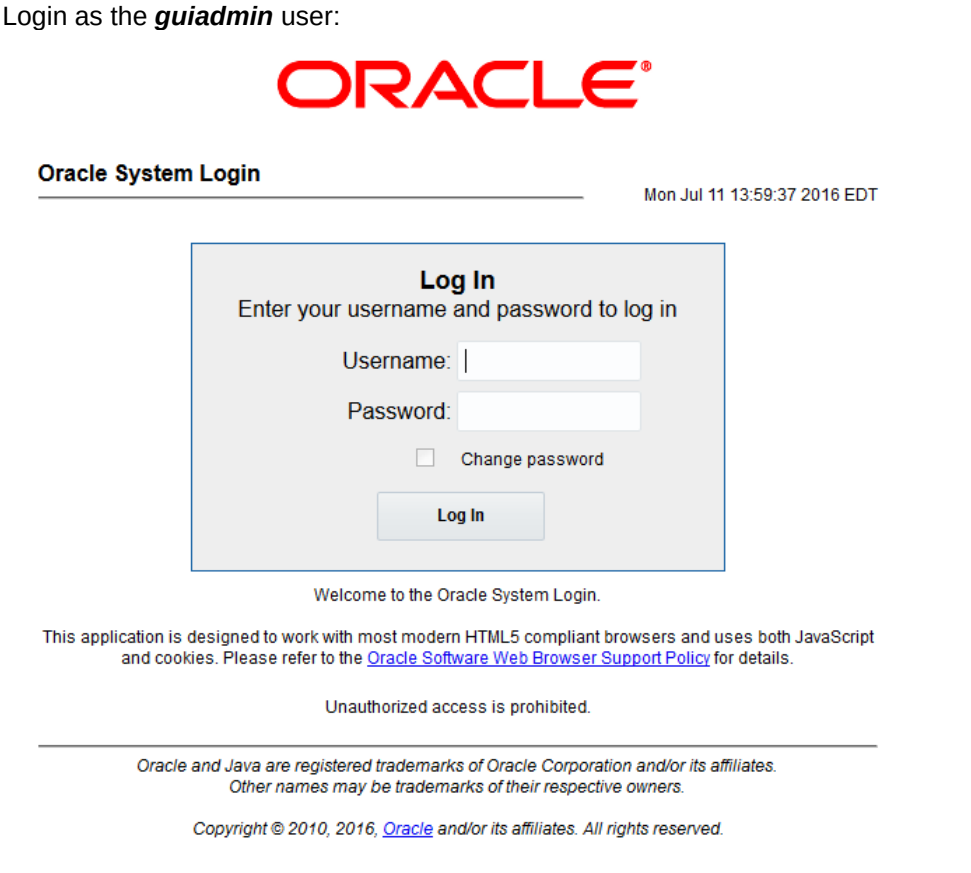
Procedure 22. NOAM Configuration for DR Site (Optional)

4 ☐	PRIMARY NOAM VIP GUI: Export the Initial Configuration	Navigate to Main Menu -> Configuration -> Servers. From the GUI screen, select the DR-NOAM server and then select Export to generate the initial configuration data for that server. Insert Edit Delete Export Report
5 ☐	1st NOAM Server: Copy Configuration File to DR NOAM Server	Obtain a terminal session to the primary NOAM VIP as the admusr user. Execute the following command to configure the 1st DR NOAM server: <pre>\$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<DRNOAM1_Hostname>.sh admusr@<DRNOAM1_xmi_IP_address>:/var/tmp/TKLCConfigData.sh</pre>
6 ☐	1st DR-NOAM Server: Verify server configuration was called and Reboot the Server	Obtain a terminal window connection on the 1st DR-NOAM Login as the admusr user. The automatic configuration daemon will look for the file named "TKLCConfigData.sh" in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server. Verify server configuration was called by checking the following file <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> Verify no errors are present and that the following message is displayed: <pre>[SUCCESS] script completed successfully!</pre> Note: The script may return success even when errors are reported in the log file. Go through the entire install.log file to verify no errors are present. Now Reboot the Server: <pre>\$ sudo init 6</pre> Wait for the server to reboot

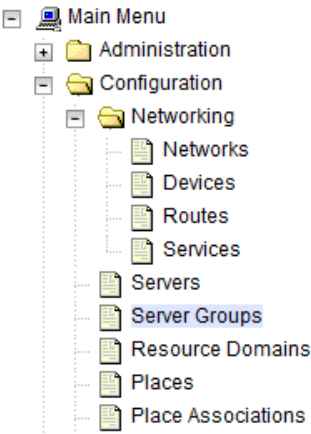
Procedure 22. NOAM Configuration for DR Site (Optional)

7 ☐	1st DR-NOAM Server: Verify Server Health	Execute the following command on the 1st DR-NOAM server and make sure that no errors are returned: <pre>\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>				
8 ☐	Repeat for 2nd DR NOAM Server	Repeat Steps 2 through 7 to configure 2nd DR-NOAM Server. When inserting the 2nd DR-NOAM server, change the NTP server address to the following: <table><tr><th>NTP Server</th><th>Preferred?</th></tr><tr><td><2nd DR-NOAM-RMS-TVOE-IP-Address></td><td>Yes</td></tr></table>	NTP Server	Preferred?	<2nd DR-NOAM-RMS-TVOE-IP-Address>	Yes
NTP Server	Preferred?					
<2nd DR-NOAM-RMS-TVOE-IP-Address>	Yes					

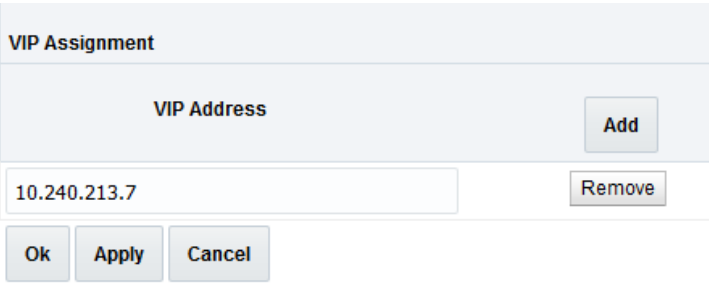
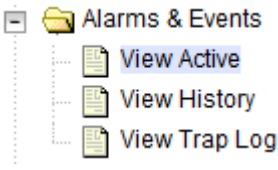
Procedure 23. Pairing for DR-NOAM Site (Optional)

S T E P #	This procedure will provide the steps to pair the DR-NOAM site. Prerequisite: Installation for DR-NOAM Site complete Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	PRIMARY NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of < NOAM_XMI_VIP_IP_Address >: Login as the <i>guiadmin</i> user:  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.

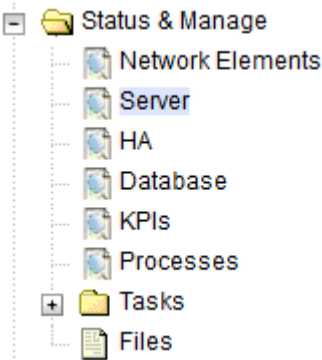
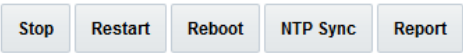
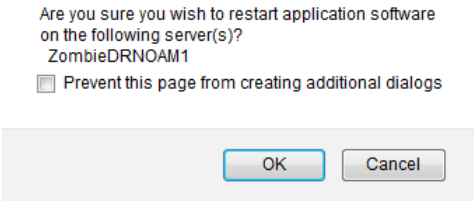
Procedure 23. Pairing for DR-NOAM Site (Optional)

2 ☐	Primary NOAM VIP GUI: Enter DR-NOAM Server Group Data	Navigate to Main Menu -> Configuration -> Server Groups  Select Insert and fill the following fields: Insert Edit Delete Report • Server Group Name: <Enter Server Group Name> • Level: A • Parent : None • Function: DSR (Active/Standby Pair) • WAN Replication Connection Count: Use Default Value Select OK when all fields are filled in.									
3 ☐	Primary NOAM VIP GUI: Update Server Group	Select the Server Group that was created in the previous step, and click on Edit. Insert Edit Delete Report The user will be presented with the Server Groups [Edit] screen Check the checkbox labeled Include in SG for both DR-NOAM Servers as shown below and click on Apply <table border="1"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>ZombieDRNOAM1</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> <tr> <td>ZombieDRNOAM2</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> </tbody> </table>	Server	SG Inclusion	Preferred HA Role	ZombieDRNOAM1	☒ Include in SG	☐ Prefer server as spare	ZombieDRNOAM2	☒ Include in SG	☐ Prefer server as spare
Server	SG Inclusion	Preferred HA Role									
ZombieDRNOAM1	☒ Include in SG	☐ Prefer server as spare									
ZombieDRNOAM2	☒ Include in SG	☐ Prefer server as spare									

Procedure 23. Pairing for DR-NOAM Site (Optional)

4 ☐	Primary NOAM VIP GUI: Add DR-NOAM VIP	Click the Add dialogue button for the VIP Address and enter an IP Address for the VIP as shown below  Then click the Apply dialogue button. Verify that the banner information message states Data committed.
5 ☐	Primary NOAM VIP GUI: Wait for Remote Database Alarm to Clear	Navigate to Main menu->Alarms & Events->View Active  Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding.

Procedure 23. Pairing for DR-NOAM Site (Optional)

6 ☐	Primary NOAM VIP GUI: Restart 1 st DR-NOAM Server	From the NOAM GUI, select the Main menu -> Status & Manage -> Server menu.  Select the 1st DR-NOAM server. Select the Restart button.  Answer OK to the confirmation popup. 						
7 ☐	Primary NOAM VIP GUI : Restart the application on the 2 nd DR-NOAM Server	Repeat Steps 6, this time select the 2nd DR-NOAM Server.						
8 ☐	Primary NOAM: Modify DSR OAM process	Establish an SSH session to the primary NOAM, login as admusr. Execute the following commands: Retrieve the cluster ID of the DR-NOAM: <pre>\$ sudo iqt -fClusterID TopologyMapping where "NodeID='<DR_NOAM_Host_Name>' "</pre> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Server_ID</th> <th style="text-align: left;">NodeID</th> <th style="text-align: left;">ClusterID</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Oahu-DSR-DR-NOAM-2</td> <td>A1055</td> </tr> </tbody> </table> Execute the following command to start the DSR OAM process on the DR-NOAM: <pre>\$ echo "<clusterID> DSROAM_Proc Yes" iload -ha -xun -fcluster -fresource -foptional HaClusterResourceCfg</pre>	Server_ID	NodeID	ClusterID	1	Oahu-DSR-DR-NOAM-2	A1055
Server_ID	NodeID	ClusterID						
1	Oahu-DSR-DR-NOAM-2	A1055						

4.14.3 DSR Configuration: SOAMs

Procedure 24. Configure the SOAM NE

S T E P #	This procedure will provide the steps to configure the SOAM Network Element Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PRIMARY NOAM VIP GUI: Login Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of < NOAM_XMI_VIP_IP_Address >: Login as the <i>guiadmin</i> user: 

Procedure 24. Configure the SOAM NE

2
☐ **PRIMARY NOAM VIP GUI:** Insert the SOAM Network Element

Note: SOAM Network Element file that describes the networking of the target install environment of the SOAM server should be created. Refer procedure 17, step 1 to find how to create this xml file

Navigate to **Main Menu->Networking -> Networks**

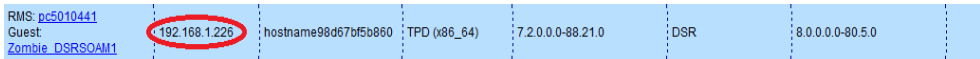
Select the **Browse** button, and enter the pathname of the SOAM network XML file:

Select the **Upload File** button to upload the XML file and configure the SOAM Network Element.

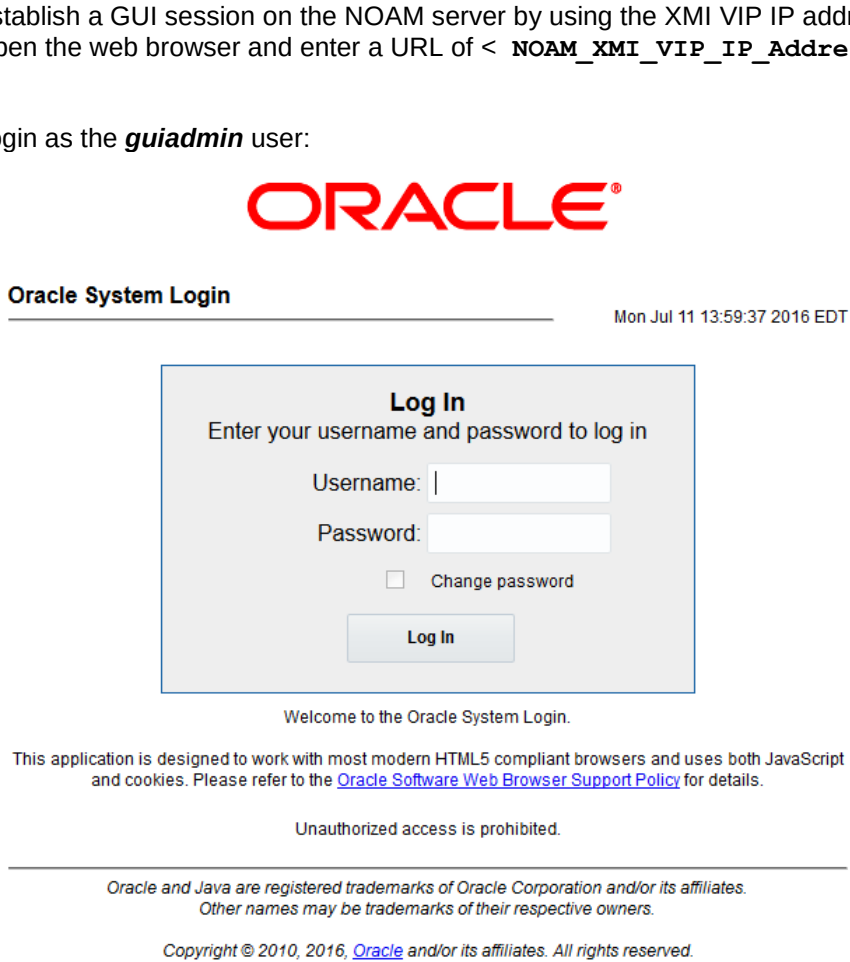
Once the data has been uploaded, you should see a folder appear with the name of your network element. Click on this folder and you will get a drop-down which describes the individual networks that are now configured:

Global ZombieNOAM ✕ ZombieDRNOAM ✕ ZombieSOAM ✕							
Network Name	Network Type	Default	Locked	Routed	VLAN	Configured Interfaces	Network
XMI	OAM	Yes	Yes	Yes	4	0	10.240.213.0/24
IMI	OAM	No	Yes	No	3	0	169.254.1.0/24

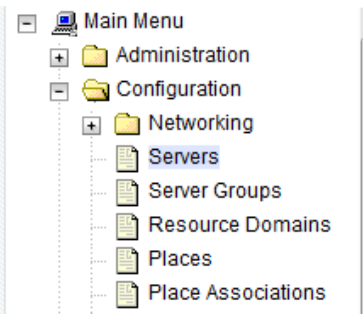
Procedure 25. Configure the SOAM Servers

S T E P #		This procedure will provide the steps to configure the SOAM servers. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	Exchange SSH keys between SOAM site's local PMAC and the SOAM Server	Use the PMAC GUI to determine the Control Network IP address of the server that is to be the SOAM server. From the PMAC GUI, navigate to Main Menu -> Software -> Software Inventory.  Note the IP address for the SOAM server. Login to the PMAC terminal as the admusr. From a terminal window connection on the PMAC as the admusr user, exchange SSH keys for admusr between the PMAC and the SOAM server using the keyexchange utility, using the Control network IP address for the SOAM server. When prompted for the password, enter the password for the admusr user of the NOAM server. <pre>\$ keyexchange admusr@<SO1_Control_IP_Address></pre>
2 ☐	Exchange SSH keys between NOAM and PMAC at the SOAM site (If necessary)	Note: If this SOAM shares the same PMAC as the NOAM, then you can skip this step. From a terminal window connection on the NOAM VIP, as the admusr, exchange SSH keys for admusr between the NOAM and the PMAC for this SOAM site using the keyexchange utility. When prompted for the password, enter the admusr password for the PMAC server. <pre>\$ keyexchange admusr@<SO1_Site_PMAC_Mgmt_IP_Address></pre> Repeat this step for the standby SOAM Server

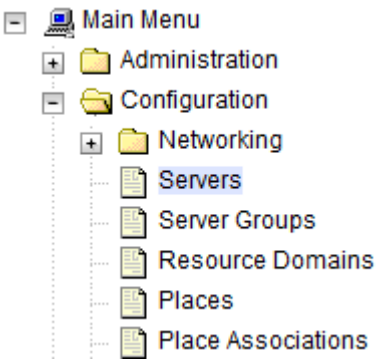
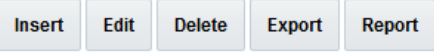
Procedure 25. Configure the SOAM Servers

3 ☐	PRIMARY NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of < NOAM_XMI_VIP_IP_Address >: Login as the <i>guiadmin</i> user: 

Procedure 25. Configure the SOAM Servers

4 ☐	NOAM VIP GUI: Insert the 1st SOAM server	Navigate to Main Menu -> Configuration -> Servers.  Select the Insert button to insert the 1st SOAM server into servers table (the first or server). Adding a new server Hostname * ZombiesSOAM1 Role * SYSTEM OAM System ID Hardware Profile DSR TVOE Guest Network Element Name * ZombieSOAM Fill in the fields as follows: Hostname: <Hostname> Role: SYSTEM OAM System ID: <Site System ID> Hardware Profile: DSR TVOE Guest Network Element Name: [Choose NE from Drop Down Box] The network interface fields will now become available with selection choices based on the chosen hardware profile and network element <table border="1"> <tr> <td>XMI (10.240.213.0/24)</td> <td> 10.240.213.9 </td> <td> xmi </td> <td>☐ VLAN (4)</td> </tr> <tr> <td>IMI (169.254.1.0/24)</td> <td> 169.254.1.9 </td> <td> imi </td> <td>☐ VLAN (3)</td> </tr> </table> Fill in the server IP addresses for the XMI network. Select xmi for the interface. Leave the “VLAN” checkbox unchecked. Fill in the server IP addresses for the IMI network. Select imi for the interface. Leave the “VLAN” checkbox unchecked. Next, add the following NTP servers: <table border="1"> <thead> <tr> <th>NTP Server</th> <th>Preferred?</th> </tr> </thead> <tbody> <tr> <td><1st SOAM-TVOE-IP-Address></td> <td>Yes</td> </tr> </tbody> </table> Select the Ok button when you have completed entering all the server data.	XMI (10.240.213.0/24)	10.240.213.9	xmi	☐ VLAN (4)	IMI (169.254.1.0/24)	169.254.1.9	imi	☐ VLAN (3)	NTP Server	Preferred?	<1st SOAM-TVOE-IP-Address>	Yes
XMI (10.240.213.0/24)	10.240.213.9	xmi	☐ VLAN (4)											
IMI (169.254.1.0/24)	169.254.1.9	imi	☐ VLAN (3)											
NTP Server	Preferred?													
<1st SOAM-TVOE-IP-Address>	Yes													

Procedure 25. Configure the SOAM Servers

5 ☐	NOAM VIP GUI: Export the Initial Configuration	Navigate to Main Menu -> Configuration -> Servers.  From the GUI screen, select the SOAM server and then select Export to generate the initial configuration data for that server. 
6 ☐	NOAM VIP: Copy Configuration File to 1 st SOAM Server	Obtain a terminal session to the NOAM VIP as the admusr user. Use the awpushcfg utility to copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the NOAM to the 1st SOAM server, using the Control network IP address for the 1st SOAM server. The configuration file will have a filename like "TKLCConfigData.<hostname>.sh". <pre>\$ awpushcfg</pre> The awpushcfg utility is interactive, so the user will be prompted for the following: • IP address of the local PMAC server: Use the management 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 1st SOAM server). • Hostname of the target server: Enter the server name configured in step 4

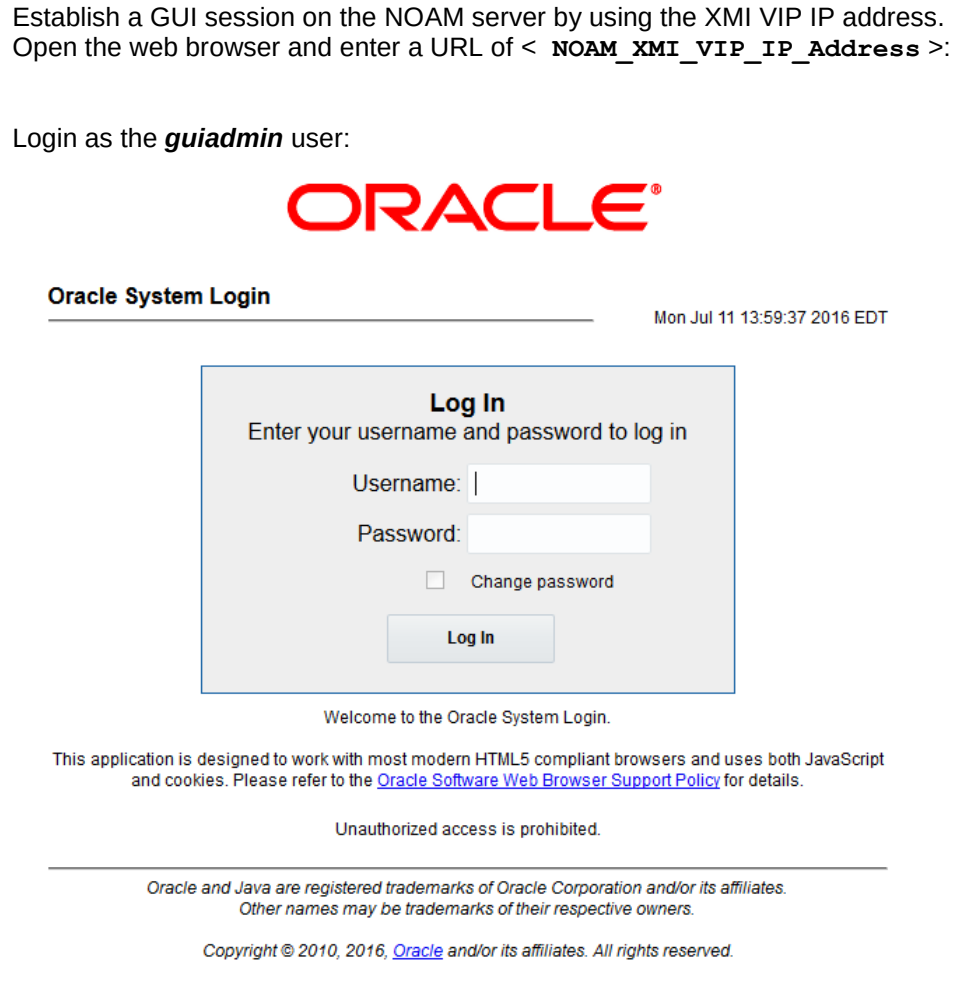
Procedure 25. Configure the SOAM Servers

7 ☐	1st SOAM Server: Verify awpushcfg was called and Reboot the Server	Obtain a terminal window connection on the 1st SOAM server console by establishing an ssh session from the Site PMAC terminal console. <pre>\$ ssh admusr@<SO1_Control_IP></pre> Login as the admusr user. The automatic configuration daemon will look for the file named “TKLCConfigData.sh” in the /var/tmp directory, implement the configuration in the file, and then prompt 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 no errors are present and that the following message is displayed: <pre>[SUCCESS] script completed successfully!</pre> Note: The script may return success even when errors are reported in the log file. Go through the entire install.log file to verify no errors are present. Now Reboot the Server: <pre>\$ sudo init 6</pre> Wait for the server to reboot
8 ☐	1st SOAM Server: Login	Obtain a terminal window connection on the 1st SOAM server console by establishing an ssh session from the site PMAC terminal console. <pre>\$ ssh admusr@<SO1_Control_IP></pre>
9 ☐	1st SOAM Server: Verify Server Health	Execute the following command on the 1st SOAM server and make sure that no errors are returned: <pre>\$ sudo syscheck</pre> <pre>Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

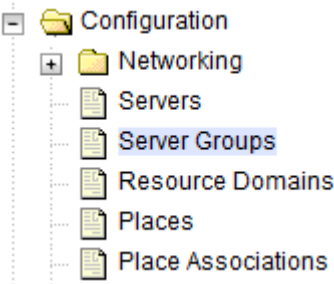
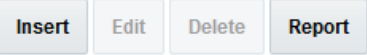
Procedure 25. Configure the SOAM Servers

10 ☐	Insert and Configure the 2nd SOAM server	Repeat this procedure to insert and configure the 2nd SOAM server, with the exception of the NTP server, which should be configured as so: <table><tr><th>NTP Server</th><th>Preferred?</th></tr><tr><td><Guest-TVOE-Host-IP-Address></td><td>Yes</td></tr></table> Instead of data for the 1st SOAM Server, insert the network data for the 2nd SOAM server, transfer the <i>TKLCCConfigData</i> file to the 2nd SOAM server, and reboot the 2nd SOAM server when prompted at a terminal window.	NTP Server	Preferred?	<Guest-TVOE-Host-IP-Address>	Yes
NTP Server	Preferred?					
<Guest-TVOE-Host-IP-Address>	Yes					
11 ☐	Insert and Configure the spare SOAM server	Repeat this procedure to insert and configure the spare SOAM server, with the exception of the NTP server, which should be configured as so: <table><tr><th>NTP Server</th><th>Preferred?</th></tr><tr><td><Guest-TVOE-Host-IP-Address></td><td>Yes</td></tr></table> Note: If the spare SOAM is located on a separate network, repeat procedure 24 to add the spare SOAM site NE. Instead of data for the 1st SOAM Server, insert the network data for the spare SOAM server, transfer the <i>TKLCCConfigData</i> file to the spare SOAM server, and reboot the spare SOAM server when prompted at a terminal window.	NTP Server	Preferred?	<Guest-TVOE-Host-IP-Address>	Yes
NTP Server	Preferred?					
<Guest-TVOE-Host-IP-Address>	Yes					
12 ☐	Install NetBackup Client Software on SOAMs (Optional)	If you are using NetBackup at this site, then execute Appendix I: Application NetBackup Client Installation Procedures again to install the NetBackup Client on all SOAM servers.				

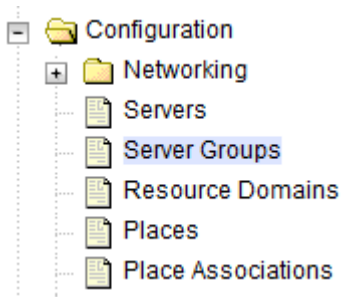
Procedure 26. Configure the SOAM Server Group

S T E P #	This procedure will provide the steps to configure the SOAM Server Group Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PRIMARY NOAM VIP GUI: Login Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of < NOAM_XMI_VIP_IP_Address >: Login as the <i>guiadmin</i> user: 

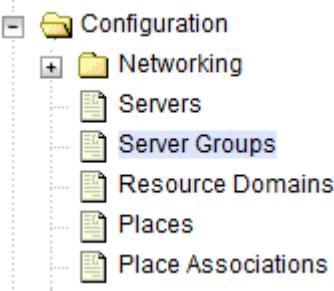
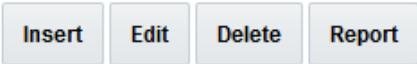
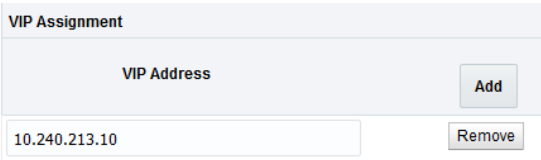
Procedure 26. Configure the SOAM Server Group

2 ☐	NOAM VIP GUI: Enter SOAM Server Group Data	After waiting approximately 5 minutes for the 2nd SOAM server to reboot, Navigate to the GUI Main Menu->Configuration->Server Groups  Select Insert  Add the SOAM Server Group name along with the values for the following fields: • Name: <Hostname> • Level: B • Parent [Select the NOAM Server Group] • Function: DSR (Active/Standby Pair) • WAN Replication Connection Count: Use Default Value Select OK when all fields are filled. Note: For DSR mated sites, repeat this step for additional SOAM server groups where the preferred SOAM spares may be entered prior to the active/Standby SOAMs.

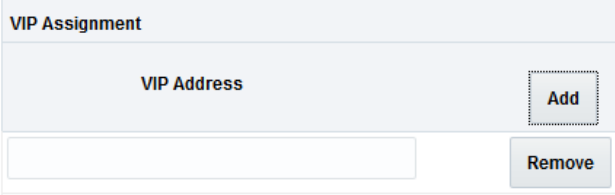
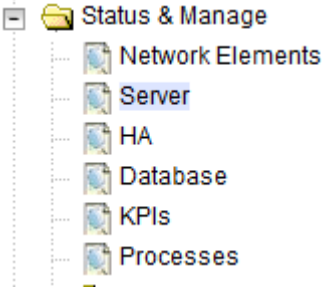
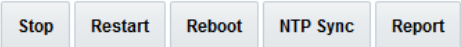
Procedure 26. Configure the SOAM Server Group

3 ☐	NOAM VIP GUI: Edit the SOAM Server Group	From the GUI Main Menu->Configuration->Server Groups  Select the new SOAM server group, and then select Edit. Insert Edit Delete Report Add both SOAM servers to the Server Group Primary Site by clicking the Include in SG checkbox. Do not check any of the Preferred Spare checkboxes. <table border="1" data-bbox="462 997 1242 1186"> <thead> <tr> <th>Server</th> <th>SG Inclusion</th> <th>Preferred HA Role</th> </tr> </thead> <tbody> <tr> <td>ZombieSOAM1</td> <td>☒ Include in SG</td> <td>☐ Prefer server as spare</td> </tr> <tr> <td>ZombieSOAM2</td> <td>☒ Include in SG</td> <td>☐ Prefer server as spare</td> </tr> </tbody> </table> Click Apply. Add a SOAM VIP by click on Add. Fill in the VIP Address and press Ok as shown below: VIP Assignment VIP Address Add 10.240.213.10 Remove	Server	SG Inclusion	Preferred HA Role	ZombieSOAM1	☒ Include in SG	☐ Prefer server as spare	ZombieSOAM2	☒ Include in SG	☐ Prefer server as spare
Server	SG Inclusion	Preferred HA Role									
ZombieSOAM1	☒ Include in SG	☐ Prefer server as spare									
ZombieSOAM2	☒ Include in SG	☐ Prefer server as spare									

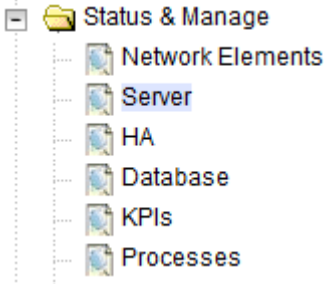
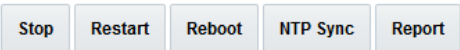
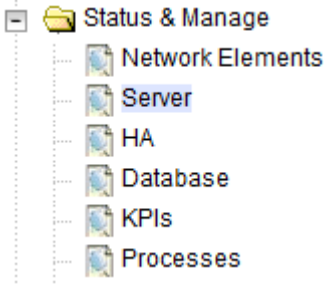
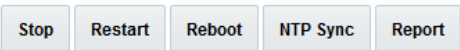
Procedure 26. Configure the SOAM Server Group

4 ☐	NOAM VIP GUI: Add VIP	From the GUI Main Menu->Configuration->Server Groups  Select the new SOAM server group, and then select Edit.  Add a SOAM VIP by click on Add. Fill in the VIP Address and press Ok as shown below: 												
5 ☐	NOAM VIP GUI: Edit the SOAM Server Group and add Preferred Spares for Site Redundancy (Optional)	If the Two Site Redundancy feature is wanted for the SOAM Server Group, add a SOAM server that is located in its Server Group Secondary Site by clicking the Include in SG checkbox. Also check the Preferred Spare checkbox. <table border="1"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>ZombieSOAM1</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> <tr> <td>ZombieSOAM2</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> <tr> <td>ZombieSOAMsp</td><td>☒ Include in SG</td><td>☒ Prefer server as spare</td></tr> </tbody> </table> For more information about Server Group Secondary Site, Tertiary Site or Site Redundancy, see Terminology section.	Server	SG Inclusion	Preferred HA Role	ZombieSOAM1	☒ Include in SG	☐ Prefer server as spare	ZombieSOAM2	☒ Include in SG	☐ Prefer server as spare	ZombieSOAMsp	☒ Include in SG	☒ Prefer server as spare
Server	SG Inclusion	Preferred HA Role												
ZombieSOAM1	☒ Include in SG	☐ Prefer server as spare												
ZombieSOAM2	☒ Include in SG	☐ Prefer server as spare												
ZombieSOAMsp	☒ Include in SG	☒ Prefer server as spare												

Procedure 26. Configure the SOAM Server Group

6 ☐	NOAM VIP GUI: Edit the SOAM Server Group and add additional SOAM VIPs (Optional)	Add additional SOAM VIPs by click on Add. Fill in the “VIP Address” and press Ok as shown below. Note: Additional SOAM VIPs only apply to SOAM Server Groups with Preferred Spare SOAMs. 
7 ☐	NOAM VIP GUI: Wait for Remote Database Alarm to Clear	Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding. Navigate to Main menu->Alarms & Events->View Active
8 ☐	NOAM VIP GUI: Restart 1 st SOAM server	From the NOAMP GUI, select Main menu->Status & Manage->Server.  Select the 1st SOAM server. Select the Restart button. Answer OK to the confirmation popup. Wait for restart to complete. 

Procedure 26. Configure the SOAM Server Group

9 ☐	NOAM VIP GUI: Restart 2 nd SOAM server	From the NOAMP GUI, select Main menu->Status & Manage->Server.  Select the 2nd SOAM server. Select the Restart button. Answer OK to the confirmation popup. Wait for restart to complete. 
10 ☐	NOAM VIP GUI: Restart all Preferred Spare SOAM Servers	If additional Preferred Spare servers are not configured for <i>Secondary or Tertiary Sites</i>, this step can be skipped. If additional Preferred Spare servers are configured for <i>Secondary and/or Tertiary Sites</i>, continuing in the Main menu->Status & Manage->Server  Select the all Preferred Spare SOAM servers. Select the Restart button. Answer OK to the confirmation popup. 

Procedure 27. Configure RMS-Specific B-Level Resources (HP DL 380 Gen 8 Servers ONLY)

S T E P #	This procedure will provide the steps to Configure RMS-specific B-level Resources  IMPORTANT: SKIP THIS STEP IF INSTALLING ON ORACLE X5-2/NETRA X5-2/X6-2/HP DL380 GEN 9  Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Active SOAM: Login	Obtain a terminal window connection on the Active SOAM server. Login as admusr .
2 ☐	Active SOAM: Execute B-Level Resource Script	Execute the following on the command line. Wait until the script completes and you are returned to the command line: <pre style="border: 1px solid black; padding: 5px; display: inline-block;">\$ sudo /usr/TKLC/dsr/bin/rmsResourceConfig.sh</pre> Verify that no errors are displayed. If any errors are displayed, halt this procedure and contact Appendix U: My Oracle Support (MOS)

4.14.5 DSR Configuration: Activate PCA**Procedure 28. Activate PCA (PCA Only)**

S T E P #	This procedure will provide the steps to activate PCA Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	(PCA Only) Activate PCA Feature	If you are installing PCA, execute applicable procedures (Added SOAM site activation or complete system activation) of the PCA activation guide [12] to activate PCA. Note: If not all SOAM sites are ready at this point, then you should repeat activation for each *new* SOAM site that comes online. Note: Ignore steps to restart DA-MPs and SBRs that have yet to be configured.

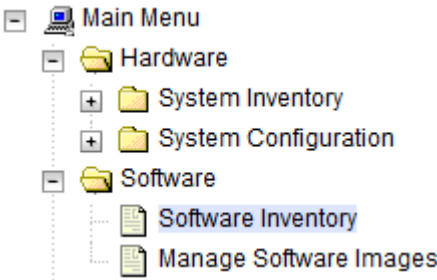
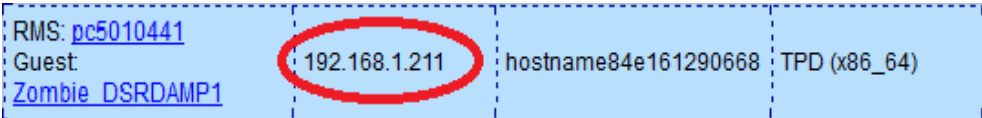
4.14.6 DSR Configuration: Activate DCA

Procedure 29. Activate DCA (DCA Only)

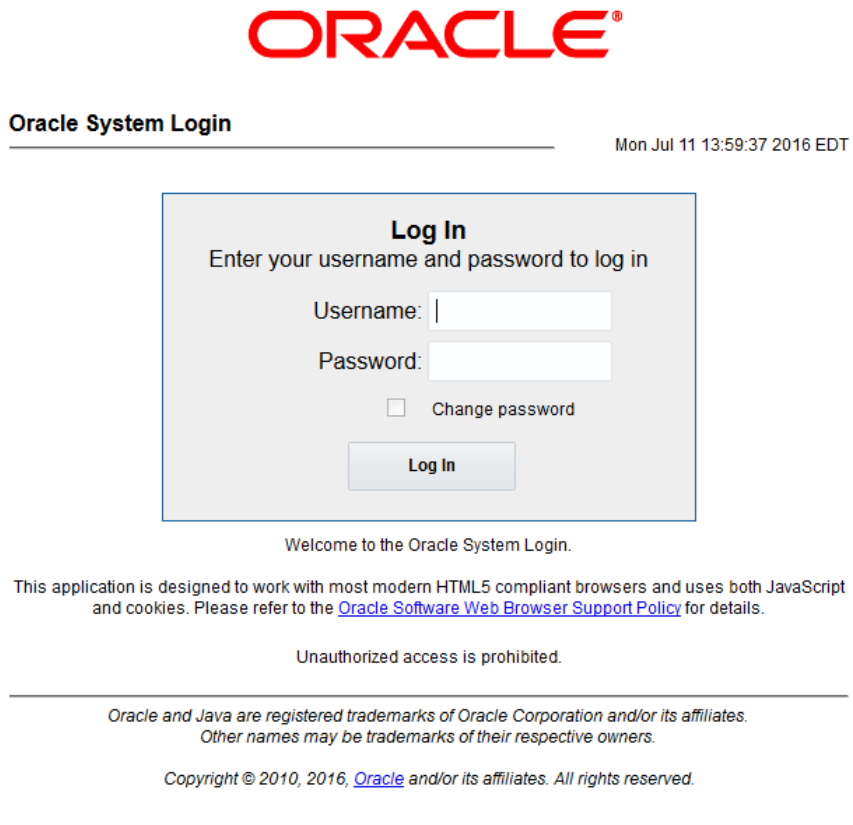
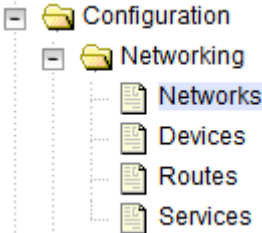
S T E P #	This procedure will provide the steps to activate DCA Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	(DCA Only) Activate DCA Feature	If you are installing DCA, execute procedures in [20] to activate DCA Framework and Feature. Note: If not all SOAM sites are ready at this point, then you should repeat activation for each *new* SOAM site that comes online. Note: Ignore steps to restart DA-MPs and SBRs that have yet to be configured.

4.14.7 DSR Configuration: MPs

Procedure 30. Configure the MP Servers

S T E P #	Note: If you are adding MPs to expand an existing DSR which was upgraded from 7.x to 8.x, skip this procedure and execute Appendix P.1.6.1 Growth: MP (7.x to 8.x upgraded system) This procedure will provide the steps to configure an MP Servers (IPFE, SBR, SS7-MP, DA-MP) Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PMAC: Exchange SSH keys between MP site's local PMAC and the MP server Use the MP site's PMAC GUI to determine the Control Network IP address of the server that is to be an MP server. From the MP site's PMAC GUI, navigate to Main Menu -> Software -> Software Inventory.   Note the IP address for an MP server. Login to the MP site's PMAC terminal as the admusr. From a terminal window connection on the MP site's PMAC as the admusr. Exchange SSH keys for admusr between the PMAC and the MP server using the keyexchange utility, using the Control network IP address for the MP server. <pre>\$ keyexchange admusr@<MP_Control_IP Address></pre> When prompted for the password, enter the password for the admusr user of the MP server.
2 ☐	PRIMARY NOAM VIP GUI: Login Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of < NOAM_XMI_VIP_IP_Address >: Login as the guiadmin user:

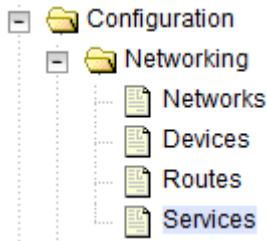
Procedure 30. Configure the MP Servers

		 Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.									
3 ☐	NOAM VIP GUI: Navigate to Signaling Network Configuration on Screen	Navigate to Main Menu -> Configuration -> Networking -> Networks  Select the associated SOAM tab for the MP Server Global ZombieNOAM ✕ ZombieDRNOAM ✕ ZombieSOAM ✕ <table border="1" data-bbox="430 1522 1177 1669"> <thead> <tr> <th>Network Name</th> <th>Network Type</th> <th>Default</th> </tr> </thead> <tbody> <tr> <td>XMI</td> <td>OAM</td> <td>Yes</td> </tr> <tr> <td>IMI</td> <td>OAM</td> <td>No</td> </tr> </tbody> </table> Click on Insert in the lower left corner. Insert Edit Lock/Unlock Delete Report Insert Network Element Export	Network Name	Network Type	Default	XMI	OAM	Yes	IMI	OAM	No
Network Name	Network Type	Default									
XMI	OAM	Yes									
IMI	OAM	No									

Procedure 30. Configure the MP Servers

4 ☐	NOAMP VIP GUI: Add Signaling Networks	You will see the following screen: Insert Network <table border="1"> <thead> <tr> <th>Field</th><th>Value</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Network Name *</td><td>xsl1</td><td>The name of this network. [Default]</td></tr> <tr> <td>Network Type</td><td>Signaling v </td><td>The type of this network.</td></tr> <tr> <td>VLAN ID *</td><td>6</td><td>The VLAN ID to use for this network.</td></tr> <tr> <td>Network Address *</td><td>10.196.227.0</td><td>The network address of this network.</td></tr> <tr> <td>Netmask *</td><td>255.255.255.0</td><td>Subnetting to apply to servers within this network.</td></tr> <tr> <td>Router IP</td><td>10.196.227.1</td><td>The IP address of a router on this network that is monitored.</td></tr> <tr> <td>Default Network</td><td>☐ Yes ☒ No</td><td>A selection indicating whether this network is the default.</td></tr> <tr> <td>Routed</td><td>☒ Yes ☐ No</td><td>Whether or not this network is routable.</td></tr> </tbody> </table> Ok Apply Cancel Enter the Network Name, VLAN ID, Network Address, Netmask, and Router IP that matches the Signaling network Note: Even if the network does not use VLAN Tagging, you should enter the correct VLAN ID here as indicated by the NAPD • Select Signaling for Network Type • Select No for Default Network • Select Yes for Routable. Press OK. If you are finished adding signaling networks -OR- Press Apply to save this signaling network and repeat this step to enter additional signaling networks.	Field	Value	Description	Network Name *	xsl1	The name of this network. [Default]	Network Type	Signaling v	The type of this network.	VLAN ID *	6	The VLAN ID to use for this network.	Network Address *	10.196.227.0	The network address of this network.	Netmask *	255.255.255.0	Subnetting to apply to servers within this network.	Router IP	10.196.227.1	The IP address of a router on this network that is monitored.	Default Network	☐ Yes ☒ No	A selection indicating whether this network is the default.	Routed	☒ Yes ☐ No	Whether or not this network is routable.
Field	Value	Description																											
Network Name *	xsl1	The name of this network. [Default]																											
Network Type	Signaling v	The type of this network.																											
VLAN ID *	6	The VLAN ID to use for this network.																											
Network Address *	10.196.227.0	The network address of this network.																											
Netmask *	255.255.255.0	Subnetting to apply to servers within this network.																											
Router IP	10.196.227.1	The IP address of a router on this network that is monitored.																											
Default Network	☐ Yes ☒ No	A selection indicating whether this network is the default.																											
Routed	☒ Yes ☐ No	Whether or not this network is routable.																											
5 ☐	NOAMP VIP GUI: [PCA/DCA Only]: Define SBR DB Replication Network	Note: Execute this step only if you are defining a separate, dedicated network for SBR Replication.																											

Procedure 30. Configure the MP Servers

		Insert Network <table border="1"> <thead> <tr> <th>Field</th><th>Value</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Network Name *</td><td>replication</td><td>The name of this</td></tr> <tr> <td>Network Type</td><td>Signaling ▾</td><td>The type of this n</td></tr> <tr> <td>VLAN ID *</td><td>9</td><td>The VLAN ID to u</td></tr> <tr> <td>Network Address *</td><td>10.240.77.0</td><td>The network add</td></tr> <tr> <td>Netmask *</td><td>255.255.255.0</td><td>Subnetting to ap</td></tr> <tr> <td>Router IP</td><td>10.240.77.1</td><td>The IP address c one monitored.</td></tr> <tr> <td>Default Network</td><td>☐ Yes ☒ No</td><td>A selection indic</td></tr> <tr> <td>Routed</td><td>☒ Yes ☐ No</td><td>Whether or not th</td></tr> </tbody> </table> Ok Apply Cancel Enter the Network Name, VLAN ID, Network Address, Netmask, and Router IP that matches the SBR DB Replication network Note: Even if the network does not use VLAN Tagging, you should enter the correct VLAN ID here as indicated by the NAPD • Select Signaling for Network Type • Select No for Default Network • Select Yes for Routable. Press Ok. If you are finished adding signaling networks –OR– Press Apply to save this signaling network and repeat this step to enter additional signaling networks.	Field	Value	Description	Network Name *	replication	The name of this	Network Type	Signaling ▾	The type of this n	VLAN ID *	9	The VLAN ID to u	Network Address *	10.240.77.0	The network add	Netmask *	255.255.255.0	Subnetting to ap	Router IP	10.240.77.1	The IP address c one monitored.	Default Network	☐ Yes ☒ No	A selection indic	Routed	☒ Yes ☐ No	Whether or not th
Field	Value	Description																											
Network Name *	replication	The name of this																											
Network Type	Signaling ▾	The type of this n																											
VLAN ID *	9	The VLAN ID to u																											
Network Address *	10.240.77.0	The network add																											
Netmask *	255.255.255.0	Subnetting to ap																											
Router IP	10.240.77.1	The IP address c one monitored.																											
Default Network	☐ Yes ☒ No	A selection indic																											
Routed	☒ Yes ☐ No	Whether or not th																											
6 □	NOAM VIP GUI: [PCA / DCA Only]: Perform Additional Service to Networks Mapping	Note: Execute this step only if you are defining a separate, dedicated network for SBR Replication. Navigate to Main Menu -> Configuration -> Services 																											

Procedure 30. Configure the MP ServersSelect the **Edit** button

Set the Services according to the below two scenarios:

1) If the Dual-Path HA Configuration is required :

Oracle recommends that inter-NE network be set to the XMI network and the intra-NE network set to the IMI network for HA_MP_Secondary. This configuration uses the XMI network as a secondary path to preserve the HA status of SBRs grouped between multiple sites. If the Primary HA path “SBR DB Replication Network” becomes lost or impaired, the XMI network is used to preserve the HA state preventing the servers from entering into a scenario known as “HA Split-Brain”. Preventing “HA Split-Brain” will keep existing database in sync, but the DSR mate site will be isolated from the active SBR and will result in traffic loss until SBR DB Replication Network is restored.

Name	Intra-NE Network	Inter-NE Network
HA_MP_Secondary	<IMI Network>	<XMI Network>*
Replication_MP	<IMI Network>	<SBR DB Replication Network>*
ComAgent	<IMI Network>	<SBR DB Replication Network>*

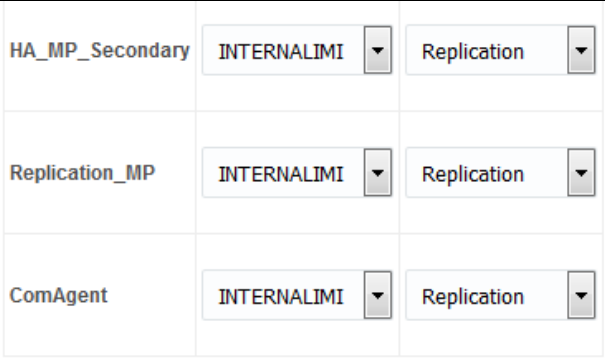
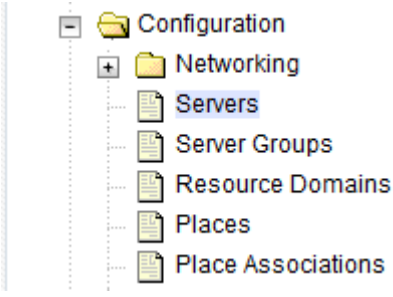
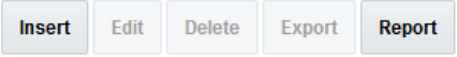
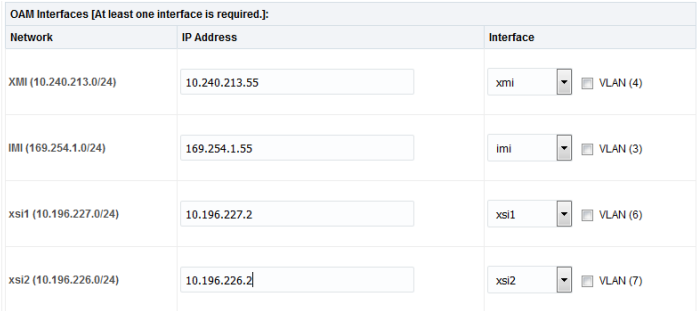
HA_MP_Secondary	INTERNALIMI ▼	INTERNALXMI ▼
Replication_MP	INTERNALIMI ▼	Replication ▼
ComAgent	INTERNALIMI ▼	Replication ▼

2) If the Dual-Path HA Configuration is NOT required :

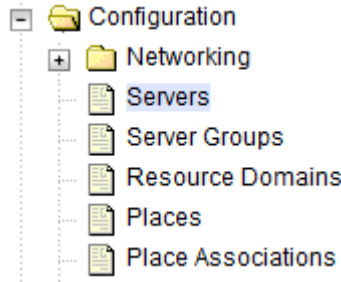
Oracle recommends that inter-NE network be set to the SBR DB Replication (configured in step 5) and the intra-NE network set to the IMI network for HA_MP_Secondary. This configuration may allow an “HA Split-Brain” condition between the SBRs should the SBR DB Replication Network become lost or impaired. During a “HA Split-Brain” condition, an active SBR server would exist at each site but the database would not be in sync between the SBRs.

Name	Intra-NE Network	Inter-NE Network
HA_MP_Secondary	<IMI Network>	<SBR DB Replication Network>*
Replication_MP	<IMI Network>	<SBR DB Replication Network>*
ComAgent	<IMI Network>	<SBR DB Replication Network>*

Procedure 30. Configure the MP Servers

		 Select the Ok button to apply the Service-to-Network selections.
7	NOAM VIP GUI: Insert the MP server (Part 1)	Navigate to Main Menu->Configuration->Servers  Select the Insert button to insert the new MP server into servers table.  Fill out the following values: Hostname: <Hostname> Role: MP Network Element: [Choose Network Element] Hardware Profile: DSR TVOE Guest Location: <enter an optional location description> The interface configuration form will now appear.  For the XMI network, enter the MP's XMI IP address. Select the xmi interface.

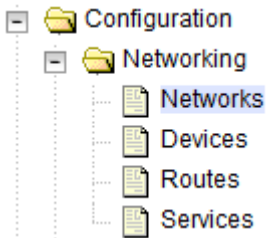
Procedure 30. Configure the MP Servers

		- For the IMI network, enter the MP's IMI IP address. Select the imi interface. - For the XSI1 network, enter the MP's XSI1 IP address. Select the xsi1 interface. - For the XSI2 network, enter the MP's XSI2 IP address. Select the xsi2 interface. - For the Replication network (If Step 5 was executed), enter the MP's Replication IP address. Select the replication interface. Note: If networks have been configured previously but are not required on the server, simply remove the populated network IP from the IP Address field and this device will not be created on the server. Note: If XSI3-16 were configured, follow the same method of entry as XSI1 and XSI2				
8	NOAM VIP GUI: Insert the MP server (Part 2)	Next, add the following NTP servers: <table><tr><th>NTP Server</th><th>Preferred?</th></tr><tr><td><MP-RMS-TVOE-IP-Address></td><td>Yes</td></tr></table> Select OK when all fields are filled in to finish MP server insertion.	NTP Server	Preferred?	<MP-RMS-TVOE-IP-Address>	Yes
NTP Server	Preferred?					
<MP-RMS-TVOE-IP-Address>	Yes					
9	NOAM VIP GUI: Export the Configuration	Navigate to Main Menu -> Configuration -> Servers.  From the GUI screen, select the MP server and then select Export to generate the initial configuration data for that server. 				
10	NOAM VIP: Copy Configuration File to MP Server	Obtain a terminal session to the NOAM VIP as the admusr user. Use the awpushcfg utility to copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the NOAM to the MP server, using the Control network IP address for the MP server. The configuration file will have a filename like "TKLCCfgData.<hostname>.sh". <pre>\$ sudo awpushcfg</pre> The awpushcfg utility is interactive, so the user will be prompted for the following: - IP address of the local PMAC server: Use the management network address from the PMAC. - Username: Use admusr - Control network IP address for the target server: In this case, enter the				

Procedure 30. Configure the MP Servers

		control IP for the MP server). • Hostname of the target server: Enter the server name configured in step 1
11 ☐	MP Server: Verify awpushcfg was called and Reboot the Configured Server	Obtain a terminal window connection on the MP server console by establishing an ssh session from the PMAC of the MP. <pre>\$ ssh admusr@<MP_Control_IP></pre> Login as the admusr user. Verify awpushcfg was called by checking the following file: <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> Verify no errors are present and that the following message is displayed: <pre>[SUCCESS] script completed successfully!</pre> Note: The script may return success even when errors are reported in the log file. Go through the entire install.log file to verify no errors are present. Reboot the sever: <pre>\$ sudo init 6</pre> Proceed to the next step once the Server finished rebooting, The server is done rebooting once the login prompt is displayed.
12 ☐	MP Server: Login	After the reboot, login as admusr .
13 ☐	MP Server: Verify Server Health	Execute the following command on the server and make sure that no errors are returned: <pre>\$ sudo syscheck</pre> <pre>Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>
14 ☐	MP Server: Delete Auto- Configured Default Route on	Note: THIS STEP IS OPTIONAL AND SHOULD ONLY BE EXECUTED IF YOU PLAN TO CONFIGURE A DEFAULT ROUTE ON YOUR MP THAT USES A SIGNALING (XSI) NETWORK INSTEAD OF THE XMI NETWORK. (Not executing this step will mean that a default route will not be configurable on this MP and you will have to create separate network routes for each signaling network

Procedure 30. Configure the MP Servers

	MP and Replace it with a Network Route via the XMI Network-Part1 (Optional)	destination.) Login into the site's PMAC then SSH to the MP's control address (<i>Alternatively you can login to the TVOE host and access the MP via virsh console <MP VM></i>) Determine <XMI_Gateway_IP> from your SO site network element info. Gather the following items: • <NO_XMI_Network_Address> • <NO_XMI_Network_Netmask> • <DR_NO_XMI_Network_Addres> • <DR_NO_XMI_Network_Netmask> • <TVOE_Mgmt_XMI_Network_Address> • <TVOE_Mgmt_XMI_Network_Netmask> Note: You can either consult the XML files you imported earlier, or go to the NO GUI and view these values from the Main Menu -> Configuration -> Networking -> Networking screen.  Proceed to the next step to modify the default routes on the MP servers.
15	☐ MP Server: Delete Auto-Configured Default Route on MP and Replace it with a Network Route via the XMI Network-Part2 (Optional)	After gathering the network information from step 14, proceed with modifying the default routes on the MP server. Establish a connection to the MP server, login as admusr. Create network routes to the NO's XMI(OAM) network: Note: If your NOAM XMI network is exactly the same as your MP XMI network, then you should skip this command and only configure the DR NO route. <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --address=<NO_Site_Network_ID> --netmask=<NO_Site_Network_Netmask> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface> Route to <MP_XMI_Interface> added.</pre> Create network routes to the DR NO's XMI(OAM) network: <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --address=<DR-NO_Site_Network_ID> --netmask=<<DR-NO_Site_Network_Netmask> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface> Route to <MP_XMI_Interface> added.</pre>

Procedure 30. Configure the MP Servers

		Create network routes to the Management Server TVOE XMI(OAM) network for NTP: <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --address=<TVOE_Mgmt_XMI_Network_Address> --netmask=<TVOE_Mgmt_XMI_Network_Netmask> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface> Route to <MP_XMI_Interface> added.</pre> (Optional) If Sending SNMP traps from individual servers, create host routes to customer SNMP trap destinations on the XMI network: <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=host --address=<Customer_NMS_IP> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface> Route to <MP_XMI_Interface> added.</pre> (Repeat for any existing customer NMS stations) Delete the existing default route: 1. Login to the PRIMARY NOAM VIP GUI 2. Navigate to Configuration->Networking->Networks 3. Select the specific SO tab. 4. Select the XMI network and click 'Unlock'. Click OK to confirm 5. Go to Configuration->Networking->Routes 6. Select the Specific MP XMI route and click 'Delete'. 7. Click OK to confirm. 8. Repeat the above steps for all required MPs to delete the XMI routes 9. Select Configuration->Networking->Networks 10. Select the respective SOAM tab. 11. Select the XMI network and click 'Lock'. 12. Click OK to confirm
16 ☐	MP Server: Verify connectivity	After steps 14 -15 have been executed, verify network connectivity. Establish a connection to the MP server, login as admusr. Ping active NO XMI IP address to verify connectivity: <pre>\$ ping <ACTIVE_NO_XMI_IP_Address> PING 10.240.108.6 (10.240.108.6) 56(84) bytes of data. 64 bytes from 10.240.108.6: icmp_seq=1 ttl=64 time=0.342 ms 64 bytes from 10.240.108.6: icmp_seq=2 ttl=64 time=0.247 ms</pre> (Optional) Ping Customer NMS Station(s): <pre>\$ ping <Customer_NMS_IP> PING 172.4.116.8 (172.4.116.8) 56(84) bytes of data. 64 bytes from 172.4.116.8: icmp_seq=1 ttl=64 time=0.342 ms 64 bytes from 172.4.116.8: icmp_seq=2 ttl=64 time=0.247 ms</pre>

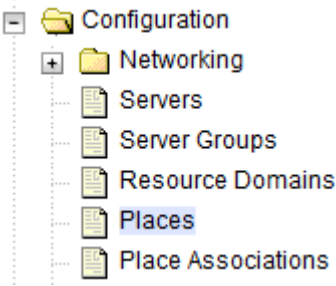
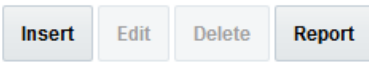
Procedure 30. Configure the MP Servers

		If you do not get a response, then verify your network configuration. If you continue to get failures then halt the installation and contact Oracle customer support.
17 ☐	Repeat for remaining MPs	Repeat this entire procedure for all remaining MP (SS7-MP, DA-MP, SBR and IPFE) servers.

Procedure 31. Configure Places and Assign MP Servers to Places (PCA & DCA ONLY)

S T E P #	This procedure will provide the steps/reference to add “Places” in the PCA / DCA Network. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	PRIMARY NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of < NOAM_XMI_VIP_IP_Address >: Login as the <i>guiadmin</i> user: 

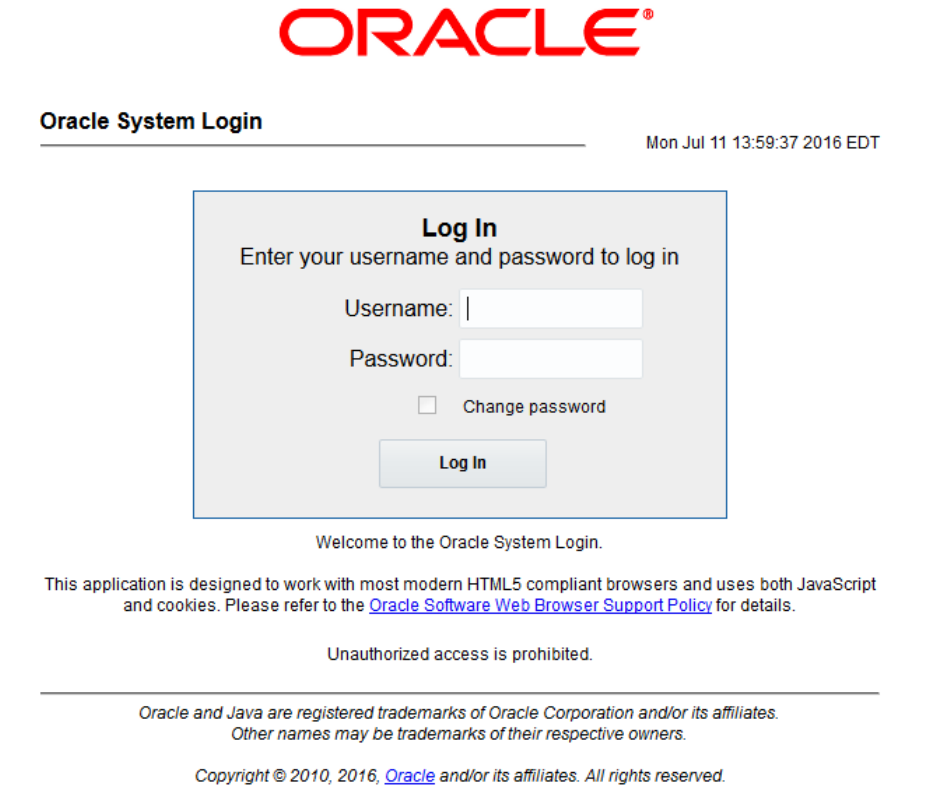
Procedure 31. Configure Places and Assign MP Servers to Places (PCA & DCA ONLY)

2 ☐	NOAM VIP GUI: Configure Places	Establish a GUI session on the NOAMP by using the XMI VIP address. Login as user guiadmin. Navigate to Main Menu -> Configuration -> Places  Select the Insert button  Inserting a new Place <table border="1" data-bbox="467 945 1269 1339"> <thead> <tr> <th colspan="3">Place</th></tr> <tr> <th>Field</th><th>Value</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Place Name *</td><td>ZombiePlace</td><td>Unique identifier used to label a Place. [Default and space.] [A value is required.]</td></tr> <tr> <td>Parent *</td><td>NONE</td><td>The Parent of this Place [A value is required.]</td></tr> <tr> <td>Place Type *</td><td>Site</td><td>The Type of this Place [A value is required.]</td></tr> </tbody> </table> Place Name: <Site Name> Parent: NONE Place Type: Site Repeat this step for each of the <i>PCA / DCA Places (Sites)</i> in the network. See the Terminology section for more information on <i>Sites & Places</i>.	Place			Field	Value	Description	Place Name *	ZombiePlace	Unique identifier used to label a Place. [Default and space.] [A value is required.]	Parent *	NONE	The Parent of this Place [A value is required.]	Place Type *	Site	The Type of this Place [A value is required.]
Place																	
Field	Value	Description															
Place Name *	ZombiePlace	Unique identifier used to label a Place. [Default and space.] [A value is required.]															
Parent *	NONE	The Parent of this Place [A value is required.]															
Place Type *	Site	The Type of this Place [A value is required.]															

Procedure 31. Configure Places and Assign MP Servers to Places (PCA & DCA ONLY)

3 ☐	NOAM VIP GUI: Assign MP Servers To Places	Select the place configured in step 2, press the edit button. Insert Edit Delete Report For each place you have defined, choose the set of MP servers that will be assigned to those places. Editing Place ZombiePlace <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Place Type *</td> <td style="width: 40%;"> Site </td> <td style="width: 30%;">The Ty</td> </tr> <tr> <td colspan="3" style="background-color: #f2f2f2;">Servers</td> </tr> <tr> <td rowspan="2">ZombieNOAM</td> <td>☐ ZombieNOAM1</td> <td rowspan="2">Availa</td> </tr> <tr> <td>☐ ZombieNOAM2</td> </tr> <tr> <td rowspan="2">ZombieDRNOAM</td> <td>☐ ZombieDRNOAM1</td> <td rowspan="2">Availa</td> </tr> <tr> <td>☐ ZombieDRNOAM2</td> </tr> <tr> <td rowspan="4">ZombieSOAM</td> <td>☐ ZombieSOAM1</td> <td rowspan="4">Availa</td> </tr> <tr> <td>☐ ZombieSOAM2</td> </tr> <tr> <td>☒ ZombieDAMP1</td> </tr> <tr> <td>☒ ZombieDAMP2</td> </tr> </table> Ok Apply Cancel Check all the check boxes for SS7-MPs and PCA / DCA DA-MP and SBR servers that will be assigned to this place. Repeat this step for all other DA-MP or SBR servers you wish to assign to places. Note: All DA-MPs and SBR servers must be added to the <i>Site Place</i> that corresponds to the physical location of the server. See the Terminology section for more information on <i>Sites</i>.	Place Type *	Site	The Ty	Servers			ZombieNOAM	☐ ZombieNOAM1	Availa	☐ ZombieNOAM2	ZombieDRNOAM	☐ ZombieDRNOAM1	Availa	☐ ZombieDRNOAM2	ZombieSOAM	☐ ZombieSOAM1	Availa	☐ ZombieSOAM2	☒ ZombieDAMP1	☒ ZombieDAMP2
Place Type *	Site	The Ty																				
Servers																						
ZombieNOAM	☐ ZombieNOAM1	Availa																				
	☐ ZombieNOAM2																					
ZombieDRNOAM	☐ ZombieDRNOAM1	Availa																				
	☐ ZombieDRNOAM2																					
ZombieSOAM	☐ ZombieSOAM1	Availa																				
	☐ ZombieSOAM2																					
	☒ ZombieDAMP1																					
	☒ ZombieDAMP2																					

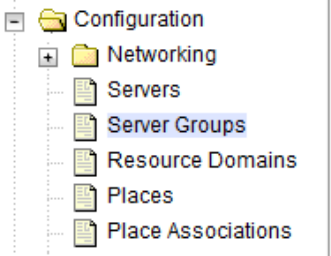
Procedure 32. Configure the MP Server Group(s) and Profile(s)

S T E P #	This procedure will provide the steps to configure MP Server Groups Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PRIMARY NOAM VIP GUI: Login Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of < NOAM_XMI_VIP_IP_Address >: Login as the <i>guiadmin</i> user: 

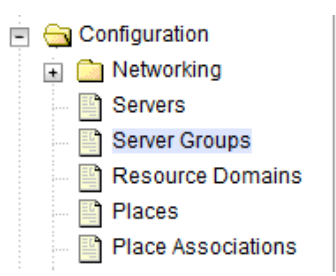
Procedure 32. Configure the MP Server Group(s) and Profile(s)

2 ☐	NOAM VIP GUI: Determine Server Group Function	Determine what server group function will be configured, make note the following configuration decisions. <table border="1"> <thead> <tr> <th>Server Group Function</th><th>MPs Will Run</th><th>Redundancy Model</th></tr> </thead> <tbody> <tr> <td>DSR (multi-active cluster)</td><td>Diameter Relay and Application Services</td><td>Multiple MPs active Per SG</td></tr> <tr> <td>IP Load Balancer</td><td>IPFE application</td><td>1 Active MP Per SG</td></tr> <tr> <td>SS7-IWF</td><td>MAP IWF Application</td><td>1 Active MP Per SG</td></tr> <tr> <td>SBR</td><td>Policy and Charging Session/or Policy Binding Function/Universal SBR</td><td>1 Active MP, 1 Standby MP, 2 Optional Spare Per SG</td></tr> </tbody> </table> For PCA application: - Online Charging function (only) - o At least one MP Server Group with the “SBR” function must be configured - o At least one MP Server Group with the “DSR (multi-active cluster)” function must be configured - o MP Server Groups with the “IP Load Balancer” function (IPFE) are optional. - Policy DRA function - o At least two MP Server Groups with the “SBR” function must be configured. One will store Session data and one will store Binding data. - o At least one MP Server Group with the “DSR (multi-active cluster)” function must be configured - o MP Server Groups with the “IP Load Balancer” function (IPFE) are optional. For DCA application: - o At least one MP Server Group with the “DSR (multi-active cluster)” function must be configured. - o At least one MP Server Group with the “SBR” function may be configured in case of Session based DCA Application. - o NOTE: If PCA application is already functional, then an existing SBR for Session SBR may be re-used instead of configuring a new “SBR”. WAN Replication Connection Count: - For non- SBR Server Groups and “Session Binding Repository” : Default Value - For SBR Server Groups and “Session Binding Repository” SGs: 8 For the PCA application, the following types of MP Server Groups must be configured: - DA-MP (Function: DSR (multi-active cluster)) - SBR (Function: SBR) - IPFE (Function: IP Load Balancer) – Optional) - - For the DCA application, the following types of MP Server Groups must be configured: - DA-MP (Function: DSR (multi-active cluster)) - SBR (Function: Session Binding Repository) = Optional for Session less Apps “OR” SBR (Function: SBR) assigned to Session Resource Domain. - IPFE (Function: IP Load Balancer) – Optional)	Server Group Function	MPs Will Run	Redundancy Model	DSR (multi-active cluster)	Diameter Relay and Application Services	Multiple MPs active Per SG	IP Load Balancer	IPFE application	1 Active MP Per SG	SS7-IWF	MAP IWF Application	1 Active MP Per SG	SBR	Policy and Charging Session/or Policy Binding Function/Universal SBR	1 Active MP, 1 Standby MP, 2 Optional Spare Per SG
Server Group Function	MPs Will Run	Redundancy Model															
DSR (multi-active cluster)	Diameter Relay and Application Services	Multiple MPs active Per SG															
IP Load Balancer	IPFE application	1 Active MP Per SG															
SS7-IWF	MAP IWF Application	1 Active MP Per SG															
SBR	Policy and Charging Session/or Policy Binding Function/Universal SBR	1 Active MP, 1 Standby MP, 2 Optional Spare Per SG															

Procedure 32. Configure the MP Server Group(s) and Profile(s)

3 ☐	NOAM VIP GUI: Enter MP Server Group Data	From the data collected from step 2, create the server group with the following: Navigate to Main Men ->Configuration ->Server Groups  Select Insert Insert Edit Delete Report Fill out the following fields: Server Group Name: <Server Group Name> Level: C Parent: [SOAMP Server Group That is Parent To this MP] Function: Select the Proper Function for this MP Server Group (Gathered in Step 2) Select OK when all fields are filled in.
4 ☐	NOAM VIP GUI: Repeat For Additional Server Groups	Repeat Steps 2-3 for any remaining MP server groups you wish to create. For instance, if you are installing IPFE, you will need to create an IP Load Balancer server group.

Procedure 32. Configure the MP Server Group(s) and Profile(s)

5 ☐	NOAM VIP GUI: Edit the MP Server Groups to include MPs	From the GUI, navigate to Main Menu->Configuration->Server Groups  Select a server group that you just created and then select Edit. Insert Edit Delete Report Select the Network Element that represents the MP server group you wish to edit. Click the Include in SG box for every MP server that you wish to include in <i>this</i> server group. Leave other checkboxes blank. <table border="1" data-bbox="462 907 1263 1108"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>ZombieDAMP1</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> <tr> <td>ZombieDAMP2</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> </tbody> </table> Note: Each IPFE server should be in its own server group. Select OK.	Server	SG Inclusion	Preferred HA Role	ZombieDAMP1	☒ Include in SG	☐ Prefer server as spare	ZombieDAMP2	☒ Include in SG	☐ Prefer server as spare
Server	SG Inclusion	Preferred HA Role									
ZombieDAMP1	☒ Include in SG	☐ Prefer server as spare									
ZombieDAMP2	☒ Include in SG	☐ Prefer server as spare									

Procedure 32. Configure the MP Server Group(s) and Profile(s)

6 ☐	NOAM VIP GUI: [PCA/DCA ONLY] Edit the MP Server Group and add Preferred Spares for Site Redundancy (Optional)	If Two Site Redundancy for the Policy and Charging SBR Server Group/ Session Binding Repository SBR Server Group is wanted, add a MP server that is physically located in a separate site (location) to the Server Group by clicking the Include in SG checkbox and also check the Preferred Spare checkbox. <table border="1" data-bbox="472 432 1406 562"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>ZombieSBRsp</td><td>☒ Include in SG</td><td>☒ Prefer server as spare</td></tr> </tbody> </table> If Three Site Redundancy for the SBR MP Server Group is wanted, add two SBR MP servers that are both physically located in separate sites (<i>location</i>) to the Server Group by clicking the Include in SG checkbox and also check the Preferred Spare checkbox for both servers. Note: The Preferred Spare servers should be different sites from the original server and should not be in the same site. There should be servers from three separate sites (locations). Note: There must first be Non-Preferred spare present the server group before adding the preferred spare. For more information about Site Redundancy for Policy and Charging SBR / Session Binding Repository Server Groups, see the Terminology section. Select OK to save	Server	SG Inclusion	Preferred HA Role	ZombieSBRsp	☒ Include in SG	☒ Prefer server as spare
Server	SG Inclusion	Preferred HA Role						
ZombieSBRsp	☒ Include in SG	☒ Prefer server as spare						
7 ☐	NOAM VIP GUI: Repeat For Additional Server Groups	Repeat Steps 5-6 for any remaining MP server groups you need to edit.						
8 ☐	NOAM VIP GUI: Wait for Remote Database Alarm to Clear	Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding. Navigate to Main menu->Alarms & Events->View Active						

Procedure 32. Configure the MP Server Group(s) and Profile(s)

9 ☐	SOAM VIP GUI: Login	If not already done, establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of: <code>https://<Primary_SOAM_VIP_IP_Address></code> Login to the SOAM GUI as the <i>guiadmin</i> user: 

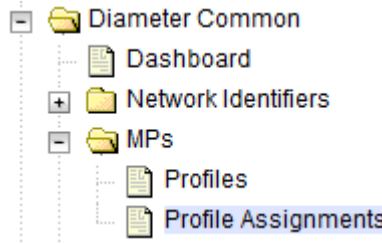
Procedure 32. Configure the MP Server Group(s) and Profile(s)

10

☐

SOAM VIP GUI: Assign Profiles to DA-MPs from SOAM GUI.

Navigate to **Main Menu -> Diameter Common -> MPs -> Profiles Assignments**



Refer to the **DA-MP** section. (If the site has both DSR and MAP-IWF server groups, you will see both a DA-MP section and an SS7-MP section)

Main Menu: Diameter Common -> MPs -> Profile Assignments

DA-MP	MP Profile	current value
ZombieDAMP1	VM:10K_MPS	The current MP Profile for ZombieDAMP1 is VM:10K_MPS . <i>Virtualized DA-MP rated at 10K MPS for all configurations [A value is required.]</i>
ZombieDAMP2	VM:10K_MPS	The current MP Profile for ZombieDAMP2 is VM:10K_MPS . <i>Virtualized DA-MP rated at 10K MPS for all configurations [A value is required.]</i>

For each MP, select the proper profile assignment based on the function each MP will serve:

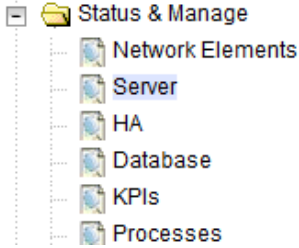
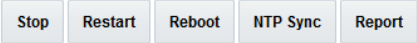
Profile Name	Description
VM:Relay (HP DL380 Gen 8 / Gen 9 (1Gbps) Only)	Virtualized DA-MP on TVOE Guest running the relay application
VM:Database (HP DL380 Gen 8 Only)	Virtualized DA-MP on TVOE Guest running relay and database applications
VM:10K_MPS (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)	Virtualized DA-MP on TVOE Guest running relay, session, and database applications
VM:MD-IWF	Virtualized SS7-MP on TVOE Guest running MD-IWF applications

When finished, press the **Assign** button

Procedure 32. Configure the MP Server Group(s) and Profile(s)

11 ☐	PRIMARY NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of < NOAM_XMI_VIP_IP_Address >: Login as the <i>guiadmin</i> user:  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. <i>Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</i> <i>Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.</i>

Procedure 32. Configure the MP Server Group(s) and Profile(s)

12 ☐	NOAM VIP GUI: Restart MP servers	Navigate to Main menu->Status & Manage->Server  For each MP (SS7-MP, DA-MP, SBR) server: • Select the MP server. • Select the Restart button. • Answer OK to the confirmation popup. Wait for the message which tells you that the restart was successful.  Note: POLICY AND CHARGING DRA INSTALLATIONS/ DCA INSTALLATIONS: You may continue to see alarms related to ComAgent until you complete PCA / DCA installation.

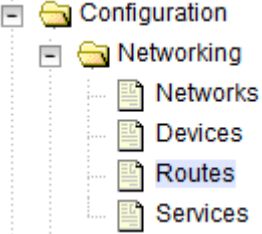
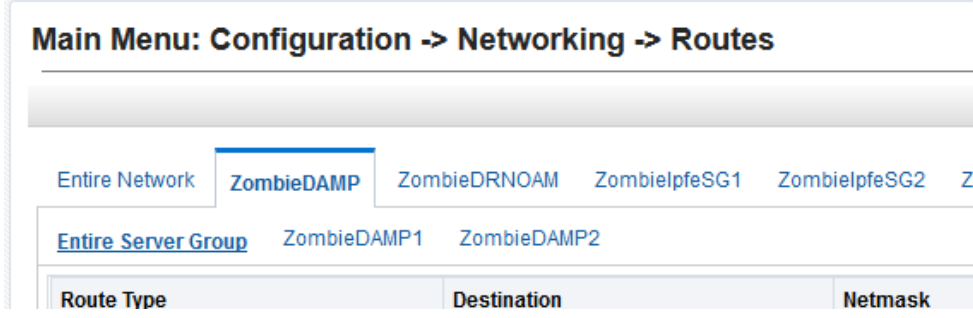
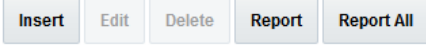
4.14.8 DSR Configuration: Signaling Network**Procedure 33. Configure the Signaling Network Routes**

S T E P #	This procedure will provide the steps to configure Signaling Network Routes on MP-type servers (DA-MP, SBRs, IPFE, SS7-MP, etc.) Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

Procedure 33. Configure the Signaling Network Routes

1 ☐	PRIMARY NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of < NOAM_XMI_VIP_IP_Address >: Login as the <i>guiadmin</i> user: 

Procedure 33. Configure the Signaling Network Routes

2 ☐	NOAM VIP GUI: Navigate to Routes Configuration Screen	Navigate to Main Menu -> Configuration -> Networking -> Routes  Select the first MP Server group you see listed on the first row of tabs as shown, then click the Entire Server Group link. Initially, no routes should be displayed.  Note: For SBRs that span multiple sites, routes should be added individually.
3 ☐	NOAM VIP GUI: Add Route	Click on Insert at the bottom of the screen to add additional routes. 

Procedure 33. Configure the Signaling Network Routes

4 ☐	NOAM VIP GUI: Add Default Route for MPs Going Through Signaling Network Gateway (Optional)	OPTIONAL - Only execute this step if you performed Procedure 30 Step 14: which removed the XML gateway default route on MPs If your MP servers no longer have a default route, then you can now insert a default route here which uses one of the signaling network gateways. Main Menu: Configuration -> Networking -> Info* ▼ Insert Route on ZombieDAMP <table border="1"> <thead> <tr> <th>Field</th><th>Value</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Route Type *</td><td> ☐ Net ☒ Default ☐ Host </td><td>Select a route type. </td></tr> <tr> <td>Device *</td><td>xsi1 ▼</td><td>Select the network c</td></tr> <tr> <td>Destination</td><td></td><td>The destination net</td></tr> <tr> <td>Netmask</td><td></td><td>A valid netmask for l</td></tr> <tr> <td>Gateway IP *</td><td></td><td>The IP address of th</td></tr> </tbody> </table> Ok Apply Cancel Route Type: Default Device: Select the signaling device that is directly attached to the network where the XSI default gateway resides. Gateway IP: The XSI gateway you wish to use for default signaling network access. Select OK Ok Apply Cancel	Field	Value	Description	Route Type *	☐ Net ☒ Default ☐ Host	Select a route type.	Device *	xsi1 ▼	Select the network c	Destination		The destination net	Netmask		A valid netmask for l	Gateway IP *		The IP address of th
Field	Value	Description																		
Route Type *	☐ Net ☒ Default ☐ Host	Select a route type.																		
Device *	xsi1 ▼	Select the network c																		
Destination		The destination net																		
Netmask		A valid netmask for l																		
Gateway IP *		The IP address of th																		

Procedure 33. Configure the Signaling Network Routes

5 ☐	NOAM VIP GUI: Add Network Routes for Diameter Peers	Use this step to add IPv4 and/or IPv6 routes to <i>diameter</i> peer destination networks. The goal here is to ensure that diameter traffic uses the gateway(s) on the signaling networks. Insert Route on ZombieDAMP <table border="1"> <thead> <tr> <th>Field</th><th>Value</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Route Type *</td><td> ☒ Net ☐ Default ☐ Host </td><td>Select a route type. [Default = N/A. Options = Net, Default, Host. You</td></tr> <tr> <td>Device *</td><td>xsi1</td><td>Select the network device name through which traffic is being route</td></tr> <tr> <td>Destination</td><td>10.240.55.0</td><td>The destination network address. [Default = N/A. Range = Valid Net</td></tr> <tr> <td>Netmask</td><td>255.255.255.0</td><td>A valid netmask for the network route destination IP address. [Defai</td></tr> <tr> <td>Gateway IP *</td><td>10.196.227.1</td><td>The IP address of the gateway for this route. [Default = N/A. Range :</td></tr> </tbody> </table> Route Type: Net Device: Select the appropriate signaling interface that will be used to connect to that network Destination: Enter the Network ID of Network to which the peer node is connected to. Netmask: Enter the corresponding Netmask. Gateway IP: Enter the Int-XSI switch VIP of the chosen Network for L3 deployments (either of int-XSI-1 or of int-XSI2). Or the IP of the customer gateway for L2 deployments. If you have more routes to enter, Press Apply to save the current route entry and repeat this step to enter more routes If you are finished entering routes, Press OK to save the latest route and leave this screen. If aggregation switches are used, routes should be configured on the aggregation switches so that the destination networks configured in this step are reachable. This can be done by running the following netconfig commands from the site's local PMAC (examples shown -- actual values will vary) : Add routes (IPv4 & IPv6): <pre> \$ sudo netConfig --device=switch1A addRoute network=10.10.10.0 mask=255.255.255.0 nexthop=10.50.76.81 \$ sudo netConfig --device=switch1A addRoute network6=2001::/64 nexthop=fd0f::1 </pre> Delete routes (IPv4 & IPv6): <pre> \$ sudo netConfig --device=switch1A deleteRoute network=10.10.10.0 mask=255.255.255.0 nexthop=10.50.76.81 \$ sudo netConfig --device=switch1A deleteRoute network6=2001::/64 nexthop=fd0f::1 </pre>	Field	Value	Description	Route Type *	☒ Net ☐ Default ☐ Host	Select a route type. [Default = N/A. Options = Net, Default, Host. You	Device *	xsi1	Select the network device name through which traffic is being route	Destination	10.240.55.0	The destination network address. [Default = N/A. Range = Valid Net	Netmask	255.255.255.0	A valid netmask for the network route destination IP address. [Defai	Gateway IP *	10.196.227.1	The IP address of the gateway for this route. [Default = N/A. Range :
Field	Value	Description																		
Route Type *	☒ Net ☐ Default ☐ Host	Select a route type. [Default = N/A. Options = Net, Default, Host. You																		
Device *	xsi1	Select the network device name through which traffic is being route																		
Destination	10.240.55.0	The destination network address. [Default = N/A. Range = Valid Net																		
Netmask	255.255.255.0	A valid netmask for the network route destination IP address. [Defai																		
Gateway IP *	10.196.227.1	The IP address of the gateway for this route. [Default = N/A. Range :																		

Procedure 33. Configure the Signaling Network Routes

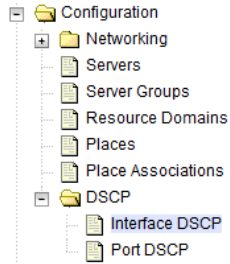
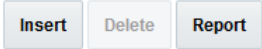
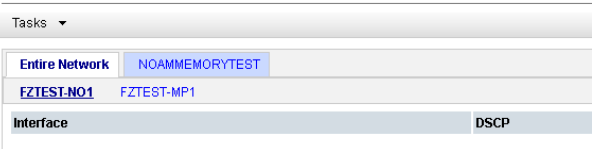
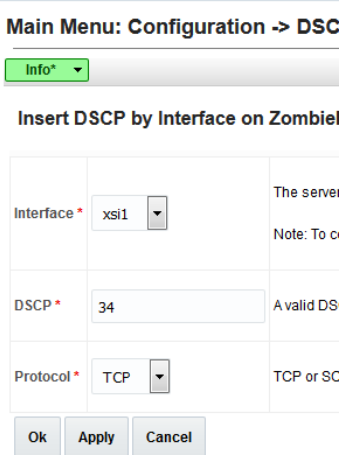
6 ☐	NOAM VIP GUI: Repeat for all other MP server groups.	The routes entered in this procedure should now be configured on all MPs in the server group for the first MP you selected. If you have additional MP server groups, repeat from step 2, but this time, select an MP from the next MP server group. Continue until you have covered all MP server groups. This includes DAMP, IPFE, and SS7MP servers. Note: IPFE and DAMP servers must have the same routes configured.

4.14.9 DSR Configuration: DSCP (Optional)

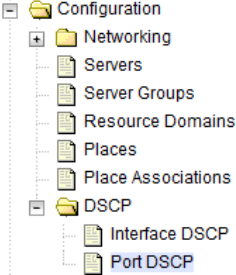
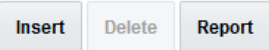
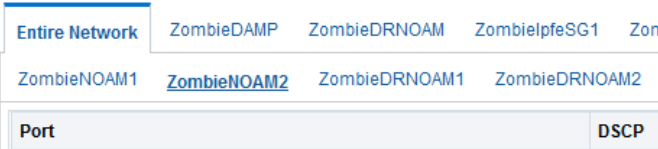
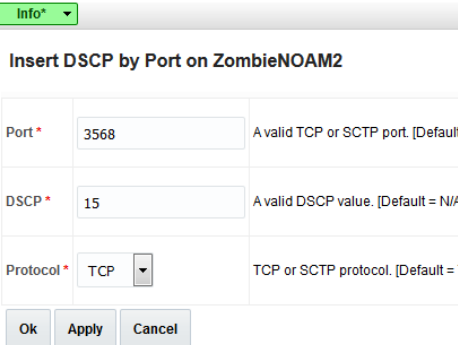
Procedure 34. Configure DSCP Values for Outgoing Traffic (Optional)

S T E P #	This procedure will provide the steps to configure the DSCP values for outgoing packets on servers. DSCP values can be applied to an outbound interface as a whole, or to all outbound traffic using a specific TCP or SCTP source port. This step is optional and should only be executed if has been decided that your network will utilize packet DSCP markings for Quality-of-Service purposes. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PRIMARY NOAM VIP GUI: Login Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of < NOAM_XMI_VIP_IP_Address >: Login as the <i>guiadmin</i> user:  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 34. Configure DSCP Values for Outgoing Traffic (Optional)

2 ☐	NOAM VIP GUI: Option 1: Configure Interface DSCP	Note: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary. Navigate to Main Menu -> Configuration -> DSCP -> Interface DSCP  Select the server you wish to configure from the list of servers on the 2nd line. (You can view all servers with Entire Network selected; or limit yourself to a particular server group by clicking on that server group name's tab). Click Insert  Main Menu: Configuration -> DSCP -> Interface DSCP  Select the network interface from the drop down box, then enter the <i>DSCP value</i> you wish to have applied to packets leaving this interface. Main Menu: Configuration -> DSC  Click OK if there are no more interfaces on this server to configure, or Apply to finish this interface and continue on with more interfaces by selecting them from the drop down and entering their <i>DSCP values</i>.

Procedure 34. Configure DSCP Values for Outgoing Traffic (Optional)

3 ☐	NOAM VIP GUI: Option 2: Configure Port DSCP	Note: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary. Navigate to Main Menu -> Configuration -> DSCP -> Port DSCP  Select the server you wish to configure from the list of servers on the 2nd line. (You can view all servers with Entire Network selected; or limit yourself to a particular server group by clicking on that server group name's tab). Click Insert  Main Menu: Configuration -> DSCP -> Port DSCP  Enter the source port, DSCP value, and select the transport protocol. Main Menu: Configuration -> DSCP -> Port DSCP  Click OK if there are no more port DSCPs on this server to configure, or Apply to finish this port entry and continue entering more port <i>DSCP mappings</i>.

Procedure 34. Configure DSCP Values for Outgoing Traffic (Optional)

4 ☐	NOAM VIP GUI: Repeat for additional servers.	Repeat Steps 2-3 for all remaining servers.

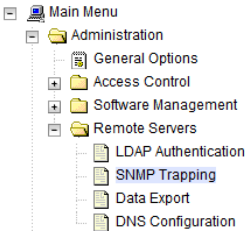
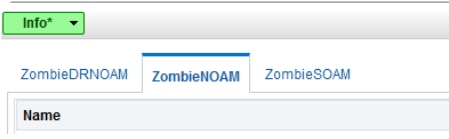
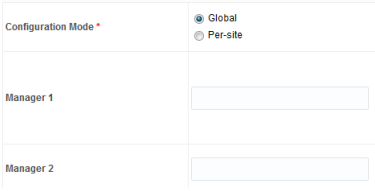
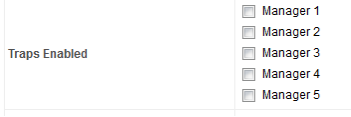
4.14.10 DSR Configuration: SNMP**Procedure 35. Configure SNMP Trap Receiver(s)**

S T E P #	This procedure will provide the steps to configure forwarding of SNMP Traps from each individual server. NOTE: If SNMP configuration is not required, skip to step 5. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

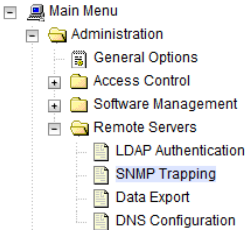
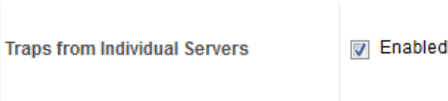
Procedure 35. Configure SNMP Trap Receiver(s)

1 ☐	PRIMARY NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of <code><Primary_DSR_NOAM_VIP_IP_Address></code>: Login as the guiadmin user: 

Procedure 35. Configure SNMP Trap Receiver(s)

2 ☐	NOAM VIP GUI: Configure System-Wide SNMP Trap Receiver(s)	Navigate to Main Menu -> Administration -> Remote Servers -> SNMP Trapping  Select the Server Group tab for SNMP trap configuration: Main Menu: Administration -> Remote Servers  Fill in the IP address or hostname of the Network Management Station (NMS) you wish to forward traps to. This IP should be reachable from the NOAMP's "XMI" network. Continue to fill in additional secondary, tertiary, etc. Manager IPs in the corresponding slots if desired. SNMP Trap Configuration Insert for ZombieNOAM  Check Traps Enabled boxes for the Manager servers being configured:  Enter the SNMP Community Name:  Leave all other fields at their default values. Press OK

Procedure 35. Configure SNMP Trap Receiver(s)

3 ☐	NOAMP VIP: Enable Traps from Individual Servers (Optional)	Note: By default SNMP traps from MPs are aggregated and then displayed at the active NOAMP. If instead, you wish for every server to send its own traps directly to the NMS, then execute this procedure. This procedure requires that all servers, including MPs, have an XMI interface on which the customer SNMP Target server (NMS) is reachable. Navigate to Main Menu -> Administration -> Remote Servers -> SNMP Trapping  Make sure the checkbox next to Enabled is checked, if not, check it as shown below  Then click on Apply and verify that the data is committed.
4 ☐	PMAC: Update the TVOE Host SNMP Community String	Establish an SSH session to the PMAC, login as admusr. Execute the following command to update the TVOE host community string: <pre>\$ sudo pmaccli setCommStr --accessType=rw --commStr=<site specific value></pre> Note: When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest on the PMAC control network will be updated. All those servers that match the existing Site Specific Community String will not be updated again until the string name is changed.

5 ☐	(Workaround) PRIMARY NOAM VIP GUI: Login	NOTE: This workaround step should be performed only in the following cases: 1) If SNMP is not configured (i.e, if above steps 1-4 are skipped) 2) 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, as PMAC does not support SNMPv3. Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of < NOAM_XMI_VIP_IP_Address > Login as the <i>guiadmin</i> user: 

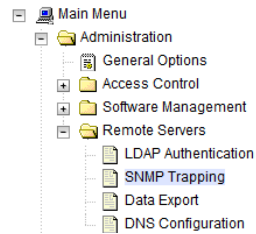
Procedure 35. Configure SNMP Trap Receiver(s)

6



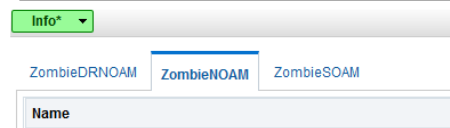
NOAM VIP GUI:
Configure
System-Wide
SNMP Trap
Receiver(s)

Navigate to **Main Menu -> Administration -> Remote Servers -> SNMP Trapping**



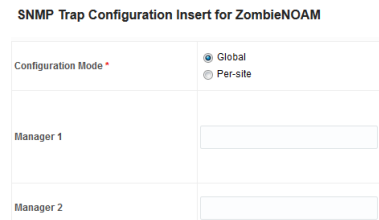
Select the Server Group tab for SNMP trap configuration:

Main Menu: Administration -> Remote Servers



Fill in the IP address or hostname of the Network Management Station (NMS) you wish to forward traps to. This IP should be reachable from the NOAMP's "XMI" network. (If already configured SNMP with **SNMPv3** as enabled version, another server needs to be configured here)

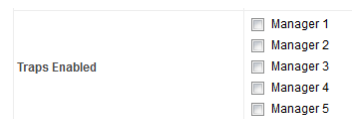
Continue to fill in additional secondary, tertiary, etc. Manager IPs in the corresponding slots if desired.



Set the Enabled Versions as **SNMPv2c and SNMPv3**:



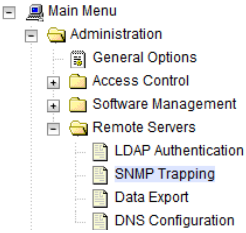
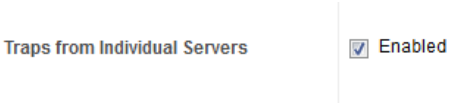
Check Traps Enabled boxes for the Manager servers being configured:



Enter the **SNMP Community Name**:

SNMPv2c Read-Only Community Name	
SNMPv2c Read-Write Community Name	

Procedure 35. Configure SNMP Trap Receiver(s)

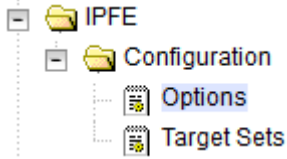
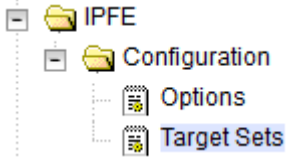
7 ☐	NOAMP VIP: Enable Traps from Individual Servers (Optional)	Note: By default SNMP traps from MPs are aggregated and then displayed at the active NOAMP. If instead, you wish for every server to send its own traps directly to the NMS, then execute this procedure. This procedure requires that all servers, including MPs, have an XMI interface on which the customer SNMP Target server (NMS) is reachable. Navigate to Main Menu -> Administration -> Remote Servers -> SNMP Trapping  Make sure the checkbox next to Enabled is checked, if not, check it as shown below  Then click on Apply and verify that the data is committed.
8 ☐	PMAC: Update the TVOE Host SNMP Community String	Establish an SSH session to the PMAC, login as admusr. Execute the following command to update the TVOE host community string: <pre>\$ sudo pmaccli setCommStr --accessType=rw --commStr=<site specific value></pre> Note: When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest on the PMAC control network will be updated. All those servers that match the existing Site Specific Community String will not be updated again until the string name is changed.
9 ☐	Restore SNMPv3 (Optional)	Refer to Appendix T: Restoring SNMP configuration to SNMPv3 (Optional) to restore SNMPv3 after installation, if required

4.14.11 DSR Configuration: IP Front End (IPFE)

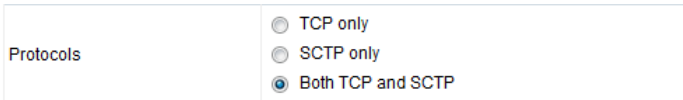
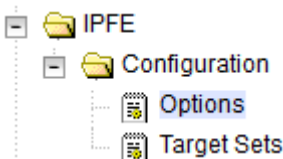
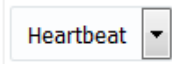
Procedure 36. IP Front End (IPFE) Configuration (Optional)

S T E P #	This procedure will provide the steps to configure IP Front End (IPFE), and optimize performance. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	SOAM VIP GUI: Login Establish a GUI session on the SOAM server the VIP IP address of the SOAM server. Open the web browser and enter a URL of: <a href="https://<Primary_SOAM_VIP_IP_Address>">https://<Primary_SOAM_VIP_IP_Address> Login to the SOAM GUI as the <i>guiadmin</i> user: 

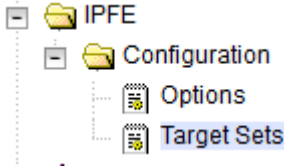
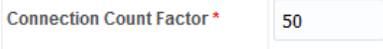
Procedure 36. IP Front End (IPFE) Configuration (Optional)

2 ☐	SOAM VIP GUI: Configuration of replication IPFE association data.	Select Main Menu -> IPFE -> Configuration -> Options  Enter the IP address of the 1st IPFE in the IPFE-A1 IP Address field and the IP address of the 2nd IPFE in the IPFE-A2 IP Address field If applicable, enter the address of the 3rd and 4th IPFE servers in IPFE-B1 IP Address and IPFE-B2 IP Address fields. Configuration Options <table border="1"> <thead> <tr> <th>Variable</th><th>Value</th><th>Description</th></tr> </thead> <tbody> <tr> <td colspan="3">Inter-IPFE Synchronization</td> </tr> <tr> <td>IPFE-A1 IP Address</td><td>169.254.1.11 - ZombieIPFE1</td><td>IPv4 or IPv6 This selection</td></tr> <tr> <td>IPFE-A2 IP Address</td><td>169.254.1.12 - ZombieIPFE2</td><td>IPv4 or IPv6 This selection</td></tr> </tbody> </table> Note: It is recommended that the address reside on the IMI (Internal Management Interface) network. Note: IPFE-A1 and IPFE-A2 must have connectivity between each other via these addresses. The same applies with IPFE-B1 and IPFE-B2. Note: Accept default configuration for remaining entries	Variable	Value	Description	Inter-IPFE Synchronization			IPFE-A1 IP Address	169.254.1.11 - ZombieIPFE1	IPv4 or IPv6 This selection	IPFE-A2 IP Address	169.254.1.12 - ZombieIPFE2	IPv4 or IPv6 This selection
Variable	Value	Description												
Inter-IPFE Synchronization														
IPFE-A1 IP Address	169.254.1.11 - ZombieIPFE1	IPv4 or IPv6 This selection												
IPFE-A2 IP Address	169.254.1.12 - ZombieIPFE2	IPv4 or IPv6 This selection												
3 ☐	SOAM VIP GUI: Configuration of IPFE Target sets-Part 1 (Insert Target Set)	Select Main Menu -> IPFE -> Configuration -> Target Sets  Select either Insert IPv4 or Insert IPv6 button, depending on the IP version of the target set you plan to use. Insert IPv4 Insert IPv6 Edit Delete												

Procedure 36. IP Front End (IPFE) Configuration (Optional)

4 ☐	SOAM VIP GUI: Configuration of IPFE Target sets-Part 2 (Target Set Configuration)	Continued from the previous step, the following are configurable: Protocols: protocols the target set will support.  Delete Age: Specifies when the IPFE should remove its association data for a connection. Any packets presenting a source IP address/port combination that had been previously stored as association state but have been idle longer than the Delete Age configuration will be treated as a new connection and will not automatically go to the same application server.  Load Balance Algorithm: <i>Hash</i> or <i>Least Load</i> options  Note: In order for the IPFE to provide Least Load distribution, Main Menu -> IPFE -> Configuration -> Options, Monitoring Protocol must be set to Heartbeat so that the application servers can provide the load information the IPFE uses to select the least-loaded server for connections.  Monitoring Protocol *  Note: The Least Load option is the default setting, and is the recommended option with exception of unique backward compatibility scenarios. Execute the following command if Hash Load Balance Algorithm was selected above. (advise cut and paste to prevent errors): Establish an SSH session to the SOAM VIP, login as admusr. <pre>\$ sudo iset -fvalue="50" DpiOption where "name='MpEngIngressMpsPercentile'" === changed 1 records ===</pre>

Procedure 36. IP Front End (IPFE) Configuration (Optional)

5 ☐	SOAM VIP GUI: Configuration of IPFE Target sets-Part 3 (Target Set Configuration)	From Main Menu -> IPFE -> Configuration -> Target Sets  (Optional): If you have selected the Least Load algorithm, you may configure the following fields to adjust the algorithm's behavior: MPS Factor – Messages per Second (MPS) is one component of the least load algorithm. This field allows you to set it from 0 (not used in load calculations) to 100 (the only component used for load calculations). It is recommended that IPFE connections have Reserved Ingress MPS set to something other than the default, which is 0.  Connection Count Factor – This is the other component of the least load algorithm. This field allows you to set it from 0 (not used in load calculations) to 100 (the only component used for load calculations). Increase this setting if connection storms (the arrival of many connections at a very rapid rate) are a concern.  To configure Reserved Ingress MPS, go to Main Menu -> Diameter -> Configuration -> Configuration Sets -> Capacity Configuration Sets. If you choose not to use Reserved Ingress MPS, set MPS Factor to 0 and Connection Count Factor, described below, to 100. Connection Count Factor – This is the other component of the least load algorithm. This field allows you to set it from 0 (not used in load calculations) to 100 (the only component used for load calculations). Increase this setting if connection storms (the arrival of many connections at a very rapid rate) are a concern. Allowed Deviation - Percentage within which two application server's load calculation results are considered to be equal. If very short, intense connection bursts are expected to occur, increase the value to smooth out the distribution. 

Procedure 36. IP Front End (IPFE) Configuration (Optional)

6	☐	SOAM VIP GUI: Configuration of IPFE Target sets-Part 4 (Target Set Configuration)	Primary Public IP Address: IP address for the target set Public IP Address Address * Active IPFE ☒ IPFE A1 ☐ IPFE A2 ☐ IPFE B1 ☐ IPFE B2 Note: This address must reside on the XSI (External Signaling Interface) network because it will be used by the application clients to reach the application servers. This address MUST NOT be a real interface address (that is, must not be associated with a network interface card). Active IPFE: IPFE to handle the traffic for the target set address. Secondary Public IP Address: If this target set supports either multi-homed SCTP or Both TCP and SCTP, provide a Secondary IP Address. Alternate Public IP Address* Alternate Address Active IPFE for alternate address ☒ IPFE A1 ☐ IPFE A2 ☐ IPFE B1 ☐ IPFE B2 Note: A secondary address is required to support SCTP multi-homing. A secondary address can support TCP, but the TCP connections will not be multi-homed. Note: If SCTP multi-homing is to be supported, select the mate IPFE of the Active IPFE for the Active IPFE for secondary address to ensure that SCTP failover functions as designed. Target Set IP List: Select an IP address, a secondary IP address if supporting SCTP multi-homing, a description, and a weight for the application server. Target Set IP List <table border="1"> <thead> <tr> <th>IP Address</th> <th>Alternate IP Address</th> <th>Description</th> <th>Weighting</th> </tr> </thead> <tbody> <tr> <td>01 - Select -</td> <td>- Select -</td> <td></td> <td>100 X</td> </tr> </tbody> </table> Add Weighting range is 0 - 65535. Note: The IP address must be on the XSI network since they must be on the same network as the target set address. This address must also match the IP version of the target set address (IPv4 or IPv6). If the Secondary Public IP Address is configured, it must reside on the same application server as the first IP address. Note: If all application servers have an equal weight (e.g., 100, which is the default), they have an equal chance of being selected. Application servers with larger weights have a greater chance of being selected. Click the Add button to add more application servers (Up to 16) Click the Apply button. Ok Apply Cancel	IP Address	Alternate IP Address	Description	Weighting	01 - Select -	- Select -		100 X
IP Address	Alternate IP Address	Description	Weighting								
01 - Select -	- Select -		100 X								

Procedure 36. IP Front End (IPFE) Configuration (Optional)

7 ☐	SOAM VIP GUI: Repeat for additional Configuration of IPFE Target sets.	Repeat steps 3-6 for each target set (Up to 16). At least one target set must be configured.

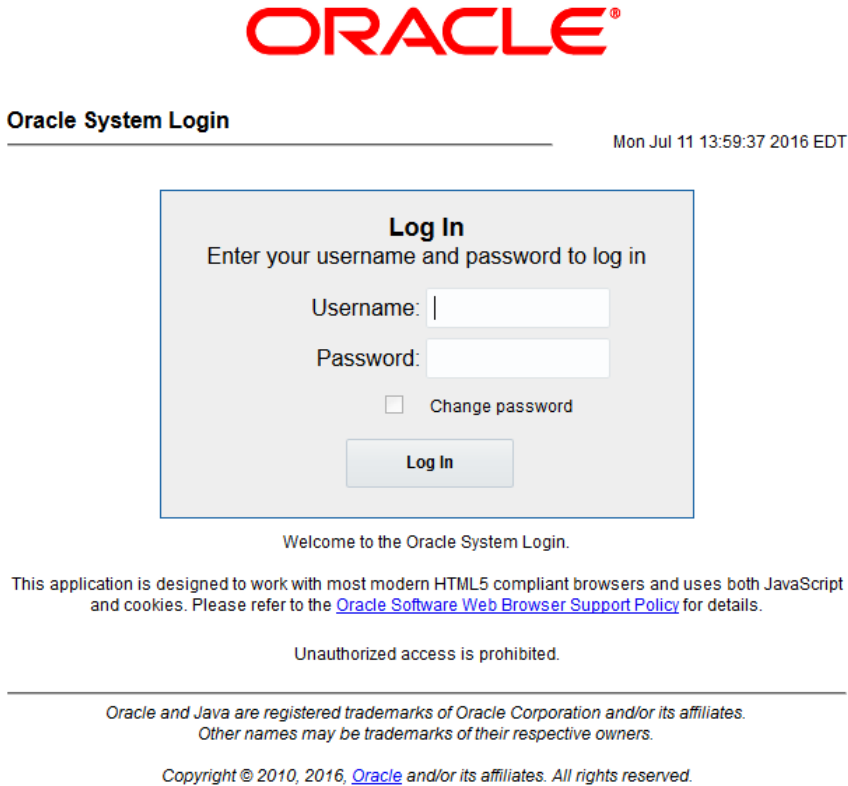
4.15 Application Configuration: SDS

4.15.1 SDS Configuration: NOAMs

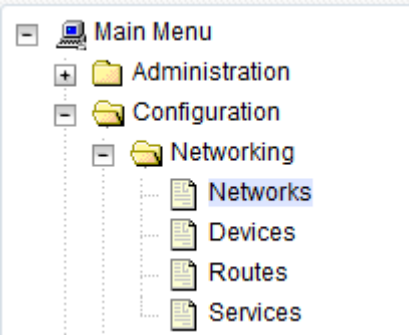
Procedure 37. Configure First SDS NOAM NE and Server

S T E P #	This procedure will provide the steps to configure the First NOAM server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Save the NOAM Network Data to an XML file	Using a text editor, create a SDS NOAM Network Element file that describes the networking of the target install environment of your first SDS NOAM server. Select an appropriate file name and save the file to a known location on your computer. A suggested filename format is “Appname_NName_NetworkElement.XML”, so for example a SDS NOAM network element XML file would have a filename “SDS_NOAM_NetworkElement.xml”. Alternatively, you can update the sample SDS Network Element file. It can be found on the management server at: <pre>/usr/TKLC/smac/html/TPD/<DSR Release>/upgrade/overlay/SAMPLE-NetworkElement.xml</pre> A sample XML file can also be found in Appendix L: Sample Network Element. Note: The following limitations apply when specifying a Network Element name: A 1-32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.

Procedure 37. Configure First SDS NOAM NE and Server

2 ☐	SDS NOAM GUI: Login	Using the xmi IP address defined and configured in the DSR fast deployment configuration file (rms.cfg). Login to the SDS NOAM GUI as the <i>guiadmin</i> user: 

Procedure 37. Configure First SDS NOAM NE and Server

3 ☐	Create the SDS NOAM Network Element using the XML File	Navigate to Main Menu->Networking -> Networks  Select the Browse button, and enter the pathname of the NOAM network XML file: To create a new Network Element, upload a valid configuration file: Browse... SDSzombie.xml Upload File Select the Upload File button to upload the XML file and configure the NOAM Network Element. Once the data has been uploaded, you should see a tab appear with the name of your network element. Click on this tab and you will get a window which describes the individual networks that are now configured: Main Menu: Configuration -> Networking -> Networks info* Global ZombieNOAM ⓘ <table border="1"> <thead> <tr> <th>Network Name</th> <th>Network Type</th> <th>Default</th> <th>Locked</th> <th>Routed</th> <th>VLAN</th> <th>Configured Interfaces</th> <th>Network</th> </tr> </thead> <tbody> <tr> <td>XMI</td> <td>OAM</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>4</td> <td>0</td> <td>10.240.213.0/24</td> </tr> <tr> <td>IMI</td> <td>OAM</td> <td>No</td> <td>Yes</td> <td>No</td> <td>3</td> <td>0</td> <td>169.254.1.0/24</td> </tr> </tbody> </table>	Network Name	Network Type	Default	Locked	Routed	VLAN	Configured Interfaces	Network	XMI	OAM	Yes	Yes	Yes	4	0	10.240.213.0/24	IMI	OAM	No	Yes	No	3	0	169.254.1.0/24
Network Name	Network Type	Default	Locked	Routed	VLAN	Configured Interfaces	Network																			
XMI	OAM	Yes	Yes	Yes	4	0	10.240.213.0/24																			
IMI	OAM	No	Yes	No	3	0	169.254.1.0/24																			

Procedure 37. Configure First SDS NOAM NE and Server

6

☐

Map Services to Networks

Navigate to **Main Menu ->Configuration-> Services**.

Select the **Edit** button and set the Services as shown in the table below:

Name	Intra-NE Network	Inter-NE Network
OAM	<IMI Network>	<XMI Network>
Replication	<IMI Network>	<XMI Network>
Signaling	Unspecified	Unspecified
HA_Secondary	<IMI Network>	<XMI Network>
HA_MP_Secondary	<IMI Network>	<XMI Network>
Replication_MP	<IMI Network>	<XMI Network>
ComAgent	<IMI Network>	<XMI Network>

For example, if your IMI network is named **IMI** and your XMI network is named **XMI**, then your services config should look like the following:

Services

Name	Intra-NE Network	Inter-NE Network
OAM	INTERNALIMI ▾	INTERNALXMI ▾
Replication	INTERNALIMI ▾	INTERNALXMI ▾
Signaling	Unspecified ▾	Unspecified ▾
HA_Secondary	INTERNALIMI ▾	INTERNALXMI ▾
HA_MP_Secondary	INTERNALIMI ▾	INTERNALXMI ▾
Replication_MP	INTERNALIMI ▾	INTERNALXMI ▾
ComAgent	INTERNALIMI ▾	INTERNALXMI ▾

Select the **Ok** button to apply the Service-to-Network selections.

Procedure 37. Configure First SDS NOAM NE and Server

7 ☐	Insert the 1st SDS NOAM server	Navigate to Main Menu -> Configuration -> Servers. Select the Insert button to insert the new SDS NOAM server into servers table (the first or server). <table border="1"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Hostname *</td> <td>ZombieSDSNOAM1</td> </tr> <tr> <td>Role *</td> <td>NETWORK OAM&P</td> </tr> <tr> <td>System ID</td> <td></td> </tr> <tr> <td>Hardware Profile</td> <td>SDS TVOE Guest</td> </tr> <tr> <td>Network Element Name *</td> <td>ZombieSDSNOAM</td> </tr> <tr> <td>Location</td> <td>pc5010441</td> </tr> </tbody> </table> Fill in the fields as follows: Hostname: <Hostname> Role: NETWORK OAM&P System ID: <Site System ID> Hardware Profile: SDS TVOE Guest Network Element Name: [Choose NE from Drop Down Box] Location: <NOAM Server Location> The network interface fields will now become available with selection choices based on the chosen hardware profile and network element <table border="1"> <tbody> <tr> <td>XMI (10.240.213.0/24)</td> <td>10.240.213.20</td> <td>xmi</td> <td>☐ VLAN (4)</td> </tr> <tr> <td>IMI (169.254.1.0/24)</td> <td>169.254.1.20</td> <td>imi</td> <td>☐ VLAN (3)</td> </tr> </tbody> </table> Fill in the server IP addresses for the XMI network. Select xmi for the interface. Leave the "VLAN" checkbox unchecked. Fill in the server IP addresses for the IMI network. Select imi for the interface. Leave the "VLAN" checkbox unchecked. Next, add the following NTP servers: <table border="1"> <thead> <tr> <th>NTP Server</th> <th>Preferred?</th> </tr> </thead> <tbody> <tr> <td><1st NOAM-TVOE-IP-Address></td> <td>Yes</td> </tr> </tbody> </table> Select the Ok button when you have completed entering all the server data.	Attribute	Value	Hostname *	ZombieSDSNOAM1	Role *	NETWORK OAM&P	System ID		Hardware Profile	SDS TVOE Guest	Network Element Name *	ZombieSDSNOAM	Location	pc5010441	XMI (10.240.213.0/24)	10.240.213.20	xmi	☐ VLAN (4)	IMI (169.254.1.0/24)	169.254.1.20	imi	☐ VLAN (3)	NTP Server	Preferred?	<1st NOAM-TVOE-IP-Address>	Yes
Attribute	Value																											
Hostname *	ZombieSDSNOAM1																											
Role *	NETWORK OAM&P																											
System ID																												
Hardware Profile	SDS TVOE Guest																											
Network Element Name *	ZombieSDSNOAM																											
Location	pc5010441																											
XMI (10.240.213.0/24)	10.240.213.20	xmi	☐ VLAN (4)																									
IMI (169.254.1.0/24)	169.254.1.20	imi	☐ VLAN (3)																									
NTP Server	Preferred?																											
<1st NOAM-TVOE-IP-Address>	Yes																											

Procedure 37. Configure First SDS NOAM NE and Server

8 ☐	Export the Initial Configuration	Navigate to Main Menu -> Configuration -> Servers. From the GUI screen, select the SDS NOAM server and then select Export to generate the initial configuration data for that server.
9 ☐	SDS NOAM iLO: Copy Configuration File to 1 st SDS NOAM Server	Obtain a terminal window to the 1st SDS NOAM server, logging in as the admusr user. Copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the 1st SDS NOAM to the /var/tmp directory. The configuration file will have a filename like TKLCConfigData.<hostname>.sh. The following is an example: <pre>\$ sudo cp /var/TKLC/db/filemgmt/TKLCConfigData.RMS01.sh /var/tmp/TKLCConfigData.sh</pre>
10 ☐	SDS NOAM iLO: Wait for Configuration to Complete	The automatic configuration daemon will look for the file named “TKLCConfigData.sh” in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server. Wait to be prompted to reboot the server, but DO NOT reboot the server, it will be rebooted later on in this procedure. Note: Ignore the warning about removing the USB key, since no USB key is present.
11 ☐	SDS NOAM iLO: Set the Time zone and Reboot the Server	From the command line prompt, execute set_ini_tz.pl. This will set the system time zone. The following command example uses the America/New_York time zone. Replace as appropriate with the time zone you have selected for this installation. For a full list of valid time zones, see Appendix J: List of Frequently used Time Zones. <pre>\$ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York" >/dev/null 2>&1</pre> <pre>\$ sudo init 6</pre>

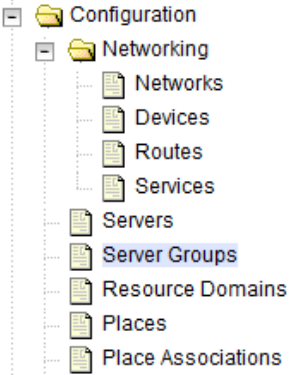
Procedure 37. Configure First SDS NOAM NE and Server

12 ☐	1st SDS NOAM Server: Verify Server Health	Execute the following command on the 1st SDS NOAM server and make sure that no errors are returned: <pre>\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

Procedure 38. Configure the SDS NOAM Server Group

S T E P #	This procedure will provide the steps to configure the SDS NOAM server group. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	SDS NOAM GUI: Login	Establish a GUI session on the first SDS NOAM server by using the XMI IP address of the first SDS NOAM server. Open the web browser and enter a URL of: <code>https://<SDS_NO1_XMI_IP_Address></code> Login as the <i>guiadmin</i> user:  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 38. Configure the SDS NOAM Server Group

2 ☐	SDS NOAM GUI: Enter NOAM Server Group Data	Navigate to Main Menu -> Configuration -> Server Groups  Select Insert Insert Edit Delete Report Fill the following fields: • Server Group Name: <Enter Server Group Name> • Level: A • Parent : None • Function: SDS • WAN Replication Connection Count: Use Default Value Adding new server group <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Server Group Name *</td> <td> SDSNOAM </td> <td>Unique iden required.]</td> </tr> <tr> <td>Level *</td> <td> A ▼</td> <td>Select one o</td> </tr> <tr> <td>Parent *</td> <td> NONE ▼</td> <td>Select an ex</td> </tr> <tr> <td>Function *</td> <td> SDS ▼</td> <td>Select one o</td> </tr> <tr> <td>WAN Replication Connection Count</td> <td> 1 </td> <td>Specify the r</td> </tr> </tbody> </table> Select OK when all fields are filled in.	Field	Value	Description	Server Group Name *	SDSNOAM	Unique iden required.]	Level *	A ▼	Select one o	Parent *	NONE ▼	Select an ex	Function *	SDS ▼	Select one o	WAN Replication Connection Count	1	Specify the r
Field	Value	Description																		
Server Group Name *	SDSNOAM	Unique iden required.]																		
Level *	A ▼	Select one o																		
Parent *	NONE ▼	Select an ex																		
Function *	SDS ▼	Select one o																		
WAN Replication Connection Count	1	Specify the r																		

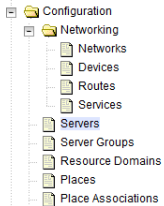
Procedure 38. Configure the SDS NOAM Server Group

3 ☐	SDS NOAM GUI: Edit the SDS NOAM Server Group	From the GUI Main Menu -> Configuration -> Server Groups. Select the new server group, and then select Edit Insert Edit Delete Report Select the Network Element that represents the SDS NOAM. <table border="1" data-bbox="462 493 1380 640"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>ZombieSDSNOAM1</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> </tbody> </table> In the portion of the screen that lists the servers for the server group, find the SDS NOAM server being configured. Click the Include in SG checkbox. Leave other boxes blank. Press OK	Server	SG Inclusion	Preferred HA Role	ZombieSDSNOAM1	☒ Include in SG	☐ Prefer server as spare
Server	SG Inclusion	Preferred HA Role						
ZombieSDSNOAM1	☒ Include in SG	☐ Prefer server as spare						
4 ☐	SDS NOAM GUI: Restart 1 st SDS NOAM Server	From the SDS NOAM GUI, select the Main menu -> Status & Manage -> Server menu. <pre> - Status & Manage - Network Elements - Server - HA - Database - KPIs - Processes </pre> Select the first SDS NOAM server. Select the Restart button. Stop Restart Reboot NTP Sync Report Answer OK to the confirmation popup. Are you sure you wish to restart application software on the following server(s)? ZombieSDSNOAM1 OK Cancel Wait for restart to complete.						

Procedure 39. Configure the Second SDS NOAM Server

S T E P #	This procedure will provide the steps to configure the Second SDS NOAM server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	SDS NOAM GUI: Login If not already done, establish a GUI session on the first SDS NOAM server by using the XMI IP address of the first SDS NOAM server. Open the web browser and enter a URL of: <code>https://<SDS_NO1_XMI_IP_Address></code> Login to the SDS NOAM GUI as the <i>guiadmin</i> user:  Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.

Procedure 39. Configure the Second SDS NOAM Server

2 ☐	SDS NOAM GUI: Insert the 2nd SDS NOAM server	Navigate to Main Menu -> Configuration -> Servers.  Select the Insert button to insert the 2nd SDS NOAM server into servers table (the first or server). <table border="1" data-bbox="462 619 1036 913"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Hostname *</td> <td>ZombieSDSNOAM2</td> </tr> <tr> <td>Role *</td> <td>NETWORK OAM&P</td> </tr> <tr> <td>System ID</td> <td></td> </tr> <tr> <td>Hardware Profile</td> <td>SDS TVOE Guest</td> </tr> </tbody> </table> Fill in the fields as follows: Hostname: <Hostname> Role: NETWORK OAM&P System ID: <Site System ID> Hardware Profile: SDS TVOE Guest Network Element Name: [Choose NE from Drop Down Box] Location: <NOAM Server Location> The network interface fields will now become available with selection choices based on the chosen hardware profile and network element <table border="1" data-bbox="462 1333 1339 1459"> <tbody> <tr> <td>XMI (10.240.213.0/24)</td> <td>10.240.213.21</td> <td>xmi ☐ VLAN (4)</td> </tr> <tr> <td>IMI (169.254.1.0/24)</td> <td>169.254.1.21</td> <td>imi ☐ VLAN (3)</td> </tr> </tbody> </table> Fill in the server IP addresses for the XMI network. Select xmi for the interface. Leave the "VLAN" checkbox unchecked. Fill in the server IP addresses for the IMI network. Select imi for the interface. Leave the "VLAN" checkbox unchecked. Next, add the following NTP servers: <table border="1" data-bbox="483 1680 1360 1780"> <thead> <tr> <th>NTP Server</th> <th>Preferred?</th> </tr> </thead> <tbody> <tr> <td><2nd NOAM-TVOE-IP-Address></td> <td>Yes</td> </tr> </tbody> </table> Select the Ok button when you have completed entering all the server data.	Attribute	Value	Hostname *	ZombieSDSNOAM2	Role *	NETWORK OAM&P	System ID		Hardware Profile	SDS TVOE Guest	XMI (10.240.213.0/24)	10.240.213.21	xmi ☐ VLAN (4)	IMI (169.254.1.0/24)	169.254.1.21	imi ☐ VLAN (3)	NTP Server	Preferred?	<2nd NOAM-TVOE-IP-Address>	Yes
Attribute	Value																					
Hostname *	ZombieSDSNOAM2																					
Role *	NETWORK OAM&P																					
System ID																						
Hardware Profile	SDS TVOE Guest																					
XMI (10.240.213.0/24)	10.240.213.21	xmi ☐ VLAN (4)																				
IMI (169.254.1.0/24)	169.254.1.21	imi ☐ VLAN (3)																				
NTP Server	Preferred?																					
<2nd NOAM-TVOE-IP-Address>	Yes																					

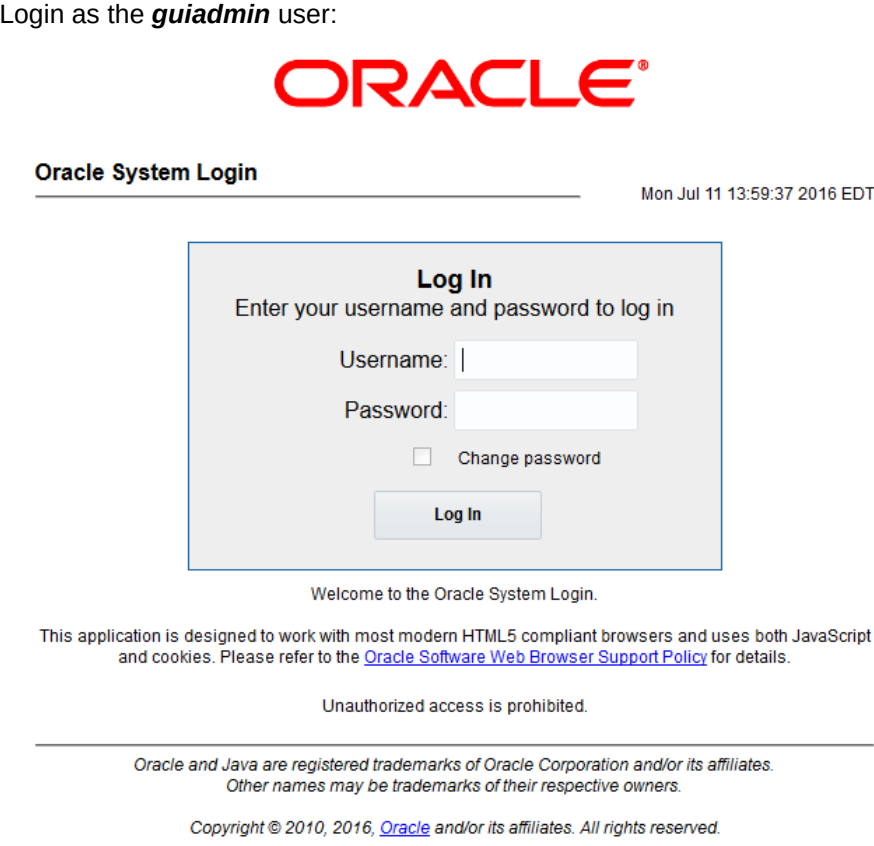
Procedure 39. Configure the Second SDS NOAM Server

3 ☐	SDS NOAM GUI: Export the Initial Configuration	Navigate to Main Menu -> Configuration -> Servers. From the GUI screen, select the SDS NOAM server and then select Export to generate the initial configuration data for that server. Insert Edit Delete Export Report
4 ☐	1st NOAM Server: Copy Configuration File to 2 nd NOAM Server	Obtain a terminal session to the 1st NOAM as the admusr user. Execute the following command to configure the 2nd NOAM server: <pre>\$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<NOAM2_Hostname>.sh admusr@<NOAM2_xmi_IP_address>:/var/tmp/TKLCConfigData.sh</pre>
5 ☐	2nd NOAM Server: Verify server configuration was called and Reboot the Server	Obtain a terminal window connection on the 2nd NOAM. Login as the admusr user. The automatic configuration daemon will look for the file named “TKLCConfigData.sh” in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server. Verify server configuration was called by checking the following file <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> Verify no errors are present and that the following message is displayed: <pre>[SUCCESS] script completed successfully!</pre> Note: The script may return success even when errors are reported in the log file. Go through the entire install.log file to verify no errors are present. Now Reboot the Server: <pre>\$ sudo init 6</pre> Wait for the server to reboot

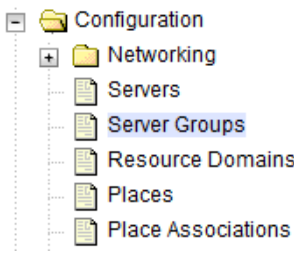
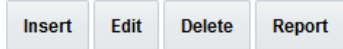
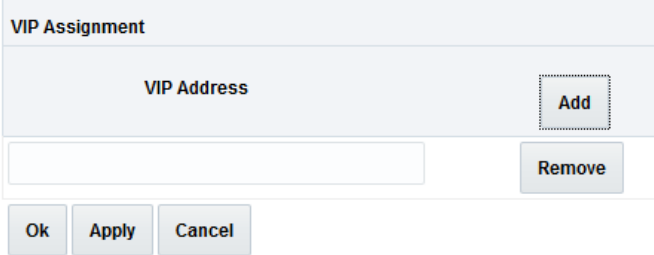
Procedure 39. Configure the Second SDS NOAM Server

6 ☐	2nd SDS NOAM Server: Verify Server Health	Execute the following command on the 2nd SDS NOAM server and make sure that no errors are returned: <pre>\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

Procedure 40. Complete SDS NOAM Server Group Configuration

S T E P #	This procedure will provide the steps to finish configuring the SDS NOAM server group. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	SDS NOAM GUI: Login	Establish a GUI session on the first SDS NOAM server by using the XMI IP address of the first SDS NOAM server. Open the web browser and enter a URL of: <code>https://<SDS_NO1_XMI_IP_Address></code> Login as the <i>guiadmin</i> user:  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.

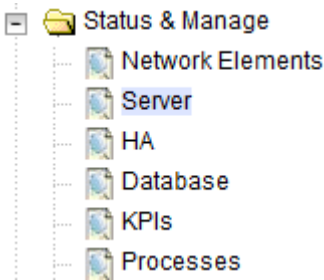
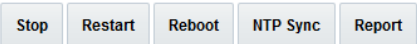
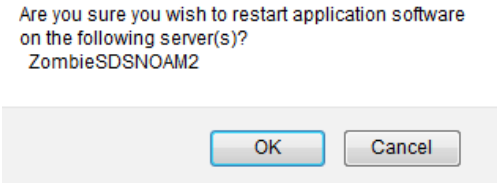
Procedure 40. Complete SDS NOAM Server Group Configuration

2 ☐	SDS NOAM GUI: Edit the SDS NOAM Server Group Data	Navigate to Main Menu->Configuration->Server Groups.  Select the SDS NOAM Server group and click on Edit  Add the 2nd SDS NOAM server to the Server Group by clicking the <i>Include in SG</i> checkbox for the 2nd SDS NOAM server. <table border="1" data-bbox="462 798 1242 997"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>ZombieSDSNOAM1</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> <tr> <td>ZombieSDSNOAM2</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> </tbody> </table> Click Apply. Add a SDS NOAM VIP by click on Add. Fill in the VIP Address and press Ok as shown below 	Server	SG Inclusion	Preferred HA Role	ZombieSDSNOAM1	☒ Include in SG	☐ Prefer server as spare	ZombieSDSNOAM2	☒ Include in SG	☐ Prefer server as spare
Server	SG Inclusion	Preferred HA Role									
ZombieSDSNOAM1	☒ Include in SG	☐ Prefer server as spare									
ZombieSDSNOAM2	☒ Include in SG	☐ Prefer server as spare									

Procedure 40. Complete SDS NOAM Server Group Configuration

3 ☐	SDS NOAM VIP: Establish GUI Session	Establish a GUI session on the SDS NOAM by using the XMI VIP address: <code>https://<SDS_NOAM_VIP_IP_Address></code> Login as user guiadmin. 
4 ☐	SDS NOAM VIP: Wait for Remote Database Alarm to Clear	Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding. Navigate to Main menu->Alarms & Events->View Active

Procedure 40. Complete SDS NOAM Server Group Configuration

5 ☐	SDS NOAM GUI: Restart 2 nd SDS NOAM Server	From the NOAM GUI, select the Main menu -> Status & Manage -> Server menu.  Select the 2nd SDS NOAM server. Select the Restart button.  Answer OK to the confirmation popup. 

4.15.2 SDS Configuration: NetBackup Client Installation (Optional)

Procedure 41. Install NetBackup Client (Optional)

S T E P #	This procedure will download and install NetBackup Client software on the server. Location of the bpstart_notify and bpend_notify scripts is required for the execution of this procedure. For Appworks based applications the scripts are located as follows: - /usr/TKLC/appworks/sbin/bpstart_notify - /usr/TKLC/appworks/sbin/bpend_notify Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Install NetBackup Client Software	If a customer has a way of transferring and installing the NetBackup client without the aid of TPD tools (push configuration) then use Appendix I.2: NETBACKUP CLIENT INSTALL/UPGRADE WITH NBAUTOINSTALL Note: This is not common. If the answer to the previous question is not known then use Appendix I.1: NetBackup Client Install using PLATCFG
2 ☐	Install NetBackup Client Software	Choose the same method used in step 1 to install NetBackup on the 2nd SDS NOAM.

4.15.3 SDS Configuration: Disaster Recovery SDS NOAM (Optional)

Procedure 42. SDS NOAM Configuration for DR Site (Optional)

S T E P #	This procedure will provide the steps to configure the First SDS DR NOAM server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PRIMARY SDS NOAM VIP GUI: Login Establish a GUI session on the SDS NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of: <code>https://<SDS_NOAM_XMI_VIP_IP_Address></code> Login as the <i>guiadmin</i> user: 

Procedure 42. SDS NOAM Configuration for DR Site (Optional)

2

☐

**PRIMARY
SDS NOAM
VIP GUI:**

Insert the SDS
DR NOAM
Network
Element

Navigate to **Main Menu->Networking -> Networks**

Select the **Browse** button, and enter the pathname of the DR-NOAM network XML file:

To create a new Network Element, upload a valid configuration file:

SDDSRNOAMzombie.xml

Select the **Upload File** button to upload the XML file and configure the NOAM Network Element.

Once the data has been uploaded, you should see a tab appear with the name of your network element. Click on this tab and you will get a window which describes the individual networks that are now configured:

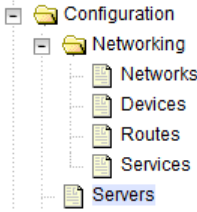
Global

ZombieSDSNOAM

ZombieSDSDRNOAM

Network Name	Network Type
XMI	OAM
IMI	OAM

Procedure 42. SDS NOAM Configuration for DR Site (Optional)

3 ☐	PRIMARY SDS NOAM VIP GUI: Insert the 1st SDS DR-NOAM server	Navigate to Main Menu -> Configuration -> Servers.  Select the Insert button to insert the new SDS DR-NOAM server into servers table. Adding a new server <table border="1"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Hostname *</td> <td>ZombieSDSDRNOAM1</td> </tr> <tr> <td>Role *</td> <td>NETWORK OAM&P</td> </tr> <tr> <td>System ID</td> <td></td> </tr> <tr> <td>Hardware Profile</td> <td>SDS TVOE Guest</td> </tr> <tr> <td>Network Element Name *</td> <td>ZombieSDSDRNOAM</td> </tr> </tbody> </table> Fill in the fields as follows: Hostname: <Hostname> Role: NETWORK OAM&P System ID: <Site System ID> Hardware Profile: SDS TVOE Guest Network Element Name: [Choose NE from Drop Down Box] The network interface fields will now become available with selection choices based on the chosen hardware profile and network element <table border="1"> <tbody> <tr> <td>XMI (10.240.213.0/24)</td> <td>10.240.213.23</td> <td>xmi ☐ VLAN (4)</td> </tr> <tr> <td>IMI (169.254.1.0/24)</td> <td>169.254.1.23</td> <td>imi ☐ VLAN (3)</td> </tr> </tbody> </table> Fill in the server IP addresses for the XMI network. Select xmi for the interface. Leave the "VLAN" checkbox unchecked. Fill in the server IP addresses for the IMI network. Select imi for the interface. Leave the "VLAN" checkbox unchecked. Next, add the following NTP servers: <table border="1"> <thead> <tr> <th>NTP Server</th> <th>Preferred?</th> </tr> </thead> <tbody> <tr> <td><1st SDS-DR-NOAM-RMS-TVOE-IP-Address></td> <td>Yes</td> </tr> </tbody> </table> Select the Ok button when you have completed entering all the server data.	Attribute	Value	Hostname *	ZombieSDSDRNOAM1	Role *	NETWORK OAM&P	System ID		Hardware Profile	SDS TVOE Guest	Network Element Name *	ZombieSDSDRNOAM	XMI (10.240.213.0/24)	10.240.213.23	xmi ☐ VLAN (4)	IMI (169.254.1.0/24)	169.254.1.23	imi ☐ VLAN (3)	NTP Server	Preferred?	<1st SDS-DR-NOAM-RMS-TVOE-IP-Address>	Yes
Attribute	Value																							
Hostname *	ZombieSDSDRNOAM1																							
Role *	NETWORK OAM&P																							
System ID																								
Hardware Profile	SDS TVOE Guest																							
Network Element Name *	ZombieSDSDRNOAM																							
XMI (10.240.213.0/24)	10.240.213.23	xmi ☐ VLAN (4)																						
IMI (169.254.1.0/24)	169.254.1.23	imi ☐ VLAN (3)																						
NTP Server	Preferred?																							
<1st SDS-DR-NOAM-RMS-TVOE-IP-Address>	Yes																							

Procedure 42. SDS NOAM Configuration for DR Site (Optional)

4 ☐	PRIMARY SDS NOAM VIP GUI: Export the Initial Configuration	Navigate to Main Menu -> Configuration -> Servers. From the GUI screen, select the SDS DR-NOAM server and then select Export to generate the initial configuration data for that server. Insert Edit Delete Export Report
5 ☐	PRIMARY SDS NOAM Server: Copy Configuration File to DR NOAM Server	Obtain a terminal session to the primary NOAM VIP as the admusr user. Execute the following command to configure the 1st DR NOAM server: <pre>\$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<DRNOAM1_Hostname>.sh admusr@<DRNOAM1_xmi_IP_address>:/var/tmp/TKLCConfigData.sh</pre>
6 ☐	1st SDS DR-NOAM Server: Verify server configuration was called and Reboot the Server	The automatic configuration daemon will look for the file named "TKLCConfigData.sh" in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server. Verify server configuration was called by checking the following file <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> Verify no errors are present and that the following message is displayed: <pre>[SUCCESS] script completed successfully!</pre> Note: The script may return success even when errors are reported in the log file. Go through the entire install.log file to verify no errors are present. Now Reboot the Server: <pre>\$ sudo init 6</pre> Wait for the server to reboot
7 ☐	1st SDS DR-NOAM Server: Verify Server Health	Execute the following command on the 1st SDS DR-NOAM server and make sure that no errors are returned: <pre>\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

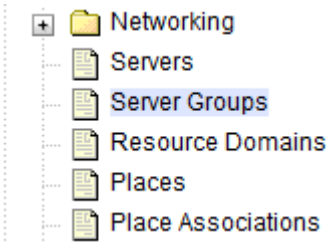
Procedure 42. SDS NOAM Configuration for DR Site (Optional)

8	Repeat for 2 nd SDS DR NOAM Server	Repeat Steps 3-7 to configure 2 nd SDS DR-NOAM Server. When inserting the 2 nd SDS DR-NOAM server, change the NTP server address to the following:				
☐		<table><tr><th>NTP Server</th><th>Preferred?</th></tr><tr><td><2nd SDS DR-NOAM-RMS-TVOE-IP-Address></td><td>Yes</td></tr></table>	NTP Server	Preferred?	<2nd SDS DR-NOAM-RMS-TVOE-IP-Address>	Yes
NTP Server		Preferred?				
<2nd SDS DR-NOAM-RMS-TVOE-IP-Address>	Yes					

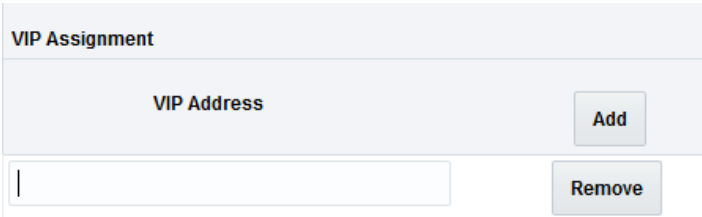
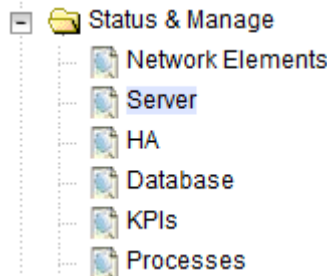
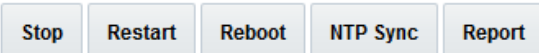
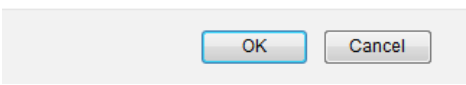
Procedure 43. Pairing for SDS DR-NOAM Site (Optional)

S T E P #	This procedure will provide the steps to pair the SDS DR-NOAM site. Prerequisite: Installation for SDS DR-NOAM Site complete Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	Primary SDS NOAM VIP GUI: Login Establish a GUI session on the primary SDS NOAM server by using the VIP IP address of the primary SDS NOAM server. Open the web browser and enter a URL of: https://<Primary_SDS_NOAM_VIP_IP_Address> Login as the <i>guiadmin</i> user:  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 43. Pairing for SDS DR-NOAM Site (Optional)

2 ☐	Primary SDS NOAM VIP GUI: Enter SDS DR-NOAM Server Group Data	Navigate to Main Menu -> Configuration -> Server Groups  Select Insert and fill the following fields: Insert Edit Delete Report • Server Group Name: <Enter Server Group Name> • Level: A • Parent : None • Function: SDS • WAN Replication Connection Count: Use Default Value Select OK when all fields are filled in.									
3 ☐	Primary SDS NOAM VIP GUI: Update Server Group	Select the Server Group that was created in the previous step, and click on Edit. Insert Edit Delete Report The user will be presented with the Server Groups [Edit] screen Check the checkbox labeled Include in SG for both SDS DR-NOAM Servers as shown below : <table border="1" data-bbox="462 1249 1226 1449"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>ZombieSDSDRNOAM1</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> <tr> <td>ZombieSDSDRNOAM2</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> </tbody> </table> Click on Apply	Server	SG Inclusion	Preferred HA Role	ZombieSDSDRNOAM1	☒ Include in SG	☐ Prefer server as spare	ZombieSDSDRNOAM2	☒ Include in SG	☐ Prefer server as spare
Server	SG Inclusion	Preferred HA Role									
ZombieSDSDRNOAM1	☒ Include in SG	☐ Prefer server as spare									
ZombieSDSDRNOAM2	☒ Include in SG	☐ Prefer server as spare									

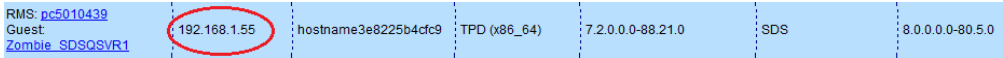
Procedure 43. Pairing for SDS DR-NOAM Site (Optional)

4 ☐	Primary SDS NOAM VIP GUI: Add SDS DR- NOAM VIP	Click the Add dialogue button for the VIP Address and enter an IP Address for the VIP as shown below  Then click the OK dialogue button. Verify that the banner information message states Data committed. 
5 ☐	Primary SDS NOAM VIP GUI: Wait for Remote Database Alarm to Clear	Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding. Navigate to Main menu->Alarms & Events->View Active
6 ☐	Primary SDS NOAM VIP GUI: Restart 1 st SDS DR-NOAM Server	From the SDS NOAM GUI, select the Main menu -> Status & Manage -> Server menu.  Select the 1st SDS DR-NOAM server. Select the Restart button.  Answer OK to the confirmation popup. 
7 ☐	Primary SDS NOAM VIP GUI : Restart the application on the 2 nd DR-NOAM Server	Repeat Step 6, this time select the 2nd SDS DR-NOAM Server.

4.15.4 SDS Configuration: Query Servers

The user should be aware that during the Query Server installation procedure, various errors may be seen at different stages of the procedure. During the execution of a step, the user is directed to ignore errors related to values other than the ones referenced by that step.

Procedure 44. Configuring SDS Query Servers

S T E P #	This procedure will provide the steps to configure SDS query servers Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Exchange SSH keys between SOAM site's local PMAC and the Query Server	Use the PMAC GUI to determine the Control Network IP address of the server that is to be the query server. From the PMAC GUI, navigate to Main Menu -> Software -> Software Inventory.  Note the IP address for the Query Server server. Login to the PMAC terminal as the admusr. From a terminal window connection on the PMAC as the admusr user, exchange SSH keys for admusr between the PMAC and the query server using the keyexchange utility, using the Control network IP address for the query server. When prompted for the password, enter the password for the admusr user of the NOAM server. <pre>\$ keyexchange admusr@<Query_Server_Control_IP Address></pre>

Procedure 44. Configuring SDS Query Servers

2 ☐	Primary SDS NOAM VIP GUI: Login	Establish a GUI session on the primary SDS NOAM server by using the VIP IP address of the primary SDS NOAM server. Open the web browser and enter a URL of: <code>https://<Primary_SDS_NOAM_VIP_IP_Address></code> Login as the <i>guiadmin</i> user:  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. <i>Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</i> <i>Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.</i>

Procedure 44. Configuring SDS Query Servers

3

Primary SDS NOAM VIP GUI: Insert the first Query Server

Navigate to Main Menu -> Configuration -> Servers.

Select the Insert button to insert the new SDS Query server into servers table (the first or server).

Adding a new server

Role *

QUERY SERVER

System ID

Hardware Profile

SDS TVOE Guest

Network Element Name *

ZombieSDSNOAM

Fill in the fields as follows:

Hostname: <Hostname>

Role: Query Server

System ID: <Site System ID>

Hardware Profile: SDS TVOE Guest

Network Element Name: [Choose NE from Drop Down Box]

The network interface fields will now become available with selection choices based on the chosen hardware profile and network element

XMI (10.240.213.0/24)

10.240.213.29

xmi

☐ VLAN (4)

IMI (169.254.1.0/24)

169.254.1.29

imi

☐ VLAN (3)

Fill in the server IP addresses for the XMI network. Select xmi for the interface. Leave the "VLAN" checkbox unchecked.

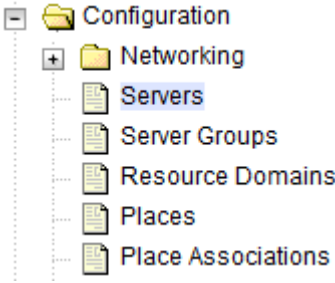
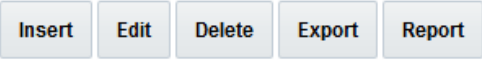
Fill in the server IP addresses for the IMI network. Select imi for the interface. Leave the "VLAN" checkbox unchecked.

Next, add the following NTP servers:

NTP Server	Preferred?
<Query-Server-TVOE-IP-Address>	Yes

Select the Ok button when you have completed entering all the server data.

Procedure 44. Configuring SDS Query Servers

4 ☐	SDS NOAM VIP: Export the Initial Configuration	Navigate to Main Menu -> Configuration -> Servers.  From the GUI screen, select the query server and then select Export to generate the initial configuration data for that server. 
5 ☐	SDS NOAM VIP: Copy Configuration File to Query Server	Obtain a terminal session to the SDS NOAM VIP as the admusr user. Use the awpushcfg utility to copy the configuration file created in the previous step from the <code>/var/TKLC/db/filemgmt</code> directory on the SDS NOAM to the query server, using the Control network IP address for the query server. The configuration file will have a filename like “TKLCConfigData.<<i>hostname</i>>.sh”. <pre>\$ sudo awpushcfg</pre> The awpushcfg utility is interactive, so the user will be 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 query server). • Hostname of the target server: Enter the server name configured in step 3

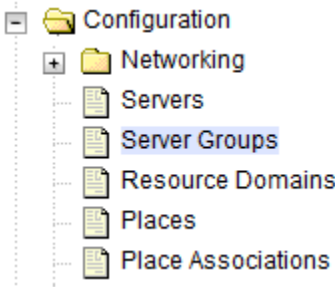
Procedure 44. Configuring SDS Query Servers

6 ☐	Query Server: Verify awpushcfg was called and Reboot the Server	Obtain a terminal window connection on the query server console by establishing an ssh session from the SDS NOAM VIP terminal console. <pre>\$ ssh admusr@<query_Server_Control_IP></pre> Login as the admusr user. The automatic configuration daemon will look for the file named “TKLCConfigData.sh” in the /var/tmp directory, implement the configuration in the file, and then prompt 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 no errors are present and that the following message is displayed: <pre>[SUCCESS] script completed successfully!</pre> Note: The script may return success even when errors are reported in the log file. Go through the entire install.log file to verify no errors are present. Now Reboot the Server: <pre>\$ sudo init 6</pre> Wait for the server to reboot
7 ☐	Query Server: Verify Server Health	Execute the following command on the query server and make sure that no errors are returned: <pre>\$ sudo syscheck</pre> <pre>Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

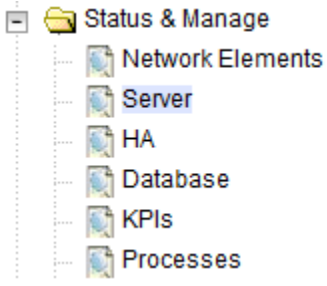
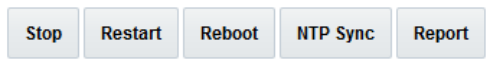
Procedure 45. Query Server SDS NOAM Pairing

S T E P #	This procedure will provide the steps to pair the SDS query server with the SDS NOAMs Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	SDS NOAM VIP GUI: Login	Establish a GUI session on the primary SDS NOAM server by using the VIP IP address of the primary SDS NOAM server. Open the web browser and enter a URL of: <code>https://<Primary_SDS_NOAM_VIP_IP_Address></code> Login as the <i>guiadmin</i> user:  The screenshot shows the Oracle System Login page. At the top is the Oracle logo. Below it, the text 'Oracle System Login' is on the left and 'Mon Jul 11 13:59:37 2016 EDT' is on the right. A central box contains a 'Log In' form with fields for 'Username:' and 'Password:', a 'Change password' checkbox, and a 'Log In' button. Below the form, it says 'Welcome to the Oracle System Login.' and '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.' At the bottom, it states 'Unauthorized access is prohibited.' and includes copyright information for Oracle and Java.

Procedure 45. Query Server SDS NOAM Pairing

2 ☐	SDS NOAM VIP GUI: Edit the SDS NOAM Server Group Data	Navigate to Main Menu->Configuration->Server Groups.  Select the SDS NOAM Server group and click on Edit Insert Edit Delete Report Add the query server to the Server Group by clicking the <i>Include in SG</i> checkbox for the query server. <table border="1" data-bbox="435 840 1430 1218"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>ZombieSDSNOAM1</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> <tr> <td>ZombieSDSNOAM2</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> <tr> <td>ZombieQS1</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> </tbody> </table> Click OK.	Server	SG Inclusion	Preferred HA Role	ZombieSDSNOAM1	☒ Include in SG	☐ Prefer server as spare	ZombieSDSNOAM2	☒ Include in SG	☐ Prefer server as spare	ZombieQS1	☒ Include in SG	☐ Prefer server as spare
Server	SG Inclusion	Preferred HA Role												
ZombieSDSNOAM1	☒ Include in SG	☐ Prefer server as spare												
ZombieSDSNOAM2	☒ Include in SG	☐ Prefer server as spare												
ZombieQS1	☒ Include in SG	☐ Prefer server as spare												
3 ☐	SDS NOAM VIP GUI: Wait for Remote Database Alarm to Clear	Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding. Navigate to Main menu->Alarms & Events->View Active												

Procedure 45. Query Server SDS NOAM Pairing

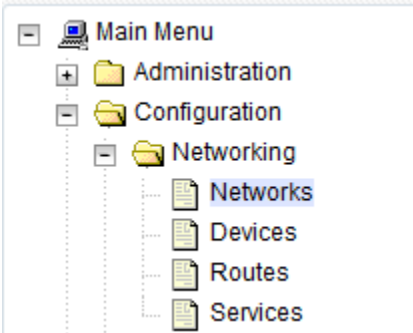
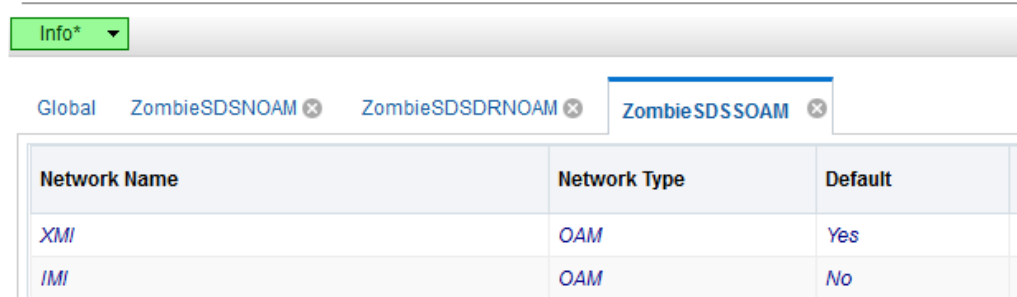
4 ☐	SDS NOAM VIP GUI: Restart query server	Navigate to Main menu->Status & Manage->Server.  Select the query server. Select the Restart button.  Answer OK to the confirmation popup. Wait for restart to complete.
5 ☐	Repeat for SDS DR-NOAM	If SDS DR-NOAMs have been configured, repeat this procedure at the site of the SDS DR-NOAMs

4.15.5 SDS Configuration: SOAMs

Procedure 46. Configure the SDS DP SOAM NE

S T E P #	This procedure will provide the steps to configure the SOAM Network Element Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	NOAM SDS VIP GUI: Login Establish a GUI session on the SDS NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: https://<Primary_SDS_NOAM_VIP_IP_Address> Login as the <i>guiadmin</i> user:  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 46. Configure the SDS DP SOAM NE

2 ☐	NOAM SDS VIP GUI: Create the SOAM Network Element using an XML File	Navigate to Main Menu->Networking -> Networks  Select the Browse button, and enter the pathname of the NOAM network XML file: To create a new Network Element, upload a valid configuration file: Browse... SDSOAMzombie.xml Upload File Select the Upload File button to upload the XML file and configure the NOAM Network Element. Once the data has been uploaded, you should see a tab appear with the name of your network element. Click on this tab and you will get a window which describes the individual networks that are now configured: Main Menu: Configuration -> Networking -> Networks  <table border="1"> <thead> <tr> <th>Network Name</th> <th>Network Type</th> <th>Default</th> </tr> </thead> <tbody> <tr> <td>XMI</td> <td>OAM</td> <td>Yes</td> </tr> <tr> <td>IMI</td> <td>OAM</td> <td>No</td> </tr> </tbody> </table>	Network Name	Network Type	Default	XMI	OAM	Yes	IMI	OAM	No
Network Name	Network Type	Default									
XMI	OAM	Yes									
IMI	OAM	No									

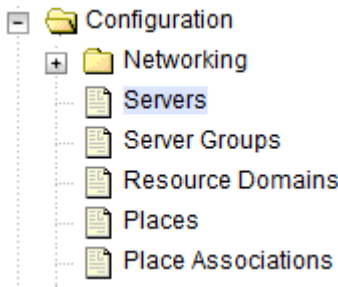
Procedure 47. Configure the SDS DP SOAM Servers

S T E P #	This procedure will provide the steps to configure the SDS DP SOAM servers. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Exchange SSH keys between SDS DP SOAM site's local PMAC and the SOAM Server	Use the PMAC GUI to determine the Control Network IP address of the server that is to be the SDS DP SOAM server. From the PMAC GUI, navigate to Main Menu -> Software -> Software Inventory.  Note the IP address for the SDS DP SOAM server. Login to the PMAC terminal as the admusr. From a terminal window connection on the PMAC as the admusr user, exchange SSH keys for admusr between the PMAC and the SDS DP SOAM server using the keyexchange utility, using the Control network IP address for the SDS DP SOAM server. When prompted for the password, enter the password for the admusr user of the SDS DP SOAM server. <pre>\$ keyexchange admusr@<SO1_Control_IP_Address></pre>
2 ☐	Exchange SSH keys between SDS NOAM and PMAC at the SDS DP SOAM site (If necessary)	Note: If this SDS DP SOAM shares the same PMAC as the SDS NOAM, then you can skip this step. From a terminal window connection on the SDS NOAM VIP, as the admusr, exchange SSH keys for admusr between the SDS NOAM and the PMAC for this SDS DP SOAM site using the keyexchange utility. When prompted for the password, enter the admusr password for the PMAC server. <pre>\$ keyexchange admusr@<SO1_Site_PMAC_Mgmt_IP_Address></pre> Repeat this step for the standby SDS DP SOAM Server

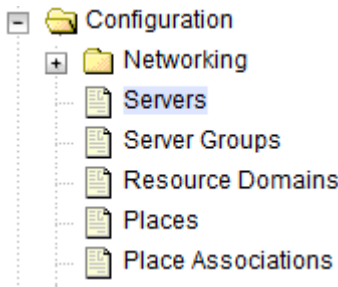
Procedure 47. Configure the SDS DP SOAM Servers

3 ☐	NOAM SDS VIP GUI: Login	If not already done, establish a GUI session on the SDS NOAM server by using the XMI VIP address. Open the web browser and enter a URL of: <code>https://<Primary_SDS_NOAM_VIP_IP_Address></code> Login to the SDS NOAM GUI as the <i>guiadmin</i> user: 

Procedure 47. Configure the SDS DP SOAM Servers

4	SDS NOAM VIP GUI: Insert the 1 st SDS DP SOAM server	Navigate to Main Menu -> Configuration -> Servers.  Select the Insert button to insert the 1st SDS DP SOAM server into servers table (the first or server). <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Attribute</th> <th style="width: 70%;">Value</th> </tr> </thead> <tbody> <tr> <td>Hostname *</td> <td>ZombieSDSSOAM1</td> </tr> <tr> <td>Role *</td> <td>SYSTEM OAM</td> </tr> <tr> <td>System ID</td> <td></td> </tr> <tr> <td>Hardware Profile</td> <td>SDS TVOE Guest</td> </tr> <tr> <td>Network Element Name *</td> <td>ZombieSDSSOAM</td> </tr> </tbody> </table> Fill in the fields as follows: Hostname: <Hostname> Role: SYSTEM OAM System ID: <Site System ID> Hardware Profile: SDS TVOE Guest Network Element Name: [Choose NE from Drop Down Box] Location: <NOAM Server Location> The network interface fields will now become available with selection choices based on the chosen hardware profile and network element <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="width: 30%;">XMI (10.240.213.0/24)</td> <td style="width: 35%;">10.240.213.26</td> <td style="width: 15%;">xmi</td> <td style="width: 20%;">☐ VLAN (4)</td> </tr> <tr> <td>IMI (169.254.1.0/24)</td> <td>169.254.1.26</td> <td>imi</td> <td>☐ VLAN (3)</td> </tr> </tbody> </table> Fill in the server IP addresses for the XMI network. Select xmi for the interface. Leave the "VLAN" checkbox unchecked. Fill in the server IP addresses for the IMI network. Select imi for the interface. Leave the "VLAN" checkbox unchecked. Next, add the following NTP servers: <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 60%;">NTP Server</th> <th style="width: 40%;">Preferred?</th> </tr> </thead> <tbody> <tr> <td><1st SDS-SOAM-RMS-TVOE-IP-Address></td> <td style="text-align: center;">Yes</td> </tr> </tbody> </table> Select the Ok button when you have completed entering all the server data.	Attribute	Value	Hostname *	ZombieSDSSOAM1	Role *	SYSTEM OAM	System ID		Hardware Profile	SDS TVOE Guest	Network Element Name *	ZombieSDSSOAM	XMI (10.240.213.0/24)	10.240.213.26	xmi	☐ VLAN (4)	IMI (169.254.1.0/24)	169.254.1.26	imi	☐ VLAN (3)	NTP Server	Preferred?	<1st SDS-SOAM-RMS-TVOE-IP-Address>	Yes
Attribute	Value																									
Hostname *	ZombieSDSSOAM1																									
Role *	SYSTEM OAM																									
System ID																										
Hardware Profile	SDS TVOE Guest																									
Network Element Name *	ZombieSDSSOAM																									
XMI (10.240.213.0/24)	10.240.213.26	xmi	☐ VLAN (4)																							
IMI (169.254.1.0/24)	169.254.1.26	imi	☐ VLAN (3)																							
NTP Server	Preferred?																									
<1st SDS-SOAM-RMS-TVOE-IP-Address>	Yes																									

Procedure 47. Configure the SDS DP SOAM Servers

5 ☐	SDS NOAM VIP GUI: Export the Initial Configuration	Navigate to Main Menu -> Configuration -> Servers.  From the GUI screen, select the SDS SOAM server and then select Export to generate the initial configuration data for that server. 
6 ☐	SDS NOAM VIP: Copy Configuration File to 1st SDS DP SOAM Server	Obtain a terminal session to the SDS NOAM VIP as the admusr user. Use the awpushcfg utility to copy the configuration file created in the previous step from the <code>/var/TKLC/db/filemgmt</code> directory on the SDS NOAM to the 1st SDS DP SOAM server, using the Control network IP address for the 1st SDS DP SOAM server. The configuration file will have a filename like “TKLCConfigData.<hostname>.sh”. <pre>\$ sudo awpushcfg</pre> The awpushcfg utility is interactive, so the user will be 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 1st SDS DP SOAM server). • Hostname of the target server: Enter the server name configured in step 4

Procedure 47. Configure the SDS DP SOAM Servers

7 ☐	1st SDS DP SOAM Server: Verify awpushcfg was called and Reboot the Server	Obtain a terminal window connection on the 1st SDS DP SOAM server console by establishing an ssh session from the site PMAC terminal console. <pre>\$ ssh admusr@<SDS_SO1_Control_IP></pre> Login as the <i>admusr</i> user. The automatic configuration daemon will look for the file named “TKLCConfigData.sh” in the /var/tmp directory, implement the configuration in the file, and then prompt 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 no errors are present and that the following message is displayed: <pre>[SUCCESS] script completed successfully!</pre> Note: The script may return success even when errors are reported in the log file. Go through the entire install.log file to verify no errors are present. Now Reboot the Server: <pre>\$ sudo init 6</pre> Wait for the server to reboot
8 ☐	1st SDS DP SOAM Server: Verify Server Health	Execute the following command on the 1st SDS DP SOAM server and make sure that no errors are returned: <pre>\$ sudo syscheck</pre> <pre>Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

Procedure 47. Configure the SDS DP SOAM Servers

9	☐ Insert and Configure the 2nd SDS DP SOAM server	Repeat this procedure to insert and configure the 2nd SDS DP SOAM server, with the exception of the NTP server, which should be configured as so: <table><tr><th>NTP Server</th><th>Preferred?</th></tr><tr><td><2nd SDS DP SOAM-RMS-TVOE-IP-Address></td><td>Yes</td></tr></table> Instead of data for the 1st SDS DP SOAM Server, insert the network data for the 2nd SDS DP SOAM server, transfer the <i>TKLCCConfigData</i> file to the 2nd SDS DP SOAM server, and reboot the 2nd SDS DP SOAM server when prompted at a terminal window.	NTP Server	Preferred?	<2nd SDS DP SOAM-RMS-TVOE-IP-Address>	Yes
NTP Server		Preferred?				
<2nd SDS DP SOAM-RMS-TVOE-IP-Address>	Yes					

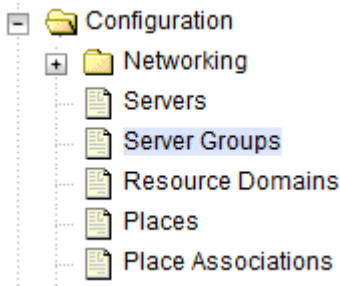
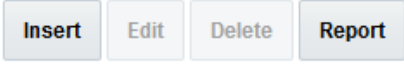
Procedure 48. Configure the SDS DP SOAM Server Group

S T E P #	This procedure will provide the steps to configure the SOAM Server Group Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

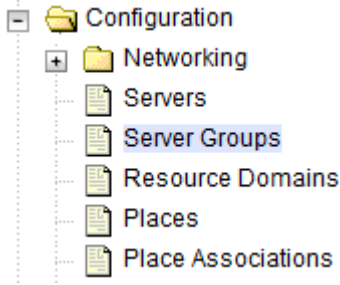
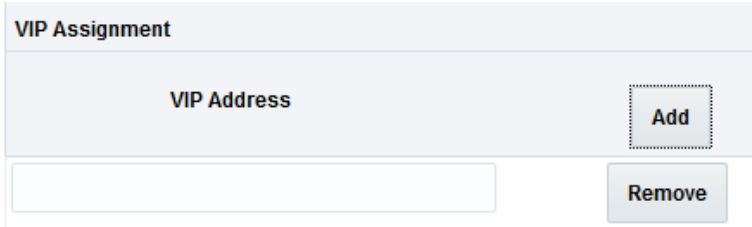
Procedure 48. Configure the SDS DP SOAM Server Group

1 ☐	NOAM SDS VIP GUI: Login	If not already done, establish a GUI session on the SDS NOAM server by using the XMI VIP address of the SDS NOAM server. Open the web browser and enter a URL of: https://<Primary_NOAM_VIP_IP_Address> Login to the SDS NOAM GUI as the <i>guiadmin</i> user: 

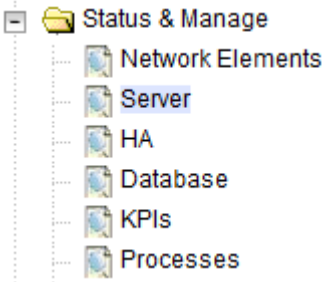
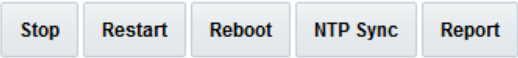
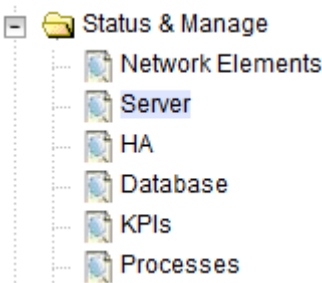
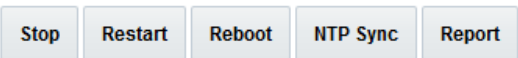
Procedure 48. Configure the SDS DP SOAM Server Group

2 ☐	SDS NOAM VIP GUI: Enter SOAM Server Group Data	After approximately 5 minutes for the 2nd SDS DP SOAM server to reboot, Navigate to the GUI Main Menu->Configuration->Server Groups  Select Insert  Add the SDS DP SOAM Server Group name along with the values for the following fields: • Name: <Hostname> • Level: B • Parent [Select the NOAM Server Group] • Function: SDS (Active/Standby Pair) • WAN Replication Connection Count: Use Default Value Select OK when all fields are filled.

Procedure 48. Configure the SDS DP SOAM Server Group

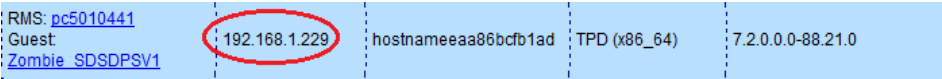
3 ☐	SDS NOAM VIP GUI: Edit the SDS DP SOAM Server Group and add VIP	From the GUI Main Menu->Configuration->Server Groups  Select the new SDS DP SOAM server group, and then select Edit. Insert Edit Delete Report Add both SDS DP SOAM servers to the Server Group Primary Site by clicking the Include in SG checkbox. Do not check any of the Preferred Spare checkboxes. <table border="1" data-bbox="457 905 1388 1100"> <tbody> <tr> <td>ZombieSDSSOAM1</td> <td>☒ Include in SG</td> <td>☐ Prefer server as spare</td> </tr> <tr> <td>ZombieSDSSOAM2</td> <td>☒ Include in SG</td> <td>☐ Prefer server as spare</td> </tr> </tbody> </table> Click Apply. Add a SDS DP SOAM VIP by click on Add. Fill in the VIP Address and press Ok as shown below: 	ZombieSDSSOAM1	☒ Include in SG	☐ Prefer server as spare	ZombieSDSSOAM2	☒ Include in SG	☐ Prefer server as spare
ZombieSDSSOAM1	☒ Include in SG	☐ Prefer server as spare						
ZombieSDSSOAM2	☒ Include in SG	☐ Prefer server as spare						
4 ☐	SDS NOAM VIP GUI: Wait for Remote Database Alarm to Clear	Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding. Navigate to Main menu->Alarms & Events->View Active						

Procedure 48. Configure the SDS DP SOAM Server Group

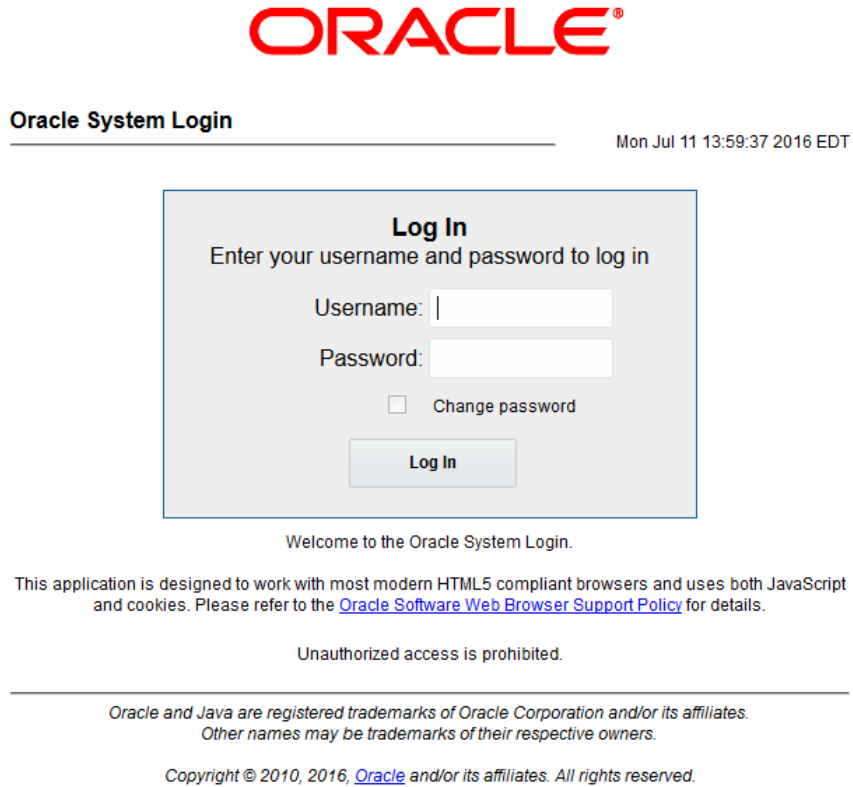
5 ☐	NOAM VIP GUI: Restart 1 st SDS DP SOAM server	From the SDS NOAMP GUI, select Main menu->Status & Manage->Server.  Select the 1st SDS DP SOAM server. Select the Restart button. Answer OK to the confirmation popup. Wait for restart to complete. 
6 ☐	SDS NOAM VIP GUI: Restart 2 nd SDS DP SOAM server	From the SDS NOAM GUI, select Main menu->Status & Manage->Server.  Select the 2nd SDS DP SOAM server. Select the Restart button. Answer OK to the confirmation popup. Wait for restart to complete. 

4.15.6 SDS Configuration: DPs

Procedure 49. Configure the SDS DP Servers

S T E P #	This procedure will provide the steps to configure SDS DP Servers Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PMAC: Exchange SSH keys between SDS DP site's local PMAC and the DP server Use the DP site's PMAC GUI to determine the Control Network IP address of the server that is to be a SDS DP server. From the MP site's PMAC GUI, navigate to Main Menu -> Software -> Software Inventory.  Note the IP address for a SDS DP server. Login to the SDS DP site's PMAC terminal as the admusr. From a terminal window connection on the SDS DP site's PMAC as the admusr. Exchange SSH keys for admusr between the PMAC and the SDS DP server using the keyexchange utility, using the Control network IP address for the SDS DP server. <pre>\$ keyexchange admusr@<MP_Control_IP Address></pre> When prompted for the password, enter the password for the admusr user of the SDS DP server.

Procedure 49. Configure the SDS DP Servers

2 ☐	SDS NOAM VIP GUI: Login	If not already done, establish a GUI session on the SDS NOAM server by using the XMI VIP address of the SDS NOAM server. Open the web browser and enter a URL of: <code>https://<Primary_SDS_NOAM_VIP_IP_Address></code> Login to the SDS NOAM GUI as the guiadmin user:  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 49. Configure the SDS DP Servers

3

SDS NOAM VIP GUI:

Insert the SDS DP server (Part 1)

Configuration

Networking

Servers

Server Groups

Resource Domains

Places

Place Associations

Select the **Insert** button to insert the new SDS DP server into servers table.

Insert

Edit

Delete

Export

Report

Fill out the following values:

Hostname:<Hostname>

Role: **MP**

Network Element: **[Choose Network Element]**

Hardware Profile: **SDS TVOE Guest**

Location: **<enter an optional location description>**

The interface configuration form will now appear.

XMI (10.240.213.0/24)

10.240.213.30

xmi

☐ VLAN (4)

IMI (169.254.1.0/24)

169.254.1.30

imi

☐ VLAN (3)

For the XMI network, enter the SDS DP's XMI IP address. Select the xmi interface. **Leave the "VLAN" checkbox unchecked.**

For the IMI network, enter the SDS DP's IMI IP address. Select the imi interface. **Leave the "VLAN" checkbox unchecked.**

4

NOAM VIP GUI:

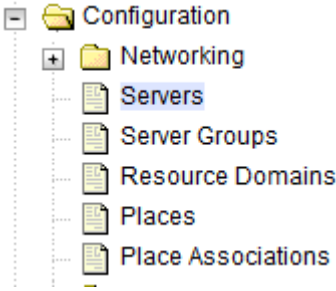
Insert the DP server (Part 2)

Next, add the following NTP servers:

NTP Server	Preferred?
<SDS-DP-RMS-TVOE-IP-Address>	Yes

Select **OK** when all fields are filled in to finish SDS DP server insertion.

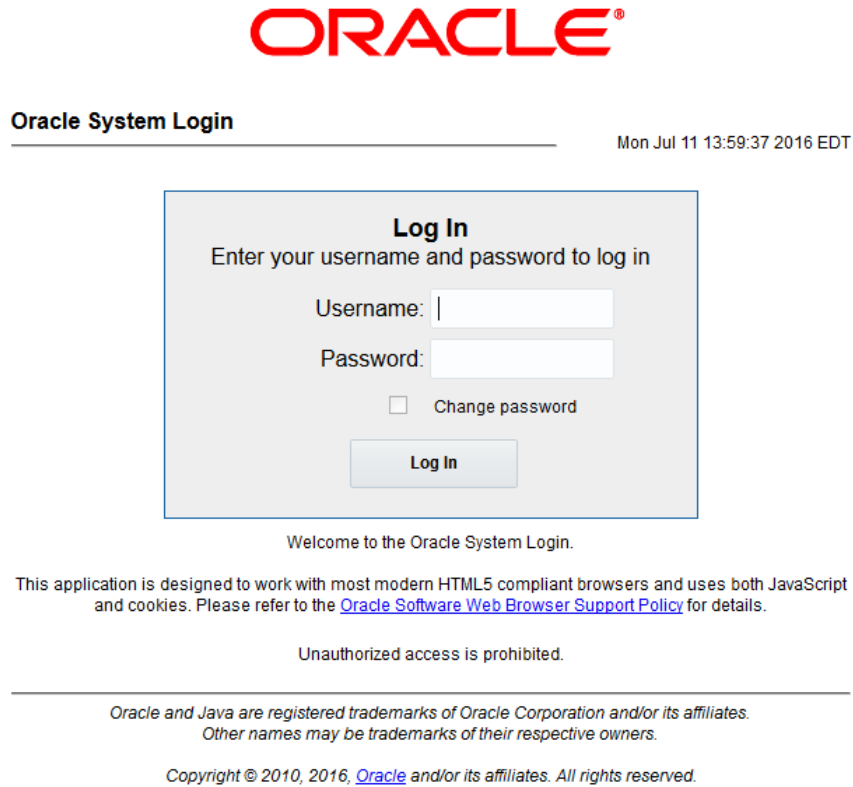
Procedure 49. Configure the SDS DP Servers

5 ☐	SDS NOAM VIP GUI: Export the Configuration	Navigate to Main Menu -> Configuration -> Servers.  From the GUI screen, select the SDS DP server and then select Export to generate the initial configuration data for that server. 
6 ☐	SDS NOAM VIP GUI: Copy Configuration File to SDS DP Server	Obtain a terminal session to the SDS NOAM VIP as the admusr user. Use the awpushcfg utility to copy the configuration file created in the previous step from the <code>/var/TKLC/db/filemgmt</code> directory on the SDS NOAM to the SDS DP server, using the Control network IP address for the MP server. The configuration file will have a filename like “TKLCCfgData.<hostname>.sh”. <pre>\$ sudo awpushcfg</pre> The awpushcfg utility is interactive, so the user will be 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 SDS DP server). • Hostname of the target server: Enter the server name configured in step 3

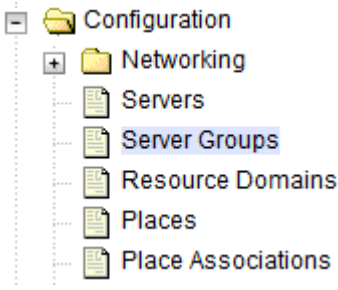
Procedure 49. Configure the SDS DP Servers

7 ☐	SDS DP Server: Verify awpushcfg was called and Reboot the Configured Server	Obtain a terminal window connection on the SDS DP server console by establishing an ssh session from the SDS NOAM VIP terminal console. <pre>\$ ssh admusr@<DP_Control_IP></pre> Login as the admusr user. Verify awpushcfg was called by checking the following file: <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> Verify no errors are present and that the following message is displayed: <pre>[SUCCESS] script completed successfully!</pre> Note: The script may return success even when errors are reported in the log file. Go through the entire install.log file to verify no errors are present. Reboot the sever: <pre>\$ sudo init 6</pre> Proceed to the next step once the Server finished rebooting, The server is done rebooting once the login prompt is displayed.
8 ☐	SDS DP Server: Verify Server Health	Execute the following command as super-user on the server and make sure that no errors are returned: <pre>\$ sudo syscheck</pre> <pre>Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>
9 ☐	Repeat for remaining SDS DPs	Repeat this entire procedure for all remaining SDS DP servers.

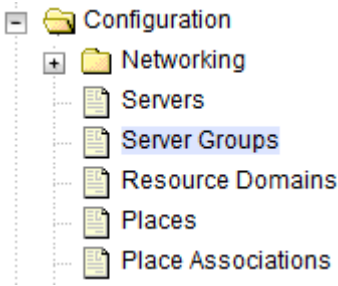
Procedure 50. Configure the SDS DP Server Group(s)

S T E P #	This procedure will provide the steps to configure MP Server Groups Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	SDs NOAM VIP GUI: Login	If not already done, establish a GUI session on the SDS NOAM server the VIP address. Open the web browser and enter a URL of: https://<Primary_NOAM_VIP_IP_Address> Login to the SDS NOAM GUI as the <i>guiadmin</i> user:  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.

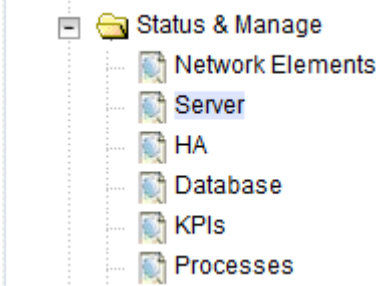
Procedure 50. Configure the SDS DP Server Group(s)

2 ☐	SDS NOAM VIP GUI: Enter SDS DP Server Group Data	Navigate to Main Menu ->Configuration ->Server Groups  Select Insert Insert Edit Delete Report Fill out the following fields: Server Group Name: <Server Group Name> Level: C Parent: [SDS DP SOAM Server Group That is Parent To this SDS DP] Function: SDS Select OK when all fields are filled in.
3 ☐	SDS NOAM VIP GUI: Repeat For Additional Server Groups	Repeat Step 2 for any remaining SDS DP server groups you wish to create.

Procedure 50. Configure the SDS DP Server Group(s)

4 ☐	SDS NOAM VIP GUI: Edit the SDS DP Server Groups to include SDS DPs	From the GUI, navigate to Main Menu->Configuration->Server Groups  Select a server group that you just created and then select Edit. Select the Network Element that represents the SDS DP server group you wish to edit. Click the Include in SG box for the SDS DP server that you wish to include in <i>this</i> server group. Leave other checkboxes blank. <table border="1" data-bbox="456 894 1317 1041"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>ZombieSDSDP1</td><td>☒ Include in SG</td><td>☐ Prefer server as spare</td></tr> </tbody> </table> Note: Each SDS DP server should be in its own server group. Select OK.	Server	SG Inclusion	Preferred HA Role	ZombieSDSDP1	☒ Include in SG	☐ Prefer server as spare
Server	SG Inclusion	Preferred HA Role						
ZombieSDSDP1	☒ Include in SG	☐ Prefer server as spare						
5 ☐	SDS NOAM VIP GUI: Repeat For Additional Server Groups	Repeat Step 4 for any remaining SDS DP server groups you need to edit.						
6 ☐	SDS NOAM VIP GUI: Wait for Remote Database Alarm to Clear	Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding. Navigate to Main menu->Alarms & Events->View Active						

Procedure 50. Configure the SDS DP Server Group(s)

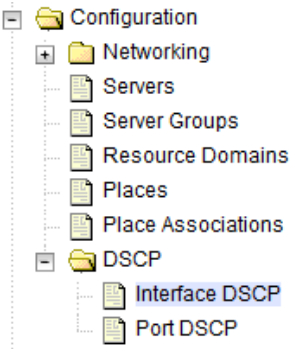
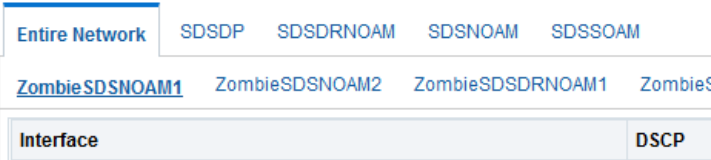
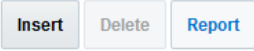
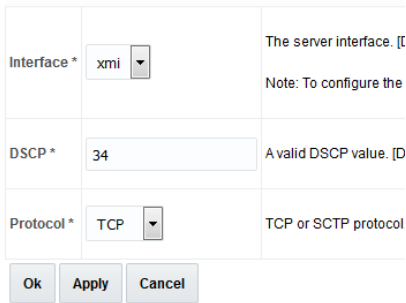
7 ☐	SDS NOAM VIP GUI: Restart SDS DP servers	Navigate to Main menu->Status & Manage->Server  For each SDS DP server: • Select the SDS DP server. • Select the Restart button. • Answer OK to the confirmation popup. Wait for the message which tells you that the restart was successful. Stop Restart Reboot NTP Sync Report

4.15.7 SDS Configuration: DSCP (Optional)

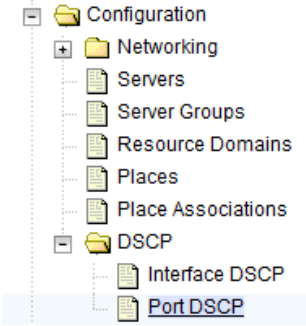
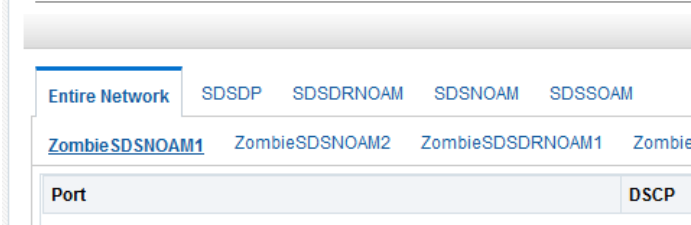
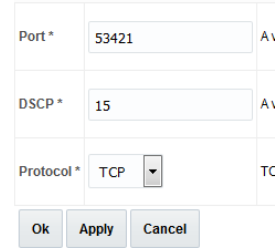
Procedure 51. Configure DSCP Values for Outgoing Traffic (Optional)

S T E P #	This procedure will provide the steps to configure the DSCP values for outgoing packets on servers. DSCP values can be applied to an outbound interface as a whole, or to all outbound traffic using a specific TCP or SCTP source port. This step is optional and should only be executed if has been decided that your network will utilize packet DSCP markings for Quality-of-Service purposes. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	NOAM VIP GUI: Login 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="https://<Primary_NOAM_VIP_IP_Address>">https://<Primary_NOAM_VIP_IP_Address> Login to the NOAM GUI as the <i>guiadmin</i> user:  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 51. Configure DSCP Values for Outgoing Traffic (Optional)

2 ☐	NOAM VIP GUI: Option 1: Configure Interface DSCP	Note: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary. Navigate to Main Menu -> Configuration -> DSCP -> Interface DSCP  Select the server you wish to configure from the list of servers on the 2nd line. (You can view all servers with Entire Network selected; or limit yourself to a particular server group by clicking on that server group name's tab).  Click Insert  Select the network interface from the drop down box, then enter the <i>DSCP value</i> you wish to have applied to packets leaving this interface. Insert DSCP by Interface on ZombieSDSNOA  Click OK if there are no more interfaces on this server to configure, or Apply to finish this interface and continue on with more interfaces by selecting them from the drop down and entering their <i>DSCP values</i>.

Procedure 51. Configure DSCP Values for Outgoing Traffic (Optional)

3 ☐	NOAM VIP GUI: Option 2: Configure Port DSCP	Note: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary. Navigate to Main Menu -> Configuration -> DSCP -> Port DSCP  Select the server you wish to configure from the list of servers on the 2nd line. (You can view all servers with Entire Network selected; or limit yourself to a particular server group by clicking on that server group name's tab). Main Menu: Configuration -> DSCP -> Port DSCP  Click Insert  Enter the source port, DSCP value, and select the transport protocol. Click OK if there are no more port DSCPs on this server to configure, or Apply to finish this port entry and continue entering more port <i>DSCP mappings</i>.

Procedure 51. Configure DSCP Values for Outgoing Traffic (Optional)

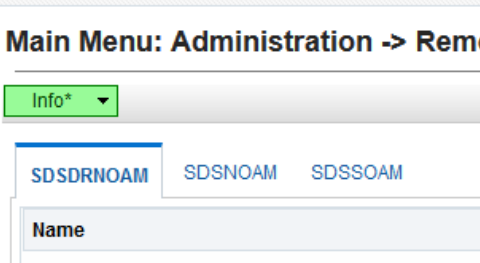
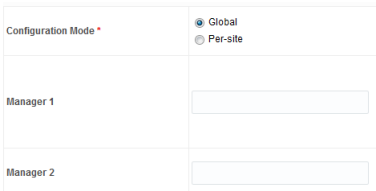
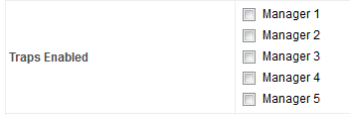
4 ☐	NOAM VIP GUI: Repeat for additional servers.	Repeat Steps 2-3 for all remaining servers.

4.15.8 SDS Configuration: SNMP (Optional)

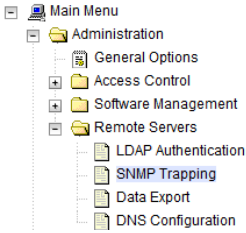
Procedure 52. Configure SNMP Trap Receiver(s) (Optional)

S T E P #	This procedure will provide the steps to configure forwarding of SNMP Traps from each individual server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	SDS NOAM VIP GUI: Login 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: https://< Primary_SDS_NOAM_VIP_IP_Address> Login to the NOAM GUI as the guiadmin user:  Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.

Procedure 52. Configure SNMP Trap Receiver(s) (Optional)

2 ☐	SDS NOAM VIP GUI: Configure System-Wide SNMP Trap Receiver(s)	Navigate to Main Menu -> Administration -> Remote Servers -> SNMP Trapping Select the Server Group tab for SNMP trap configuration:  Fill in the IP address or hostname of the Network Management Station (NMS) you wish to forward traps to. This IP should be reachable from the NOAMP's "XMI" network. Continue to fill in additional secondary, tertiary, etc. Manager IPs in the corresponding slots if desired. SNMP Trap Configuration Insert for ZombieNOAM  Check Traps Enabled boxes for the Manager servers being configured:  Enter the SNMP Community Name: SNMPv2c Read-Only Community Name SNMPv2c Read-Write Community Name Leave all other fields at their default values. Press OK

Procedure 52. Configure SNMP Trap Receiver(s) (Optional)

3 ☐	SDS NOAM VIP GUI: Enable Traps from Individual Servers (Optional)	Note: By default SNMP traps from DPs are aggregated and then displayed at the active NOAMP. If instead, you wish for every server to send its own traps directly to the NMS, then execute this procedure. This procedure requires that all servers, including DPs, have an XMI interface on which the customer SNMP Target server (NMS) is reachable. Navigate to Main Menu -> Administration -> Remote Servers -> SNMP Trapping  Make sure the checkbox next to Enabled is checked, if not, check it as shown below Traps from Individual Servers ☒ Enabled Then click on Apply and verify that the data is committed.

4.16 IDIH Installation and Configuration (Optional)

The following procedures outline the steps needed to install and configure IDIH.

Note: If IDIH already exists, and this is an IDIH re-installation; execute **Appendix O: IDIH External Drive Removal** before proceeding.

Note: Before proceeding, refer to **Section 4.10** for IDIH VM placement information.

4.16.1 IDIH Installation

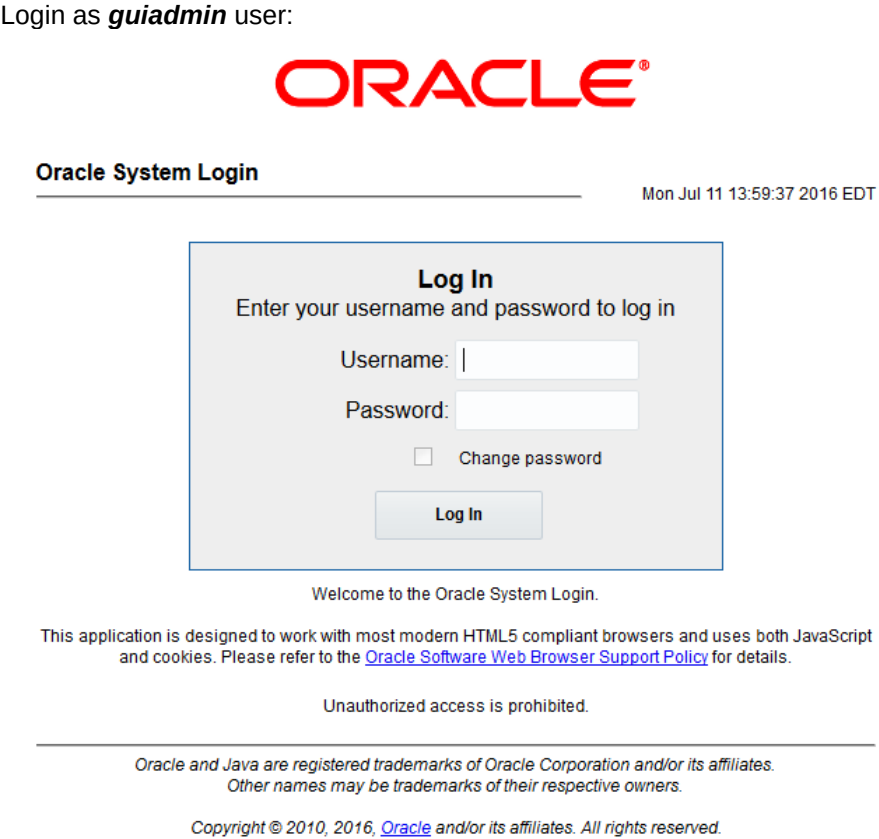
This procedure is part of DSR software installation. The installation procedure uses the “fast deployment” utility (fdconfig) bundled with the PMAC server to install and configure IDIH.

Note: [Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only]: Follow **Appendix Q.4: Non-HA Lab Node IDIH Procedure Deviation** instead of procedure 58 for IDIH installation.

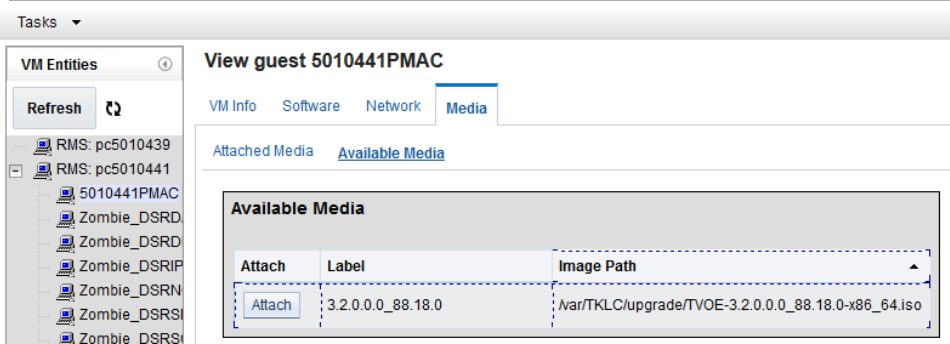
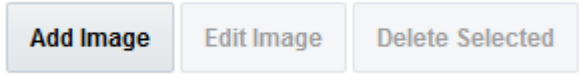
Procedure 53. IDIH Installation (Optional)

S T E P #	This procedure will provide the steps to install and configure IDIH. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	TVOE Host: Load Application ISO Note: If the IDIH ISO images have NOT yet been added to the PMAC, execute this steps 1-4 Add the Application ISO images (mediation, application, and oracleGuest) to the PMAC, this can be done in one of three ways: 1. Insert the CD containing the IDIH media into the removable media drive. 2. Attach the USB device containing the ISO to a USB port. 3. Copy the Application ISO file to the PMAC server into the /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as pmacftpusr user: cd into the directory where your ISO image is located on the TVOE Host (<i>not on the PMAC server</i>) Using sftp, connect to the PMAC server <pre>\$ sftp pmacftpusr@<pmac_management_network_ip> \$ put <image>.iso</pre> After the image transfer is 100% complete, close the connection: <pre>\$ quit</pre>

Procedure 53. IDIH Installation (Optional)

2 ☐	PMAC GUI: Login	Open web browser and enter: <code>https://<PMAC_Mgmt_Network_IP></code> Login as <i>guiadmin</i> user: 

Procedure 53. IDIH Installation (Optional)

3	PMAC GUI: Attach the software Image to the PMAC Guest	If in Step 1 the ISO image was transferred directly to the PMAC guest via sftp, skip the rest of this step and continue with step 4. If the image is on a CD or USB device, continue with this step. In the PMAC GUI, navigate to Main Menu -> VM Management. In the "VM Entities" list, select the PMAC guest. On the resulting "View VM Guest" page, select the Media tab. Under the Media tab, find the ISO image in the "Available Media" list, and click its Attach button. After a pause, the image will appear in the "Attached Media" list. Main Menu: VM Management 
4	PMAC GUI: Add Application Image	Navigate to Main Menu -> Software -> Manage Software Images Press Add Image button. Use the drop down to select the image.  If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://..."). These devices are assigned in numerical order as CD and USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the ISO image of interest is normally present on the second device, "device://dev/sr1". If one or more CD or USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number. If in Step 1 the image was transferred to PMAC via sftp it will appear in the list as a local file "/var/TKLC/...". Select the appropriate path and Press Add New Image button. You may check the progress using the Task Monitoring link. Observe the green bar indicating success. Once the green bar is displayed, remove the IDIH Media from the optical drive of the management server.
5	PMAC: Establish Terminal Session	Establish an SSH session to the PMAC. Login as admusr.

Procedure 53. IDIH Installation (Optional)

6 ☐	PMAC: Reset Create Guest Default Timeout and other timeout parameters	Reset the create guest default timeout. Execute the following commands: <pre>\$ sudo sqlite3 /usr/TKLC/plat/etc/TKLCfd-config/db/fdcRepo.fdcdb 'update params set value=3000 where name="DEFAULT_CREATE_GUEST_TIMEOUT"' ;</pre> <pre>\$ sudo pmacadm setParam --paramName=defaultTpdProvdtTimeout -paramValue=120</pre> <pre>\$ sudo pmacadm setParam --paramName=guestDiskDeployTimeout -paramValue=50</pre> To verify whether the above values are set correctly, run the below commands. <pre>\$ sudo sqlite3 /usr/TKLC/plat/etc/TKLCfd-config/db/fdcRepo.fdcdb 'select name, value from params where name like "%TIMEOUT%";</pre> <pre>\$ sudo pmacadm getParam --paramName=defaultTpdProvdtTimeout</pre> <pre>\$ sudo pmacadm getParam --paramName=guestDiskDeployTimeout</pre>
7 ☐	PMAC: Copy the fd-cfg template XML file to the guest-dropin Directory	Copy the vedsr_idih.xml.template XML file to the pmac guest-dropin directory. Execute the following command: <pre>\$ sudo cp /usr/TKLC/smac/html/TPD/mediation-8.1.0.0.0_x.x.x.x/vedsr_idih.xml.template /var/TKLC/smac/guest-dropin</pre> <pre>\$ cd /var/TKLC/smac/guest-dropin/</pre> <pre>\$ mv vedsr_idih.xml.template <idih_fdc_file_name>.xml</pre>
8 ☐	PMAC: Configure the fd-cfg.xml file	Configure the <idih_fdc_file_name>.xml file. See Appendix M: IDIH Fast Deployment Configuration for a breakdown of the parameters and a sample XML configuration file. Update the software versions, hostnames, bond interfaces, network addresses, and network VLAN information for the TVOE host and IDIH guests that you are installing.

Procedure 53. IDIH Installation (Optional)

9 ☐	PMAC: Run the fdconfig.	Run the fdconfig configuration by executing the following commands: <pre>\$ screen \$ sudo fdconfig config --file=<idih_fdc_file_name>.xml Example: \$ sudo fdconfig config --file=tvoe-ferbrms4_01-22-15.xml</pre> Note: This is a long duration command (45-90 Minutes). If the screen command was run prior to executing the fdconfig, perform a “<i>screen -dr</i>” to resume the screen session in the event of a terminal timeout etc.
10 ☐	PMAC GUI: Monitor the Configuration	If not already done so, establish a GUI session on the PMAC server. Navigate to Main Menu -> Task Monitoring   Status and Manage  Task Monitoring  Help  Legal Notices  Logout Monitor the IDIH configuration to completion.

4.16.2 Post IDIH Installation Configuration

The following sections should be executed after IDIH installation is complete.

4.17.2.1 IDIH Configuration: Configure DSR Reference Data Synchronization

After an IDIH fresh installation, reference data synchronization is initially disabled. Reference data synchronization requires some initial configuration before it is enabled.

The Trace Ref Data Adapter application must retrieve data from web services hosted by the DSR SOAM web server, and this requires the DSR SOAM virtual IP address (VIP) to be configured.

The DSR SOAM VIP will be unique at each customer site because it is defined based on the customer's network configuration. Therefore, there is no standard default value for the DSR SOAM VIP.

Procedure 54. Configure DSR Reference Data Synchronization for IDIH (Optional)

S T E P #	This procedure will provide the steps to configure DSR reference data synchronization for IDIH Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	IDIH Application Server: Login	Establish an SSH session to the IDIH Application Server. Login as user admusr. Issue the following commands to login as tekelec user. <pre>\$ sudo su - tekelec</pre>

Procedure 54. Configure DSR Reference Data Synchronization for IDIH (Optional)

2 □	IDIH Application Server: Execute Configuration Script.	Execute the following script: <pre>\$ apps/trda-config.sh Example output: corsair-app:/usr/TKLC/xIH/apps/trda-config.sh dos2unix: converting file /usr/TKLC/xIH/boa/user_projects/domains/tekelec/nsp/trace-refdata-ad Please enter DSR oam server IP address: 10.240.39.175 SQL*Plus: Release 12.1.0.2.0 Production on Thu Oct 1 15:04:40 2015 Copyright (c) 1982, 2014, Oracle. All rights reserved. Last Successful login time: Thu Oct 01 2015 13:27:57 -04:00 Connected to: Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics and Real Application Testing options SQL> SQL> 2 3 4 5 1 row merged. SQL> Commit complete. SQL> Disconnected from Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Produ With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics and Real Application Testing options Buildfile: /usr/TKLC/xIH/apps/trace-refdata-adapter/build.xml app.disable: common.weblogic.stop: [echo] [echo] [echo] ===== [echo] application: xihtra [echo] date: 2015-10-01 15:04:41 [echo] ===== [echo] === stop application EAR [echo] date: 2015-10-01 15:04:41 [java] weblogic.Deployer invoked with options: -adminurl t3://appserver:7001 -userconfigprojects/domains/tekelec/keyfile.secure -name xIH Trace Reference Data Adapter -stop [java] <Oct 1, 2015 3:05:08 PM EDT> <Info> <J2EE Deployment SPI> <BEA-260121> <Initiating [java] Task 24 initiated: [Deployer:149026]stop application xIH Trace Reference Data Adap [java] Task 24 completed: [Deployer:149026]stop application xIH Trace Reference Data Adap [java] Target state: stop completed on Server nsp [java] BUILD SUCCESSFUL Total time: 29 seconds Buildfile: /usr/TKLC/xIH/apps/trace-refdata-adapter/build.xml app.enable: common.weblogic.start: [echo] [echo] [echo] ===== [echo] application: xihtra [echo] date: 2015-10-01 15:05:10 [echo] ===== [echo] === start application EAR [echo] date: 2015-10-01 15:05:10 [java] weblogic.Deployer invoked with options: -adminurl t3://appserver:7001 -userconfigprojects/domains/tekelec/keyfile.secure -name xIH Trace Reference Data Adapter -start [java] <Oct 1, 2015 3:05:56 PM EDT> <Info> <J2EE Deployment SPI> <BEA-260121> <Initiating [java] Task 25 initiated: [Deployer:149026]start application xIH Trace Reference Data Ada [java] Task 25 completed: [Deployer:149026]start application xIH Trace Reference Data Ada [java] Target state: start completed on Server nsp [java] BUILD SUCCESSFUL Total time: 1 minute 17 seconds</pre> For prompt “Please enter DSR OAM server IP address”, enter the VIP of the DSR SOAM and press Enter. Note: If the address entered is unreachable the script will exit with error “Unable to connect to <ip-address>!”
DSR-8.0/8.1		282 February 2018

Procedure 54. Configure DSR Reference Data Synchronization for IDIH (Optional)

3 ☐	IDIH App Server: Monitor Completion	Monitor the log file located at: <code>/var/TKLC/xIH/log/apps/weblogic/apps/application.log</code> Examine the log file for entries containing text “Trace Reference Data Adapter”
4 ☐	iDIH App Server (Optional): Switch iDIH from one DSR to another DSR in a different network	Note: This is an optional step which is needed to switch an IDIH from one DSR to another DSR in a different network 1. Establish an SSH session to the iDIH Application Server. 2. Login as the tekelec user <u>Execute the below commands</u> 3. <code>cd /usr/TKLC/xIH/apps/trace-refdata-adapter</code> 4. <code>ant clean.data</code> 5. <code>cd /usr/TKLC/xIH/apps/xihoam</code> 6. <code>ant imp.init</code> (flush comagent connection data) 7. <code>cd /usr/TKLC/xIH/apps/trace-refdata-adapter</code> 8. <code>ant app.enable</code> (Sync MOs from SOAM) 9. <code>cd /usr/TKLC/xIH/apps</code> 10. <code>./trda-config.sh <DSR SOAM VIP in different network></code>

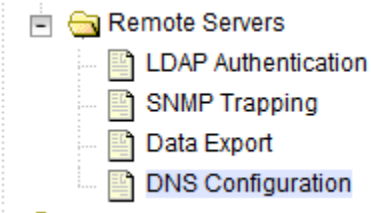
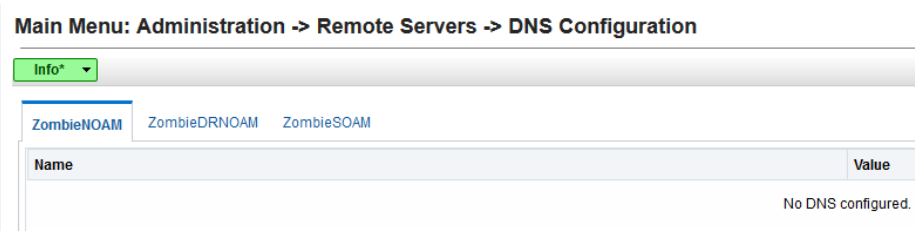
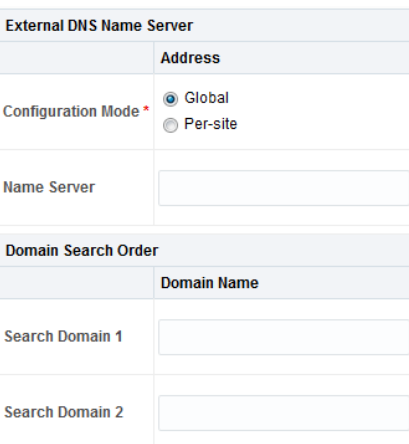
4.17.2.2 IDIH Configuration: Configuring the SSO Domain**Procedure 55. IDIH Configuration: Configuring the SSO Domain (Optional)**

STEP #	This procedure will provide the steps to configure SSO Domain for IDIH Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

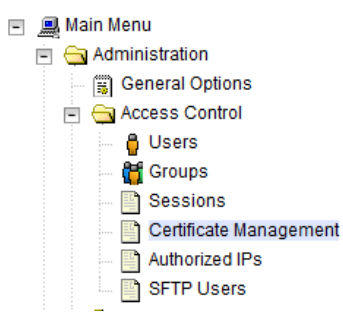
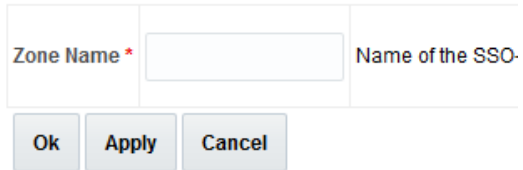
Procedure 55. IDIH Configuration: Configuring the SSO Domain (Optional)

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: <code>https://<Primary_NOAM_VIP_IP_Address></code> Login as the <i>guiadmin</i> user: 

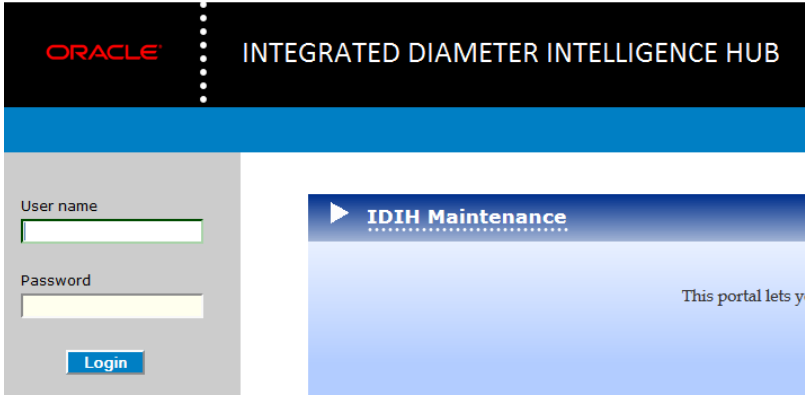
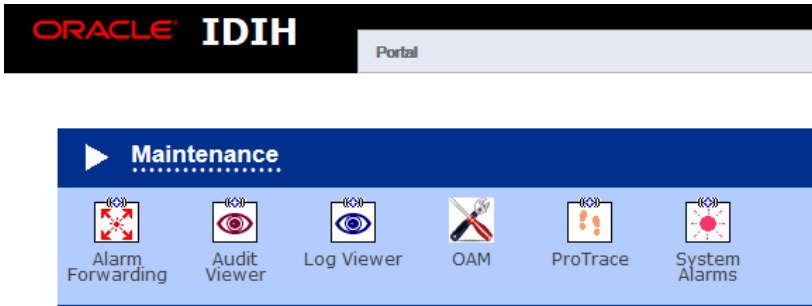
Procedure 55. IDIH Configuration: Configuring the SSO Domain (Optional)

2 ☐	NOAM VIP GUI: Configure DNS	Navigate to Main Menu -> Administration -> Remote Servers -> DNS Configuration  Select the NOAM tab:  Configure values for the following fields: • Domain Name • Name Server • Search Domain 1  If values have already been configured, select the Cancel button; otherwise configure the above values and select the Ok button. Ok Cancel

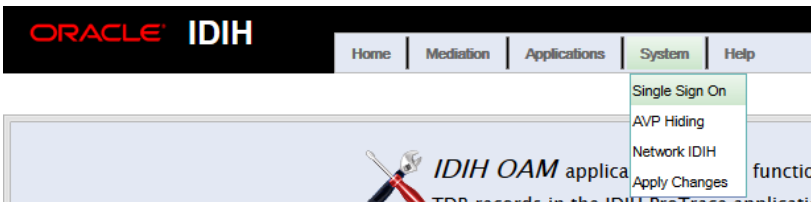
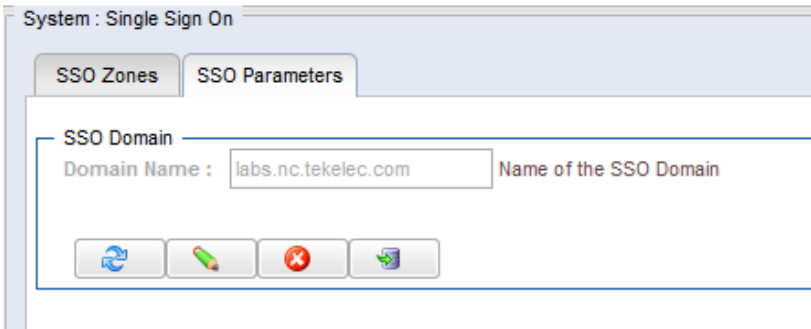
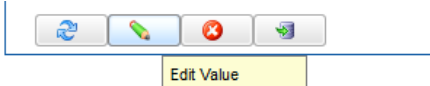
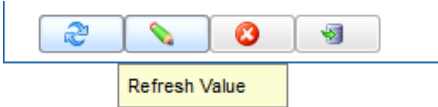
Procedure 55. IDIH Configuration: Configuring the SSO Domain (Optional)

3 ☐	NOAM VIP GUI: Establish SSO Local Zone	Navigate to Main Menu -> Access Control -> Certification Management  Select the Establish SSO Zone button  Enter a value for Zone Name:  Select the Ok button. Information for the new Certificate type of SSO Local is now displayed. Select the Report button.  The Certificate Report is displayed. Select and copy the encoded certificate text to the clipboard for future access. Example of Certificate report: <pre> -----BEGIN CERTIFICATE----- MIICKzCCAdWgAwIBAgIJAOVfSLNc3CeJMA0GCSqGSIb3DQEBCwUAMHExCzAJBgNV BAYTAlVTMQswCQYDVQQLIDAJQVJlEQMA4GA1UEBwwHUWJsZWlnaDEPMA0GA1UECgwG T3JhY2x1MQswCQYDVQQLIDAJQVJlEQMA4GA1UEAwHTG1iZXJ0eTETMBEGCSqGSIb3 DQEJARYEdGVzdDAeFw0xNTA1MDQxNDIzNTRaFw0xNjA1MDMxNDIzNTRaMHExCzAJ BgNVBAYTAlVTMQswCQYDVQQLIDAJQVJlEQMA4GA1UEBwwHUWJsZWlnaDEPMA0GA1UE CgwGT3JhY2x1MQswCQYDVQQLIDAJQVJlEQMA4GA1UEAwHTG1iZXJ0eTETMBEGCSqG SIb3DQEJARYEdGVzdDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQCZ/MpkhlvMP/iJ s5xDO2MwxJm3jYim43H8gR9pfBTMNP6L9kluJYi+2T0hngJFQLpIn6SK6pXnuAGY f/vDWfqPAgMBAAGjUDBOMB0GA1UdDgQWBBS6IzIOLP1gizQ6+BERr8Fo2XyDVFaf BgNVHSMGDAWgBS6IzIOLP1gizQ6+BERr8Fo2XyDVFADAMBgnVRMEBTADAQH/MA0G CSqGSIb3DQEBCwUAA0EAOWIqBMEQyvfv38r/yfgIx3w5dN8SBwHjHC5TpJrHV6U zFlg5dfzoLz7ditjGohWJ919VRw39LQ81KFp7SMXwA== -----END CERTIFICATE----- </pre>

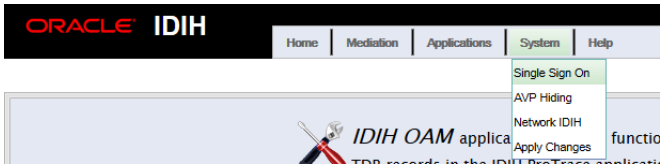
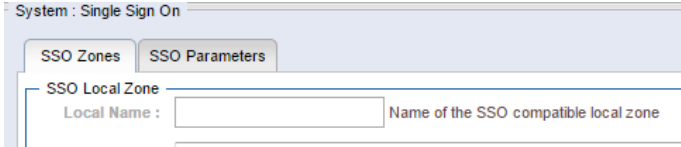
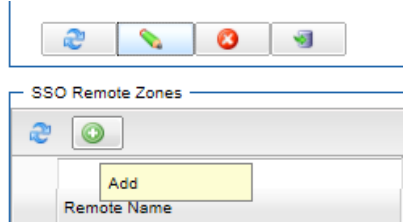
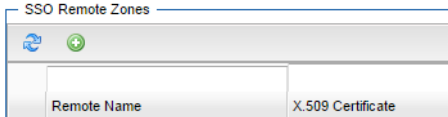
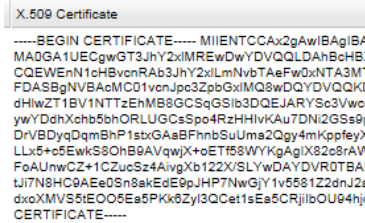
Procedure 55. IDIH Configuration: Configuring the SSO Domain (Optional)

4 ☐	IDIH Application Server GUI: Login	Establish a GUI session on the IDIH app server <app server IP>: Login as the <i>idihadmin</i> user: 
5 ☐	IDIH Application Server GUI: Launch the OAM portal	Navigate to the OAM portal Icon to Launch the OAM web application: 

Procedure 55. IDIH Configuration: Configuring the SSO Domain (Optional)

6 □	IDIH Application Server GUI: Configure the SSO Domain	Navigate to System -> Single Sign on  Select the SSO Parameters Tab  Select the Edit Value Icon Button  Enter a value for the Domain Name. Note: This should be the same domain name assigned in the DSR NOAM DNS Configuration (Step 2) Select the Save icon button.  Select the Refresh icon button to display data saved for the Remote Zone. 

Procedure 55. IDIH Configuration: Configuring the SSO Domain (Optional)

7 ☐	DIH Application Server GUI: Configure the SSO Remote Zone	Navigate to System -> Single Sign on  Select the SSO Zones Tab  Select the Add icon button  Enter a value for field Remote Name  For field X.509 Certificate, paste the encoded certificate text from the clipboard that was previously copied from the DSR NOAM.  Select the save icon  Select the Refresh icon to display the data saved for remote zone. 

4.17.2.3 IDIH Configuration: Configuring IDIH in the DSR

Procedure 56. IDIH Configuration: Configure IDIH in the DSR (Optional)

S T E P #		This procedure will provide the steps to complete the IDIH integration on the DSR. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: 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: https://<Primary_NOAM_VIP_IP_Address> Login as the <i>guiadmin</i> user:  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.
2 ☐	NOAM VIP GUI: Configure CommAgent Connection	Navigate to Main Menu -> Communication Agent -> Configuration -> Remote Servers

Procedure 56. IDIH Configuration: Configure IDIH in the DSR (Optional)

Communication Agent

Configuration

Remote Servers

Connection Groups

Routed Services

Select the **Insert** button

Insert

Edit

Delete

Add the IDIH Mediation Server

For the Remote Server IP address field, enter the IMI IP address of the IDIH Mediation Server.

For the IP address Preference field, enter the IP protocol preference (if IPv6 and IPv4 are configured)

Inserting Remote Servers

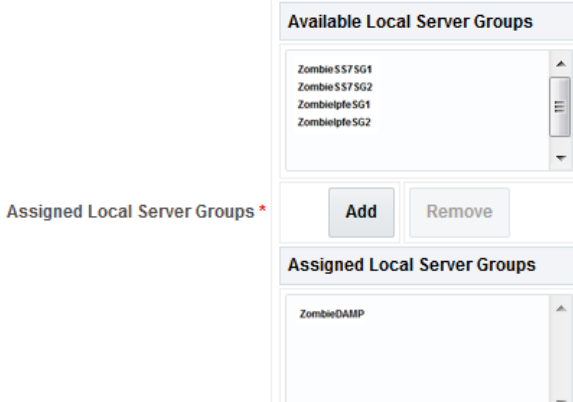
Field	Value
Remote Server Name *	
Remote Server IPv4 IP Address	
Remote Server IPv6 IP Address	
Remote Server Mode *	-- Select --
IP Address Preference	ComAgent Network Preference

Set the Remote Server Mode to **Server**

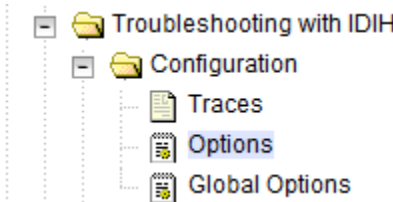
Select the DA-MP server group from the **Available Local Server Groups** column

Click the **Add** button to move the DA-MP server group to the **Assigned Local Server Groups** column

Procedure 56. IDIH Configuration: Configure IDIH in the DSR (Optional)

		 Click OK
3 ☐	SOAM VIP GUI: Login	Establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of: https://<Primary_SOAM_VIP_IP_Address> Login as the <i>guiadmin</i> user:  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.

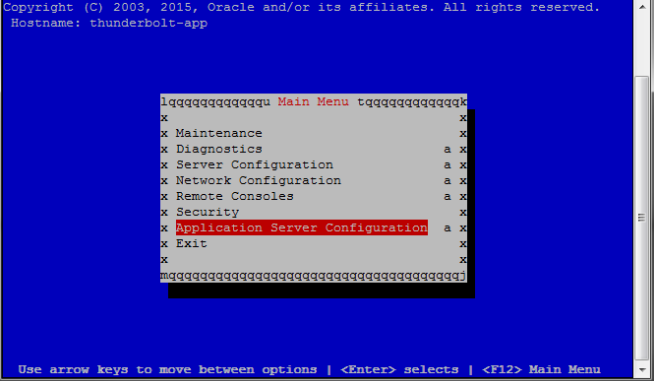
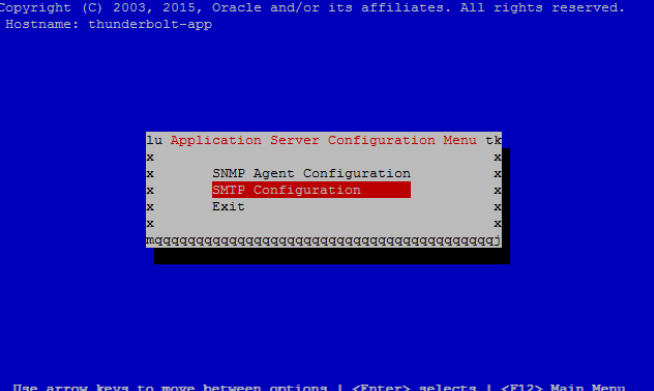
Procedure 56. IDIH Configuration: Configure IDIH in the DSR (Optional)

4 ☐	SOAM VIP GUI: Configure IDIH Hostname	Navigate to Main Menu -> Diameter -> Troubleshooting with IDIH -> Configuration -> Options  From the drop down box, Select the mediation server configured in Step to in the IDIH Host Name field Enter the fully qualified domain name (or IP address) of the App server in the IDIH Visualization Address field: IDIH Configuration <table border="1"> <thead> <tr> <th>Field</th><th>Value</th><th>Descri</th></tr> </thead> <tbody> <tr> <td>Max bandwidth *</td><td>25</td><td>Maximu will dis [Default</td></tr> <tr> <td>IDIH Host Name</td><td>- Select -</td><td>The Ho [Default</td></tr> <tr> <td>IDIH Visualization address</td><td></td><td>The IP ; If an IP [Default</td></tr> </tbody> </table> Apply Cancel Click the Apply button	Field	Value	Descri	Max bandwidth *	25	Maximu will dis [Default	IDIH Host Name	- Select -	The Ho [Default	IDIH Visualization address		The IP ; If an IP [Default
Field	Value	Descri												
Max bandwidth *	25	Maximu will dis [Default												
IDIH Host Name	- Select -	The Ho [Default												
IDIH Visualization address		The IP ; If an IP [Default												

4.17.2.4 IDIH Configuration: Configuring Mail Server (Optional)**Procedure 57. IDIH Configuration: Configure Mail Server-Optional (Optional)**

S T E P #	This procedure will provide the steps to configure the SMTP mail server. Note: This procedure is optional; however, this option is required for Security (password initialization set to AUTOMATIC) and Forwarding (forwarding by mail filter defined) and is available only on the Application server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	IDIH Application Server: Login	Establish an SSH session to the IDIH Application Server, login as admusr .

Procedure 57. IDIH Configuration: Configure Mail Server-Optional (Optional)

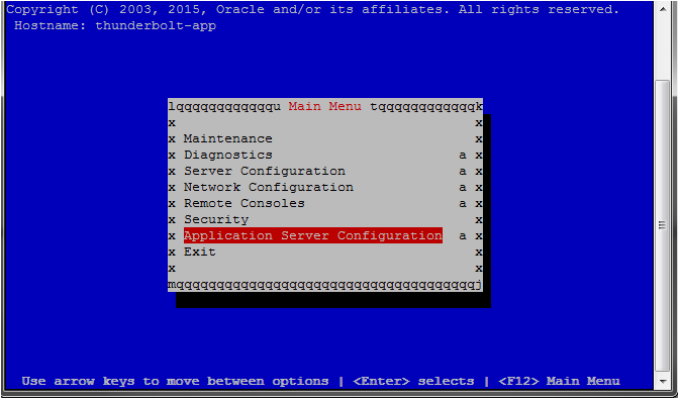
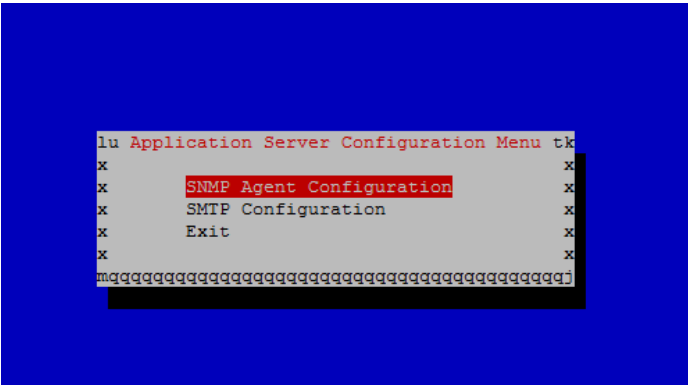
2 ☐	IDIH Application Server: Configure the Authenticated Mail Server	Enter the platcfg menu, execute the following command: \$ sudo su - platcfg Select Application Server Configuration  Select SMTP Configuration  Select Edit Enter the following parameters: 1. Mail Server IP Address 2. User 3. Password 4. Email Address (From) 5. Mail smtp timeout 6. Mail smtp connectiontimeout 7. SNMP over SSL used? Select OK Select Exit to exit the platcfg menu.

4.17.2.5 IDIH Configuration: Configuring SNMP Management Server (Optional)

Procedure 58. IDIH Configuration: Configure SNMP Management Server-Optional (Optional)

S T E P #	This procedure will provide the steps to configure the SNMP management server. Note: This procedure is optional; however, this option is required for Forwarding (forwarding by SNMP filter defined) and is available only on the application server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	IDIH Application Server: Login	Establish an SSH session to the IDIH Application Server, login as admusr .

Procedure 58. IDIH Configuration: Configure SNMP Management Server-Optional (Optional)

2 ☐	IDIH Application Server: Configure SNMP Management Server	Enter the platcfg menu, execute the following command: \$ sudo su - platcfg Select Application Server Configuration  Select SNMP Agent Configuration  Select Edit Enter the IP address of the SNMP Management Server Note: The SNMP agent configuration is updated and the SNMP Management server is automatically restarted. Select OK Select Exit to exit the platcfg menu.

4.17.2.6 IDIH Configuration: Change Network Interface (Optional)

Procedure 59. IDIH Configuration: Change Network Interface-Optional (Optional)

S T E P #	This procedure will provide the steps to change the default network interface Note: Initially the default network interface used to transport TTRs from DSR to DIH uses the internal imi network; however, this can be changed if required. It should be noted that changing this interface could degrade performance of TTR transmission. Note: A script is provided to manage the settings so that the operator doesn't need to know the details required to apply the settings. There are two settings 'interface.name' and 'interface.enabled'. When interface.enabled=True then communications over the 'interface.name =value', where value is the name of the network interface as defined on the platform, is the only specified interface that is used for communications. When 'interface.enabled=False' then communications over the named interface is not enforced, that is, all interfaces configured on the platform are allowed to be used for communications. For example, if it is required to use the xmi interface for communication instead of the default internal imi interface, then the operator would supply 'xmi' when prompted for the interface name and 'True' when prompted if interface filtering should be applied. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	IDIH Mediation Server: Login	Establish an SSH session to the IDIH Mediation Server. Login as user admusr. Issue the following commands to login as tekelec user. <pre>\$ sudo su - tekelec</pre>

Procedure 59. IDIH Configuration: Change Network Interface-Optional (Optional)

2 ☐	IDIH Mediation Server: Execute the Change Interface Script	Execute the change interface script with the following command: <pre>\$ chgIntf.sh</pre> Answer the following questions during execution of the script: This script is used to change the interface name (default = imi) used for mediation communications and whether to enable network interface filtering or not. Please answer the following questions or enter CTRL-C to exit out of the script. Current setting are: interface.name=imi interface.enabled=True Enter new network interface name, return to keep current [imi]: xmi Do you want to enable network interface filtering [True False], return to keep current [True]: Updating configuration properties file with 'interface.name=xmi' and 'interface.enable=True', and restarting mediation configuration bundle...

4.17.2.7 IDIH Configuration: CPU Pinning

Follow **Section 4.13** for CPU Pinning on the servers that host the IDIH VMs.

4.17.2.8 IDIH Configuration: Generate Disaster Recovery FDC File (Optional)**Procedure 60. IDIH Configuration: Backup the upgrade and Disaster Recovery FDC File-Optional (Optional)**

STEP #	This procedure will provide the steps to generate a disaster recovery fdc file. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Identify Backup Server	Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items: • TVOE • PMAC • DSR NOAM • DSR SOAM
2 ☐	PMAC: Establish Terminal Session	Establish an SSH session to the PMAC. Login as admusr .

Procedure 60. IDIH Configuration: Backup the upgrade and Disaster Recovery FDC File-Optional (Optional)

3 ☐	PMAC: Verify Upgrade fdc file exists	Execute the following commands to verify the upgrade FDC file for IDIH exists: <pre>\$ cd /var/TKLC/smac/guest-dropin</pre> <pre>\$ ls -l *.xml</pre> The following output is expected: <pre>-rw-r----- 1 root smac 9542 May 11 09:43 <idih_install>.xml -rw-r----- 1 root smac 5107 May 11 09:43 <idih_upgrade>.xml</pre> Note: The <idih_upgrade>.xml file is the same file used for upgrade and disaster recovery procedures.
4 ☐	PMAC: Transfer the FDC file to a remote server.	Login to the backup server identified in step 1 and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system. <pre>\$ sudo scp admusr@<PMAC_IP_Address>:/var/TKLC/smac/guest-dropin/<idih_upgrade.xml> /path/to/destination/</pre> When prompted, enter the admusr user password and press Enter. If the Customer System is a Windows system please refer to [14] procedure <i>Using WinSCP</i> to copy the backup image to the customer system.
5 ☐	PMAC Server: Backup FDC file	Transfer the fdc file to the fdc directory so that the file can be backed up with PMAC backups. Issue the following command to ensure that the directory where the backups will be stored exists: <pre>\$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/fdc</pre> If you receive an error such as the following: <pre>-bash: ls: /usr/TKLC/smac/etc/fdc: No such file or directory</pre> Create the directory by issuing the following command: <pre>\$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/fdc</pre> Issue the following command to copy the fdc files to the fdc backup directory: <pre>\$ sudo cp /var/TKLC/smac/etc/<idih_upgrade.xml> /usr/TKLC/smac/etc/fdc/</pre>

4.17 Post-Install Activities

4.17.1 Optimization (DSR & Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)

Procedure 61. Optimization Procedure (DSR & Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)

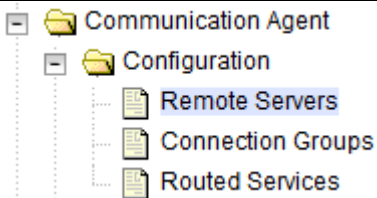
S T E P #	This procedure will provide instruction on how to run Optimization Scripts for Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only. Prerequisite: All previous DSR installation steps have been completed. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	DSR NOAM VIP: Login	Establish an SSH to the NOAM VIP address, login as admusr .
2 ☐	DSR NOAM VIP: Execute the Optimization Script on the Active NOAM	Execute the following commands to execute the performance optimization script on the active NOAM: <pre>\$ cd /usr/TKLC/dsr/bin/ \$ sudo ./rmsNoamConfig.sh</pre> Note: Configuration Successful output should be given.

4.17.2 Configure ComAgent Connections (DSR + SDS Only)

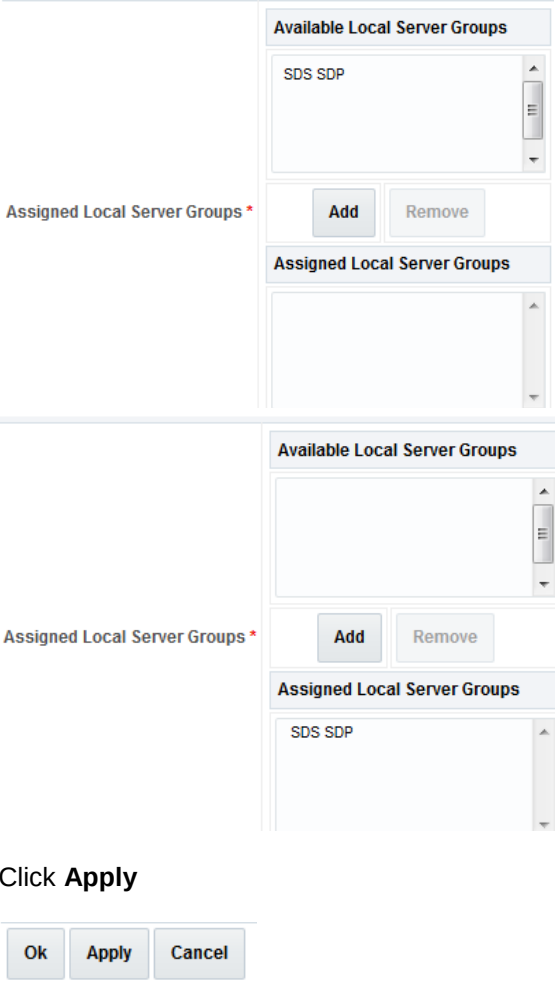
Procedure 62. Configure ComAgent Connections (DSR + SDS Only)

S T E P #	This procedure will provide instruction on how to configure ComAgent connections on DSR/SDS for use in the FABR application. Prerequisite: FABR application is activated. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	SDS NOAM VIP GUI: Login Establish a GUI session on the SDS NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: <code>https://<Primary_SDS_NOAM_VIP_IP_Address></code> Login as the <i>guiadmin</i> user: 
2 ☐	SDS NOAM VIP GUI: Configure Remote Navigate to Main Menu -> Communication Agent -> Configuration -> Remote Servers

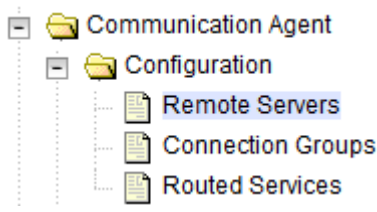
Procedure 62. Configure ComAgent Connections (DSR + SDS Only)

	Server IP Address	 Click Insert Insert Edit Delete
3	SDS NOAM VIP GUI: Configure Remote Server IP Address	Enter the Remote Server Name for the DSR MP Server: Remote Server Name * ZombieDAMP1 Enter the Remote Server IMI IP address: Remote Server IPv4 IP Address 169.254.1.13 Remote Server IPv6 IP Address Note: This should be the IMI IP address of the DAMP server. Select Client for the Remote Server Mode from the pull down menu: Remote Server Mode * Client ▼ Select Preference (ComAgent Network Preference, IPv4, or IPv6) for IP Address Preference pull down menu: IP Address Preference ComAgent Network Preference ▼ ComAgent Network Preference IPv4 Preferred IPv6 Preferred Select the Local Server Group from the available SDS DP server groups and click 'Add' to assign.

Procedure 62. Configure ComAgent Connections (DSR + SDS Only)

		 Click Apply Ok Apply Cancel
4	SDS NOAM VIP GUI: Repeat	Repeat steps 2-3 for each remote MP in the same SOAM NE.
5	DSR NOAM VIP GUI: Login	Establish a GUI session on the DSR NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: <code>https://<Primary_DSR_NOAM_VIP_IP_Address></code> Login as the guiadmin user:

Procedure 62. Configure ComAgent Connections (DSR + SDS Only)

		 The screenshot shows the Oracle System Login page. At the top is the Oracle logo. Below it is the title 'Oracle System Login' and a timestamp 'Mon Jul 11 13:59:37 2016 EDT'. A central box contains a 'Log In' form with fields for 'Username' and 'Password', a 'Change password' checkbox, and a 'Log In' button. Below the form, it says 'Welcome to the Oracle System Login.' and provides information about browser compatibility and unauthorized access. At the bottom, it includes trademark notices and copyright information for 2010, 2016, and Oracle.
6	DSR NOAM VIP GUI: ☐ Configure Remote Server IP Address	Navigate to Main Menu -> Communication Agent -> Configuration -> Remote Servers  The navigation tree shows 'Communication Agent' expanded, with 'Configuration' selected. Under 'Configuration', 'Remote Servers' is highlighted. Other options are 'Connection Groups' and 'Routed Services'. Click Insert  Buttons: Insert, Edit, Delete
7	DSR NOAM VIP GUI: ☐ Configure Remote Server IP Address	Enter the Remote Server Name for the SDS DP Server:  The form shows a label 'Remote Server Name *' and a text input field containing 'SDSDP1'. Enter the Remote Server IMI IP address:

Procedure 62. Configure ComAgent Connections (DSR + SDS Only)

	Remote Server IPv4 IP Address 169.254.1.30 Remote Server IPv6 IP Address Note: This should be the IMI IP address of the DP Server. Select Server for the Remote Server Mode from the pull down menu: Remote Server Mode * Server ▼ Select Preference (ComAgent Network Preference, IPv4, or IPv6) for IP Address Preference pull down menu: IP Address Preference ComAgent Network Preference ▼ ComAgent Network Preference IPv4 Preferred IPv6 Preferred Select the Local Server Group from the available SDS DP server groups and click 'Add' to assign: Assigned Local Server Groups * Available Local Server Groups ZombieDAMP ZombieS57SG1 ZombieS57SG2 ZombieIpfSG1 ZombieIpfSG2 Add Remove Assigned Local Server Groups

Procedure 62. Configure ComAgent Connections (DSR + SDS Only)

		Available Local Server Groups ZombieSS7SG1 ZombieSS7SG2 ZombieIpfSG1 ZombieIpfSG2 Add Remove Assigned Local Server Groups ZombieDAMP Click Apply Ok Apply Cancel				
8	DSR NOAM VIP GUI: Repeat	Repeat steps 6-7 for each remote DP in the same SOAM NE.				
9	DSR NOAM VIP GUI: Configure Connection Groups	Navigate to Main Menu -> Communication Agent -> Configuration -> Connection Groups Communication Agent Configuration Remote Servers Connection Groups Routed Services				
10	DSR NOAM VIP GUI: Edit Connection Groups	Select the DPSvcGroup Connection Group <table><tr><th>Connection Group</th><th>Server</th></tr><tr><td>DPSvcGroup</td><td>0 Servers</td></tr></table> Click Edit Select the desired DP servers from the Available Servers in Network Element:	Connection Group	Server	DPSvcGroup	0 Servers
Connection Group	Server					
DPSvcGroup	0 Servers					

Procedure 62. Configure ComAgent Connections (DSR + SDS Only)

		Connection Group Name * DPSvcGroup Available Servers in Network Element Turks-DP1 Turks-DP2 Add Remove Assigned Servers in Connection Group Assigned Servers in Connection Group * Click Add	Connection Group. [Default: n/a; Range: A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.] [A value is required.] This field specifies the Remote Servers which can be in the Connection Group. Remote Servers which are available will be in the Available Servers in Network Element list. Remote Servers which are in the Connection Group will be in the Assigned Servers in Connection Group list. [Default = n/a; Range = List of configured Remote Servers]
		Connection Group Name * DPSvcGroup Available Servers in Network Element Turks-DP2 Add Remove Assigned Servers in Connection Group Turks-DP1 Assigned Servers in Connection Group * Ok Apply Cancel Click Ok	Connection Group. [Default: n/a; Range: A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.] [A value is required.] This field specifies the Remote Servers which can be in the Connection Group. Remote Servers which are available will be in the Available Servers in Network Element list. Remote Servers which are in the Connection Group will be in the Assigned Servers in Connection Group list. [Default = n/a; Range = List of configured Remote Servers]
11	DSR NOAM VIP	Verify Correct number of servers are in the connection group.	

Procedure 62. Configure ComAgent Connections (DSR + SDS Only)

☐

GUI: Verify correct number of servers in group

Connection Group	Server
DPSvcGroup	1 Server SDSDP1

4.17.3 Activate Optional Features

Procedure 63. Activate Optional Features

S T E P #	This procedure will provide instruction on how to install DSR optional components once regular installation is complete. Prerequisite: All previous DSR installation steps have been completed. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Refer to Install Guides for Optional Features to Complete Installation	Refer to Section 3.3 for a list of feature install documents whose procedures are to be executed at this moment.
2 ☐	DR-NOAM: Feature Activation	If the DR NOAM was configured in Section 4.15.3, and MAPIWF has been activated in step 1; SSH to the active DR-NOAM, login as admusr. Execute the following commands: <pre>\$ cd /usr/TKLC/dsr/prod/maint/loaders/activate \$ sudo ./load.mapinterworkingActivateAsourced</pre> Repeat this step for the standby DR-NOAM.

4.17.4 Shared Secret Encryption Key Revocation (RADIUS Only)

Procedure 64: Shared secret encryption key revocation (RADIUS Only)

S T E P #	This procedure will provide instruction on how to change shared secret encryption key on DSR RADIUS setup. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Revoke RADIUS shared secret encryption key	Refer to RADIUS Shared Secret Key revocation MOP to change the encryption key on the DSR installed setup. Refer to [17] Note: This is highly recommended to change the key after installation due to security reasons.

4.17.5 Enable/Disable DTLS (SCTP Diameter Connections Only)

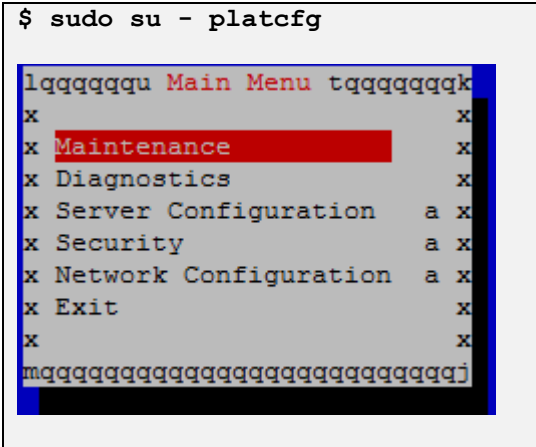
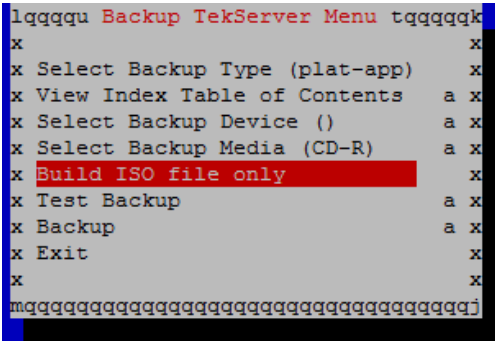
Procedure 65. Enable/Disable DTLS (SCTP Diameter Connections Only)

S T E P #	This procedure will provide instructions on how to prepare clients before configuring SCTP diameter connections.  Important  Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Enable/Disable DTLS (SCTP Diameter Connections Only)	Oracle's SCTP Datagram Transport Layer Security (DTLS) has SCTP AUTH extensions by default. SCTP AUTH extensions are required for SCTP DTLS. However, there are known impacts with SCTP AUTH extensions as covered by the CVEs referenced below. It is highly recommended that customers installing should prepare clients before the DSR connections are established after installation. This will ensure the DSR to Client SCTP connection will establish with SCTP AUTH extensions enabled. See RFC 6083. If customers DO NOT prepare clients to accommodate the DTLS changes, then the SCTP connections to client devices MAY NOT establish after the DSR is installed. https://access.redhat.com/security/cve/CVE-2015-1421 https://access.redhat.com/security/cve/CVE-2014-5077 Execute procedures in [15] to disable/enable the DTLS feature.

4.17.6 Backup TVOE Configuration**Procedure 66. Backup TVOE Configuration**

S T E P #	This procedure will provide instruction on how to back up each TVOE rack mount server after a successful installation. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Identify Backup Server	Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items: • TVOE • PMAC • DSR NOAM • DSR SOAM • SDS NOAM • SDS DP SOAM
2 ☐	TVOE Server: Login	Establish an SSH session to the TVOE host server, login as admusr.

Procedure 66. Backup TVOE Configuration

3 ☐	TVOE Server: Build ISO backup file	Execute the following command from the TVOE server: <pre>\$ sudo su - platcfg</pre>  Select the following menu options sequentially: Maintenance -> Backup and Restore ->Backup Platform (CD/DVD). The “Backup TekServer Menu” page will now be shown. Note: If no cdrom device is found by TPD, you will receive an error dialog with the message: "No disk device available. This is normal on systems without a cdrom device." Press Enter to continue. Build the backup ISO image by selecting: Build ISO file only  Note: Creating the ISO image may happen so quickly that this screen may only appear for an instant. After the ISO is created, platcfg will return to the Backup TekServer Menu. The ISO has now been created and is located in the /var/TKLC/bkp/ directory. An example filename of a backup file that was created is: "hostname1307466752-plat-app-201104171705.iso" Exit out of platcfg by selecting Exit.

Procedure 66. Backup TVOE Configuration

4 ☐	Backup Server: Transfer TVOE Files to Backup Server	Login to the backup server identified in step 1 and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system. <pre>\$ sudo scp tvoexfer@<TVOE IP Address>:/var/TKLC/bkp/* /path/to/destination/</pre> Move the TVOE backup to a customer provided backup server for safe keeping. When prompted, enter the tvoexfer user password and press Enter. If the Customer System is a Windows system please refer to [14] procedure <i>Using WinSCP</i> to copy the backup image to the customer system. The TVOE backup file has now been successfully placed on the backup server.
5 ☐	Repeat for Additional TVOE Servers	Repeat steps 2-4 for additional TVOE servers

4.17.7 Backup PMAC Application**Procedure 67. Backup PMAC Application**

STEP #	This procedure will provide instruction on how to back up each PMAC application installed in this procedure. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Identify Backup Server	Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items: • TVOE • PMAC • DSR NOAM • DSR SOAM • SDS NOAM • SDS DP SOAM
2 ☐	PMAC Server: Login	Establish an SSH session to the PMAC server, login as admusr .

Procedure 67. Backup PMAC Application

3 ☐	PMAC Server: Build backup File	Execute the following command from the PMAC server: <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm backup</pre> <pre>PM&C backup been successfully initiated as task ID 7</pre> Note: The backup runs as a background task. To check the status of the background task use the PMAC GUI Task Monitor page: or issue the command "sudo pmaccli getBgTasks". The result should eventually be "PMAC Backup successful" and the background task should indicate "COMPLETE".
4 ☐	PMAC GUI: Login	Open web browser and enter: <pre>http://<PMAC_Mgmt_Network_IP></pre> Login as guiadmin user:  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 67. Backup PMAC Application

5	PMAC Server GUI: Monitor/Verify Backup Task Completion	Navigate to Main Menu -> Task Monitoring Status and Manage Task Monitoring Help Legal Notices Logout Monitor the Backup PMAC Task: Main Menu: Task Monitoring Filter* <table><tr><th>ID</th><th>Task</th><th>Target</th><th>Status</th><th>State</th></tr><tr><td> 1458 </td><td>Backup PM&C</td><td></td><td>PM&C Backup successful</td><td>COMPLETE</td></tr></table> Note: Alternatively, you can monitor the Backup task by executing the following command: \$ sudo pmaccli getBgTasks	ID	Task	Target	Status	State	1458	Backup PM&C		PM&C Backup successful	COMPLETE
ID	Task	Target	Status	State								
1458	Backup PM&C		PM&C Backup successful	COMPLETE								
6	Backup Server: Transfer PMAC File to Backup Server	Login to the backup server identified in step 1 and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system. \$ sudo scp admusr@<PMAC_IP_Address>:/var/TKLC/smac/backup/* /path/to/destination/ When prompted, enter the admusr user password and press Enter. If the Customer System is a Windows system please refer to [14] procedure <i>Using WinSCP</i> to copy the backup image to the customer system.										
7	Repeat for Additional PMAC Servers	Repeat steps 2-6 for additional PMAC servers										

4.17.8 Backup NOAM Database

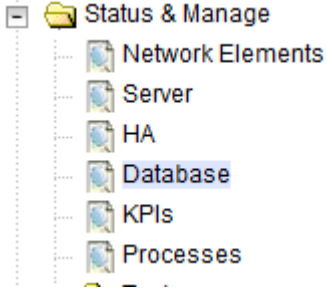
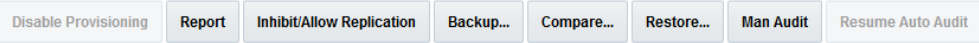
Procedure 68. NOAM Database Backup

S T E P #	This procedure will provide instruction on how to back up the NOAM Database. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Identify Backup Server	Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items: • TVOE • PMAC • DSR NOAM • DSR SOAM • SDS NOAM • SDS DP SOAM

Procedure 68. NOAM Database Backup

2 ☐	NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: <code>http://<Primary_NOAM_VIP_IP_Address></code> Login as the <i>guiadmin</i> user: 

Procedure 68. NOAM Database Backup

3	NOAM VIP GUI: Perform Database Backup	Navigate to Main Menu -> Status & Manage -> Database  Select the Active NOAM Select the Backup Button:  Select the desired file compression method Database Backup <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td colspan="3">Server: ZombieNOAM2</td> </tr> <tr> <td>Select data for backup</td> <td> ☐ Provisioning ☒ Configuration </td> <td>Select the type of Backup to perform.</td> </tr> <tr> <td>Compression *</td> <td> ☐ gzip ☒ bzip2 ☐ none </td> <td> Select the backup archive compression algorithm The following file suffix will be applied for the selected compression method: • .tar.gz - gzip compression, • .tar.bz2 - bzip2 compression, • .tar - no compression. [A value is required.] </td> </tr> <tr> <td>Archive Name *</td> <td>Backup.dsr.ZombieNOAM2.Configuration.NETWORK_OAMP.20160810_13073</td> <td>Modify archive name if desired. Do not include the following characters: ' ' \$</td> </tr> <tr> <td>Comment</td> <td> </td> <td>May not contain the following characters: ' ' \$</td> </tr> </tbody> </table> Ok Cancel Set the archive file name if needed. Select OK	Field	Value	Description	Server: ZombieNOAM2			Select data for backup	☐ Provisioning ☒ Configuration	Select the type of Backup to perform.	Compression *	☐ gzip ☒ bzip2 ☐ none	Select the backup archive compression algorithm The following file suffix will be applied for the selected compression method: • .tar.gz - gzip compression, • .tar.bz2 - bzip2 compression, • .tar - no compression. [A value is required.]	Archive Name *	Backup.dsr.ZombieNOAM2.Configuration.NETWORK_OAMP.20160810_13073	Modify archive name if desired. Do not include the following characters: ' ' \$	Comment		May not contain the following characters: ' ' \$
Field	Value	Description																		
Server: ZombieNOAM2																				
Select data for backup	☐ Provisioning ☒ Configuration	Select the type of Backup to perform.																		
Compression *	☐ gzip ☒ bzip2 ☐ none	Select the backup archive compression algorithm The following file suffix will be applied for the selected compression method: • .tar.gz - gzip compression, • .tar.bz2 - bzip2 compression, • .tar - no compression. [A value is required.]																		
Archive Name *	Backup.dsr.ZombieNOAM2.Configuration.NETWORK_OAMP.20160810_13073	Modify archive name if desired. Do not include the following characters: ' ' \$																		
Comment		May not contain the following characters: ' ' \$																		

Procedure 68. NOAM Database Backup

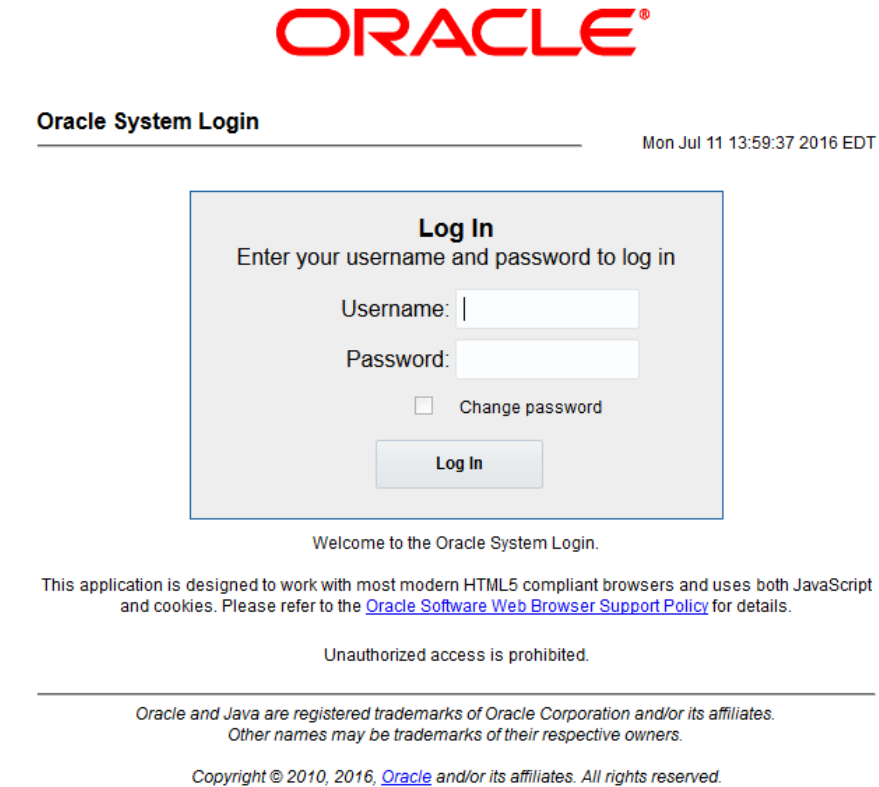
4 ☐	Backup Server: Transfer File to Backup Server	Login to the backup server identified in step 1 and copy backup image and key file (RADIUS Only) to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system. <pre>\$ sudo scp admusr@<NOAM VIP>:/var/TKLC/db/filemgmt/backup/* /path/to/destination/</pre> Execute following command to encrypt the key file before sending to filemgmt area : <pre>\$./sharedKrevo -encr</pre> Copy key file to customer server : <pre>\$ sudo scp admusr@<NOAM VIP>:/var/TKLC/db/filemgmt/DpiKf.bin.encr /path/to/destination/</pre> When prompted, enter the admusr user password and press Enter. If the Customer System is a Windows system please refer to [14] procedure <i>Using WinSCP</i> to copy the backup image to the customer system.
5 ☐	Repeat for Additional NOAM Servers	Repeat steps 2-4 for additional DSR and SDS NOAM Sites

4.17.9 Backup SOAM Database

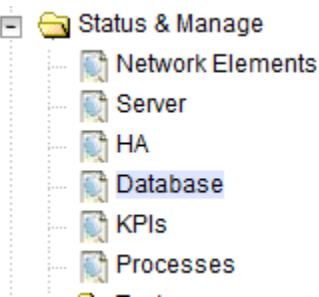
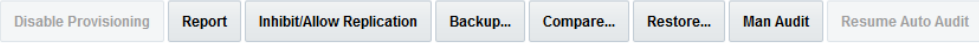
Procedure 69. SOAM Database Backup

S T E P #	This procedure will provide instruction on how to back up the SOAM Database. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Identify Backup Server	Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items: • TVOE • PMAC • DSR NOAM • DSR SOAM • SDS NOAM • SDS DP SOAM

Procedure 69. SOAM Database Backup

2 ☐	SOAM VIP GUI: Login	Establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of: <code>http://<Primary_SOAM_VIP_IP_Address></code> Login as the <i>guiadmin</i> user: 

Procedure 69. SOAM Database Backup

3 ☐	SOAM VIP GUI: Perform Database Backup	Navigate to Main Menu -> Status & Manage -> Database  Select the Active SOAM Select the Backup Button:  Select the desired file compression method Database Backup <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> <th>Descrip</th> </tr> </thead> <tbody> <tr> <td colspan="3">Server: ZombieSOAM1</td> </tr> <tr> <td>Select data for backup</td> <td> ☐ Provisioning ☒ Configuration </td> <td>Select th</td> </tr> <tr> <td>Compression *</td> <td> ☐ gzip ☒ bzip2 ☐ none </td> <td> Select th The follo • .t • .t • .t [A value </td> </tr> <tr> <td>Archive Name *</td> <td>Backup.dsr.ZombieSOAM1.Configuration.SYSTEM_OAM.20160810_130916.M</td> <td>Modify ai</td> </tr> <tr> <td>Comment</td> <td> </td> <td>May not i</td> </tr> </tbody> </table> Ok Cancel Set the archive file name if needed. Select OK	Field	Value	Descrip	Server: ZombieSOAM1			Select data for backup	☐ Provisioning ☒ Configuration	Select th	Compression *	☐ gzip ☒ bzip2 ☐ none	Select th The follo • .t • .t • .t [A value	Archive Name *	Backup.dsr.ZombieSOAM1.Configuration.SYSTEM_OAM.20160810_130916.M	Modify ai	Comment		May not i
Field	Value	Descrip																		
Server: ZombieSOAM1																				
Select data for backup	☐ Provisioning ☒ Configuration	Select th																		
Compression *	☐ gzip ☒ bzip2 ☐ none	Select th The follo • .t • .t • .t [A value																		
Archive Name *	Backup.dsr.ZombieSOAM1.Configuration.SYSTEM_OAM.20160810_130916.M	Modify ai																		
Comment		May not i																		

Procedure 69. SOAM Database Backup

4 ☐	Backup Server: Transfer SOAM File to Backup Server	Login to the backup server identified in step 1 and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system. <pre>\$ sudo scp admusr@<SOAM VIP>:/var/TKLC/db/filemgmt/backup/* /path/to/destination/</pre> When prompted, enter the admusr user password and press Enter. If the Customer System is a Windows system please refer to [14] procedure <i>Using WinSCP</i> to copy the backup image to the customer system.
5 ☐	Repeat for Additional TVOE Servers	Repeat steps 2-4 for additional DSR SOAM Sites

Appendix A: Pre-IPM Procedures

Appendix A.1: Setting the Server's CMOS Clock

The date and time in the server's CMOS clock must be set accurately before running the IPM procedure.

Note: The IPM installation process managed by PMAC for blade servers automatically sets the server's CMOS clock, so there is no need to set the server CMOS clock when using PMAC.

Appendix A.2: Configure the RMS Server BIOS Settings

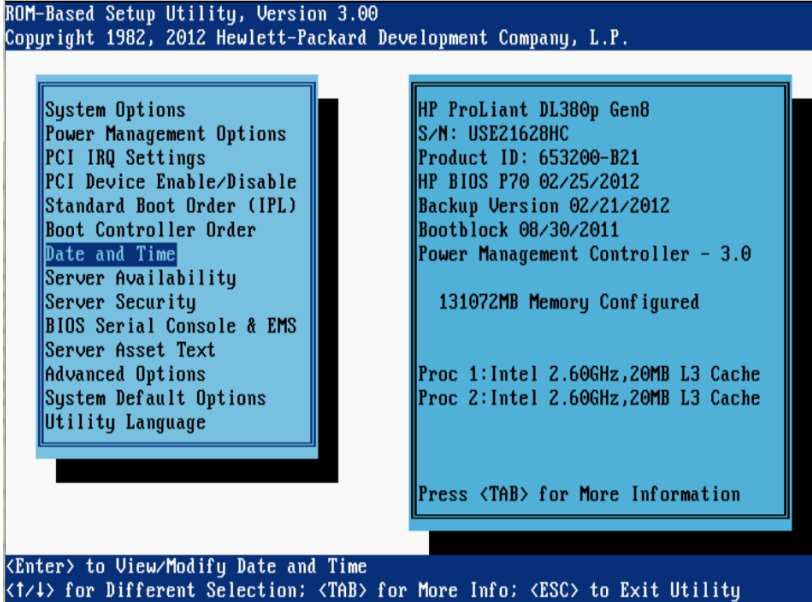
Appendix A.2.1: Configure HP Gen 8 Servers

Follow these steps to configure HP Gen 8 server BIOS settings

Appendix A.2.1. Configure HP Gen 8 Server BIOS Settings

STEP #	This procedure explains the steps needed to configure HP DL380 Server BIOS Settings Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

Appendix A.2.1. Configure HP Gen 8 Server BIOS Settings

1 ☐	HP DL380 Server: Connect VGA Monitor and USB Keyboard	Connect via a VGA monitor and USB keyboard.
2 ☐	HP DL380 Server: Reboot	Reboot the server and after the server is powered on, press the <F9> key when prompted to access the ROM-Based Setup Utility: 
3 ☐	HP DL380 Server: Select the Date and Time	From the above screen (Step 1), set the data and time to GMT (Greenwich Mean Time). Press <Esc> to navigate to the main menu
4 ☐	HP DL380 Server: Server Availability	From the above screen (Step 1), select Server Availability. • Change Automatic Power-On to Enabled • Change Power-On Delay to No Delay • Press <Esc> to navigate to the main menu
5 ☐	HP DL380 Server: System Options	From the above screen (Step 1), Select System Options. • Select Power Management Options • Select HP Power Regulator • Select HP Status High Performance Mode • Press <ESC> to navigate to the main menu.

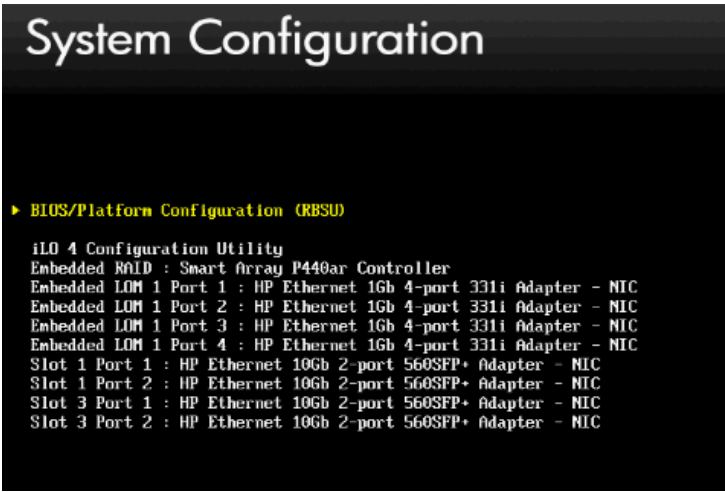
Appendix A.2.1. Configure HP Gen 8 Server BIOS Settings

6 ☐	HP DL380 Server: Power Management Options	From the above screen (Step 1), Select System Options. • Select Processor Options. • Change Intel® Virtualization Technology to Enabled. • Press <ESC> to return to System Options. • Select Serial Port Options.
7 ☐	HP DL380 Server: Exit ROM-Based Utility	Press <ESC> to Save and Exit from the ROM-Based Setup Utility.

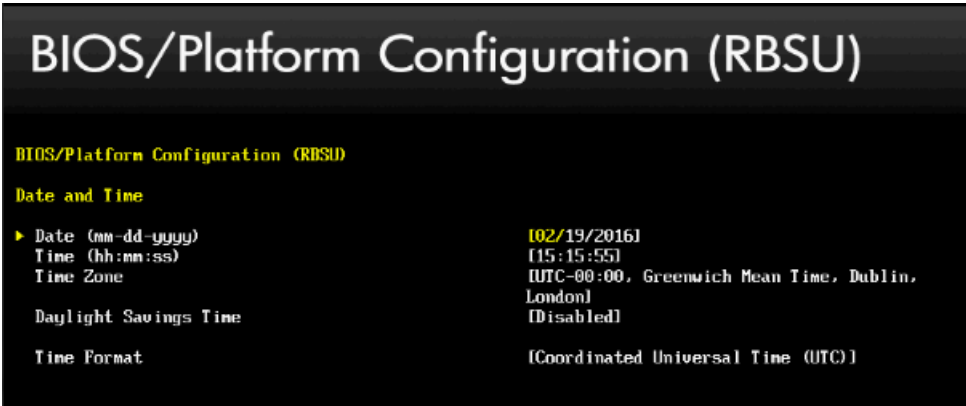
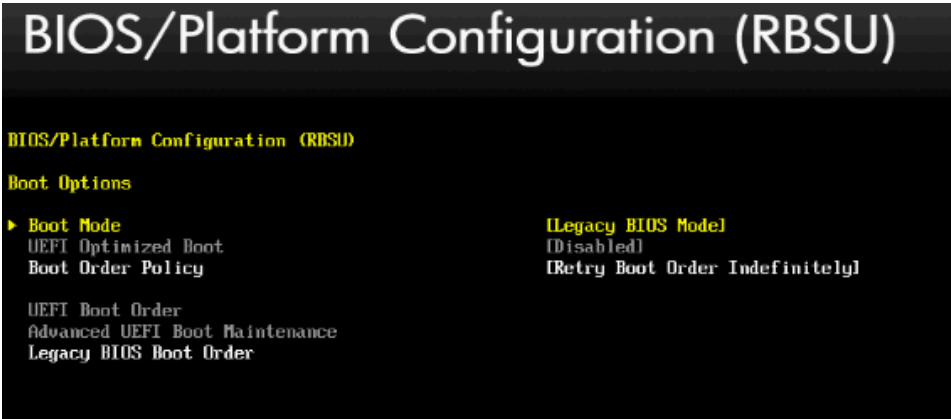
Appendix A.2.2: Configure HP Gen 9 Servers

The HP Gen 9 systems can have UEFI boot enabled. Since TPD is configured to use the Legacy BIOS option, rack mount Gen 9 servers should have their BIOS settings checked before IPM. Rack mount servers should also have the iLO serial port configured at this time. Directions for both settings are provided below.

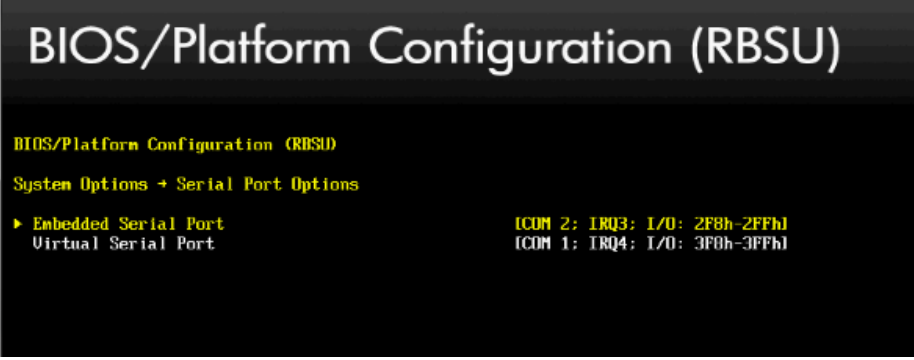
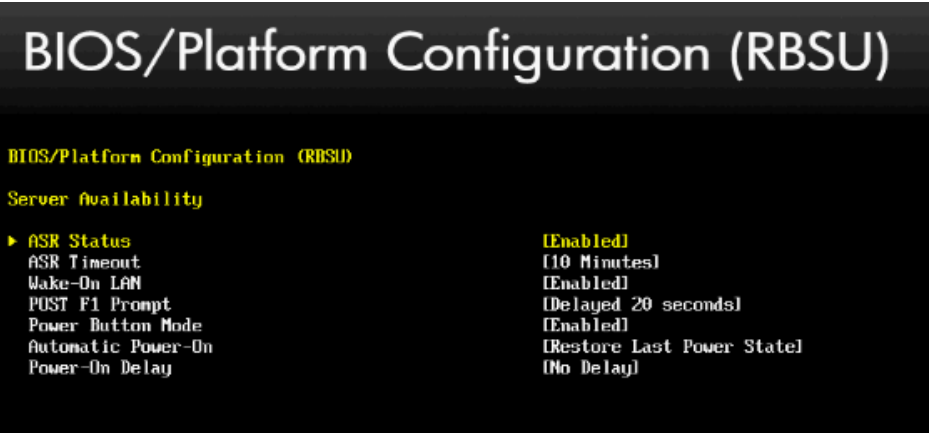
Appendix A.2.2. Configure HP Gen 9 Server BIOS Settings

S T E P #	This procedure explains the steps needed to configure HP Gen 9 server BIOS settings. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	HP Gen9 Server: Connect VGA Monitor and USB Keyboard	Connect via a VGA monitor and USB keyboard.
2 ☐	HP Gen9 Server: Reboot	Reboot the server. After the server is powered on, press the F9 key when prompted to access the System Utilities menu: Navigate to System Configuration -> BIOS/Platform Configuration (RBSU) 

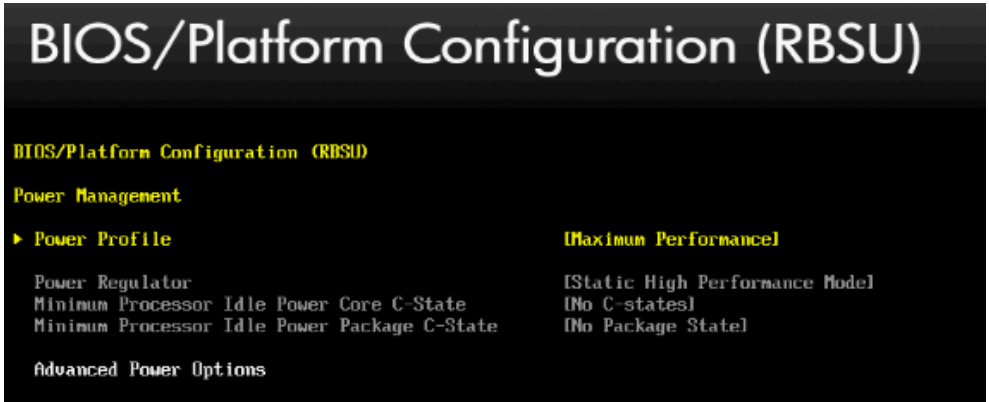
Appendix A.2.2. Configure HP Gen 9 Server BIOS Settings

3 ☐	HP Gen9 Server: Select the Date and Time	From the above screen (Step 2), navigate Date and Time Set the data and time, and time format  Press <Esc> to navigate to the main menu
4 ☐	HP Gen9 Server: System Configuration	From the above screen (Step 2) • Select the Boot Options menu • If the Boot Mode is NOT Legacy BIOS mode, press <Enter> to open the BIOS mode menu. Otherwise skip to step 5. 
5 ☐	HP Gen9 Server: System Configuration	Continued from the step 3, select Legacy BIOS Mode .
6 ☐	HP Gen9 Server: System Configuration	Press <Esc> once to back out to the BIOS/Platform Configuration (RBSU) menu.

Appendix A.2.2. Configure HP Gen 9 Server BIOS Settings

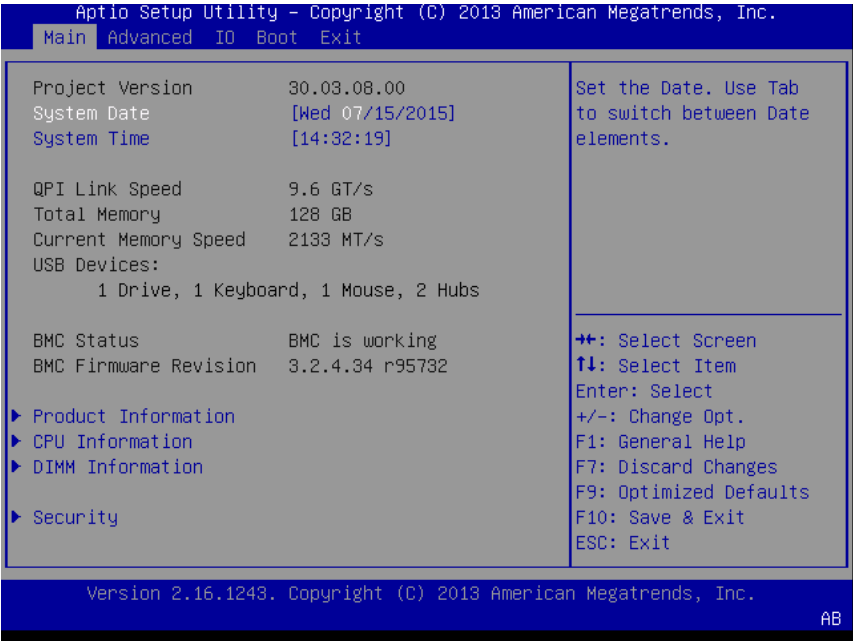
7 ☐	HP Gen9 Server: System Configuration	From the above screen (Step 2), Select the System Options menu, then select the Serial Port Options menu. • Change Embedded Serial Port to COM2 • Change Virtual Serial Port to COM1 
8 ☐	HP Gen9 Server: Exit	Press <Esc> twice to back out to the BIOS/Platform Configuration (RBSU) menu.
9 ☐	HP Gen9 Server: Server Availability	From the above screen (Step 2), Select the Server Availability menu. • Set the Automatic Power-On to Restore Last Power State • Set Power-On Delay to No Delay 
10 ☐	HP Gen9 Server: Exit	Press <Esc> twice to back out to the BIOS/Platform Configuration (RBSU) menu.

Appendix A.2.2. Configure HP Gen 9 Server BIOS Settings

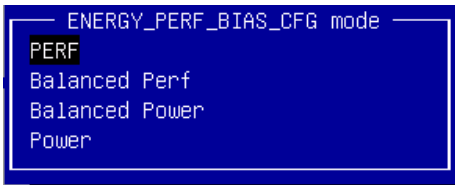
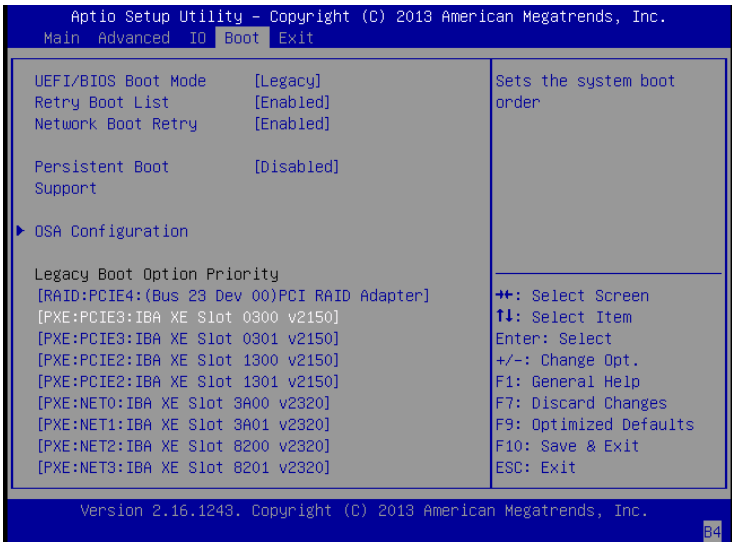
11 ☐	HP Gen9 Server: Power Management	From the above screen (Step 2), select the Power Management menu Set HP Power Profile to Maximum Performance.  Press <Esc> once to back out to the BIOS/Platform Configuration (RBSU) menu.
12 ☐	HP Gen9 Server: Save Settings and Exit	Press <F10> to save the updated settings, then <y> to confirm the settings change. Press <Esc> twice to back out to the System Utilities menu.
13 ☐	HP Gen9 Server: Reboot	Select Reboot the System and press <Enter> to confirm.

Appendix A.2.3: Configure Oracle X5-2/Netra X5-2/X6-2 Server

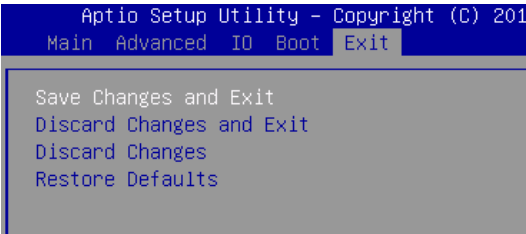
Appendix A.2.3.1. Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings

STEP #	This procedure explains the steps needed to configure Oracle rack mount server BIOS settings. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Oracle X5-2/Netra X5-2/X6-2: Access iLO GUI	Obtain access to the Oracle X5-2/Netra X5-2/X6-2 iLOM by following Appendix D.2: iLOM GUI Access (Oracle X5-2/Netra X5-2/X6-2)
2 ☐	Oracle X5-2/Netra X5-2/X6-2: Reboot	Reboot the server. After the server is powered on, press the F2 key when prompted to access the Setup Utility: 
3 ☐	Oracle X5-2/Netra X5-2/X6-2: Set Server Data and Time	From the above screen (Step 1), set the data and time:

Appendix A.2.3.1. Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings

4 ☐	Oracle X5-2/Netra X5-2/X6-2: Advanced Menu	From the above screen (Step 1) Go to the Advanced menu.  Select CPU Power Management Configuration option. If ENERGY_PERF_BIAS_CFG mode is not set to [PERF], select PERF and press Enter.  Press <ESC> to return to the advanced menu. 
5 ☐	Oracle X5-2/Netra X5-2/X6-2: Advanced Menu	Select the Boot Menu: Under Legacy Boot Option, verify the RAID Adapter is listed first. If not, highlight it and use the '+' key to move it to the top of the list: 

Appendix A.2.3.1. Configure Oracle X5-2/Netra X5-2/X6-2 Server BIOS Settings

6 ☐	Oracle X5-2/Netra X5-2/X6-2: Save Changes and Exit	Go to the Exit menu:  Select Save Changes and Exit. Confirm Yes

Appendix A.2.3.2. Enable Oracle Netra X5-2/X6-2 CPU Power Limit for NEBS (Optional)

S T E P #		This procedure explains the steps needed to configure Oracle rack mount server NEBS settings. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	Oracle Netra X5-2/X6-2: Enable CPU Power Limit after IPM	Login to the TVOE as admusr. Password: <admusr_password> <pre>\$ sudo /usr/TKLC/plat/sbin/cpuPowerLimit --enable</pre>
2 ☐	Oracle Netra X5-2/X6-2: Reboot Server	Reboot the server by executing the following command: <pre>\$ sudo init 6</pre>
3 ☐	Oracle Netra X5-2/X6-2: Check current setting	Check the current CPU Power Limit setting: <pre>\$ sudo /usr/TKLC/plat/sbin/cpuPowerLimit --status</pre>

Appendix A.2.3.3. Disable Oracle Netra X5-2/X6-2 CPU Power Limit for NEBS (Optional)

S T E P #		This procedure explains the steps needed to configure Oracle rack mount server NEBS settings. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	Oracle Netra X5-2/X6-2: Disable CPU Power Limit after IPM	Login to the TVOE as admusr. Password: <admusr_password> <pre>\$ sudo /usr/TKLC/plat/sbin/cpuPowerLimit --disable</pre>
2 ☐	Oracle Netra X5-2/X6-2: Reboot Server	Reboot the server by executing the following command: <pre>\$ sudo init 6</pre>
3 ☐	Oracle Netra X5-2/X6-2: Check current setting	Check the current CPU Power Limit setting: <pre>\$ sudo /usr/TKLC/plat/sbin/cpuPowerLimit --status</pre>

Appendix B: Upgrade Server Firmware

Appendix B.1: HP DL 380 Server

This procedure will upgrade the DL380 server firmware. All HP servers should have SNMP disabled. Refer to **Appendix C: Changing the SNMP Configuration Settings**.

The service Pack for ProLiant (SPP) installer automatically detects the firmware components available on the target server and will only upgrade those components with firmware older than what is provided by the SPP in the HP FUP version being used.

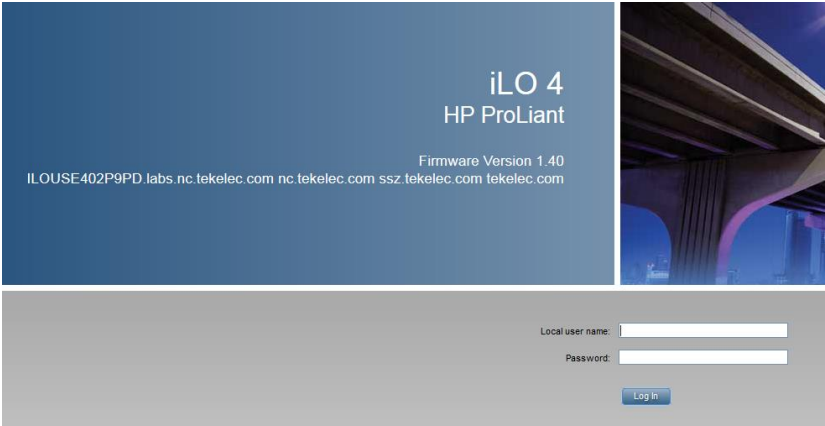
Variable	Value
<iLO_IP>	Fill in the IP address of the iLO for the server being upgraded _____
<iLO_admin_user>	Fill in the username of the iLO's Administrator user _____
<iLO_admin_password>	Fill in the password for the iLO's Administrator user _____
<local_HPSP_image_path>	Fill in the filename for the HP Support Pack for ProLiant ISO _____
<admusr_password>	Fill in the password for the admusr user for the server being upgraded _____

Needed Material:

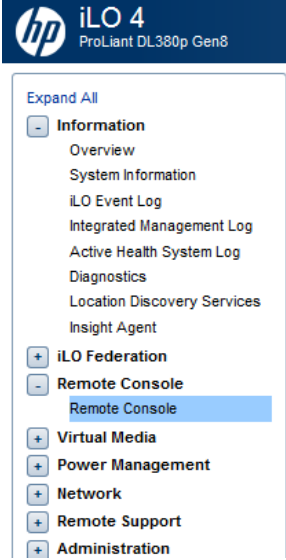
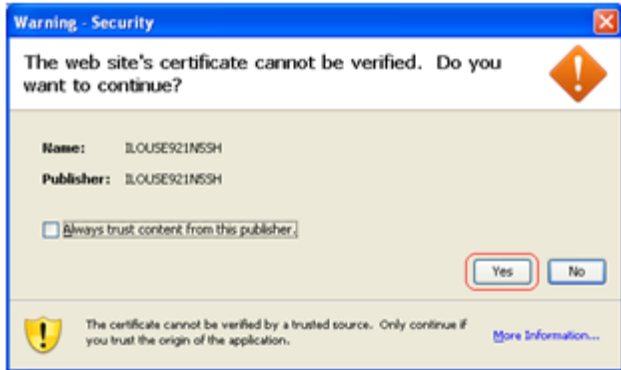
- HP Service Pack for ProLiant (SPP) firmware ISO image (min 2.2.9)
- HP MISC firmware ISO image (for errata updates if applicable)
- HP Solutions Firmware Upgrade Pack Release Notes [1]
- 4GB or larger USB stick is needed if upgrading firmware with USB media.

Note: For the "Update Firmware Errata" step check the HP Solutions Firmware Upgrade Pack Release notes [1] to see if there are any firmware errata items that apply to the server being upgraded. If there is, there will be a directory matching the errata's ID in the /errata directory of the HP MISC firmware ISO image. The errata directories contain the errata firmware and a README file detailing the installation steps.

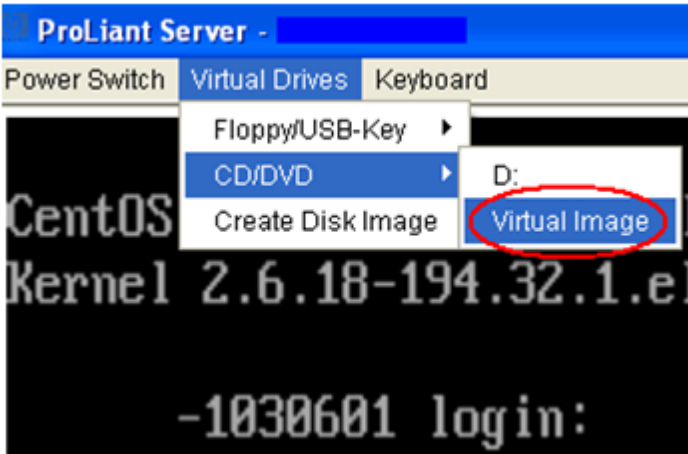
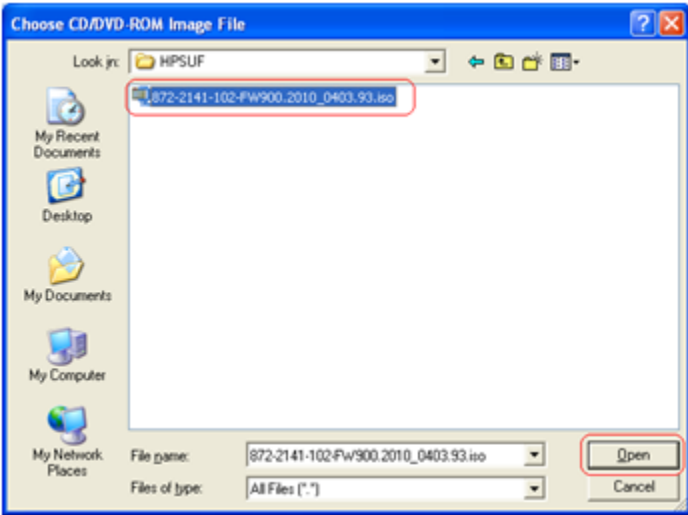
Appendix B.1.1 Upgrade HP DL380 Server Firmware

S T E P #	This procedure explains the steps needed to upgrade the HP DL380 server firmware Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Local Work Station: Insert the USB Flash Drive	Insert Update Firmware USB into a USB port of the RMS server. Refer to refer to Appendix N: Creating a Bootable USB Drive on Linux Note: There is also the option of mounting a virtual image for this process. If this option is used, skip this step.
2 ☐	Local Work Station: Login to the iLO web GUI	Access the iLO web GUI. https://<iLO_IP>/  Username = <iLO_admin_user> Password = <iLO_admin_password>

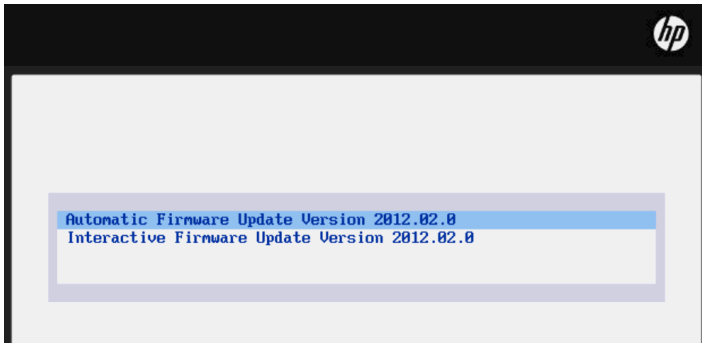
Appendix B.1.1 Upgrade HP DL380 Server Firmware

3 ☐	iLO4 Web GUI: Launch Remote Console.	Launch the Java Integrated Remote Console applet. On the menu to the left navigate to the Remote Console page. Under Java Integrated Remote Console (Java IRC), click Launch  Java Integrated Remote Console (Java IRC) The Java IRC provides remote access to the system KVM and control of Virtual Power and Media from a Java applet-based console. Java IRC requires the availability of Java. Acknowledge the security warning if presented: 

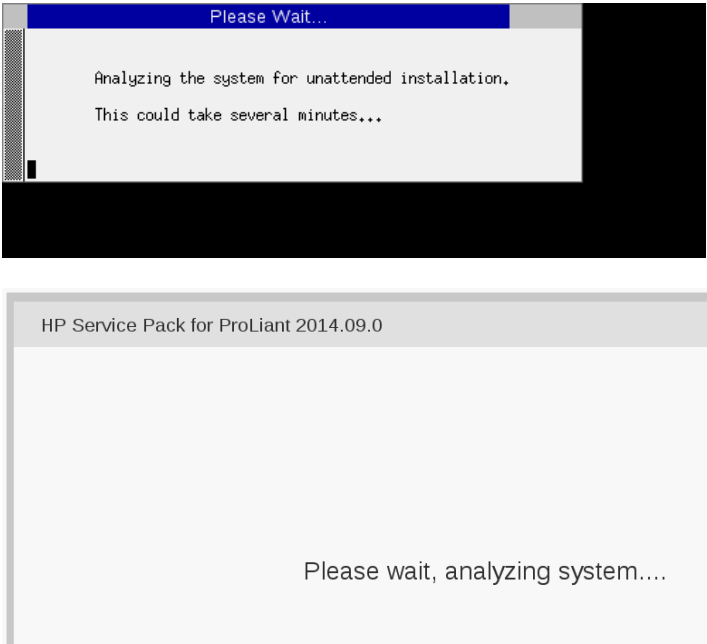
Appendix B.1.1 Upgrade HP DL380 Server Firmware

4 ☐	iLO4 Remote Console: Create Virtual Drive Connection	 If using SPP USB media plugged into the server, skip this step  Click on the Virtual Drives drop down menu. Go to CD/DVD then click on Virtual Image.  Navigate to the HP Support Pack for ProLiant ISO file copied to the workstation.  Select the ISO image file and click Open. At the bottom of the remote console window you should now see a green highlighted drive icon and VirtualIM written next to it. 

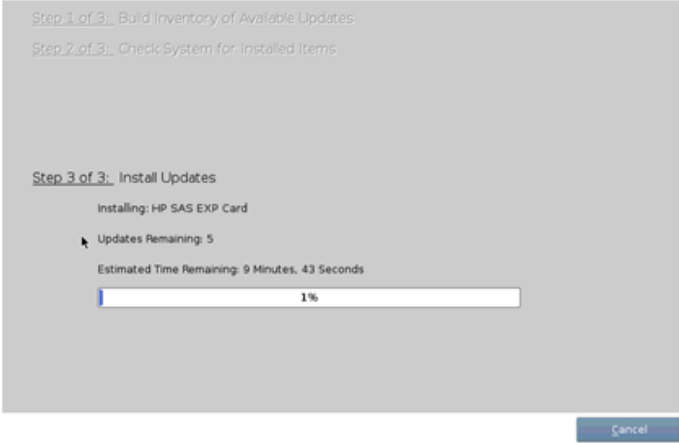
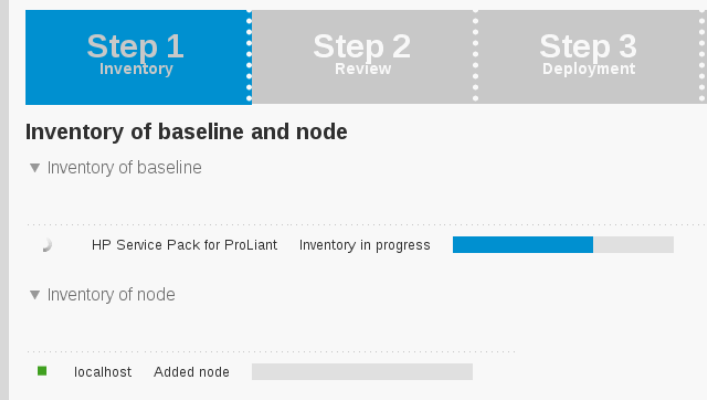
Appendix B.1.1 Upgrade HP DL380 Server Firmware

5 ☐	iLO4 Remote Console: Login	Login to the server as admusr . Password: <admusr_password>
6 ☐	iLO4 Remote Console: Reboot Server	Reboot the server by executing the following command: <pre>\$ sudo init 6</pre>
7 ☐	iLO4 Remote Console: Perform an unattended firmware upgrade.	The server will reboot into the <i>HP Support Pack for ProLiant ISO</i> and present the following boot prompt. Press [Enter] to select the Automatic Firmware Update procedure.  Note: If no key is pressed in 30 seconds the system will automatically perform an Automatic Firmware Update.

Appendix B.1.1 Upgrade HP DL380 Server Firmware

8 ☐	iLO4 Remote Console: Monitor Installation.	Important: Do not click inside the remote console during the rest of the firmware upgrade process. The firmware install will stay at the EULA acceptance screen for a short period of time. The time it takes this process to complete will vary by server and network connection speed and will take several minutes. Depending on the hardware, the following screens will be displayed:  Note: No progress indication is displayed. The installation will proceed automatically to the next step.

Appendix B.1.1 Upgrade HP DL380 Server Firmware

9 ☐	iLO4 Remote Console: Monitor Installation	Once analysis is complete, the installer will begin to upgrade inventory and deploy the eligible firmware components. A progress indicator is displayed at this time, as shown below. If iLO firmware is applied, the Remote Console will disconnect, but will continue upgrading. If the Remote Console closes due to the iLO upgrading, wait 3-5 minutes and log back in to the iLO Web GUI and re-connect to the Remote Console. The server might already be done upgrading and might have rebooted. Depending on the hardware, the following screens will be displayed:   Note: If the iLO firmware is to be upgraded, it will be upgraded last. At this point the iLO 2 session will be terminated and you will lose the remote console, virtual media and Web GUI connections to the server. This is expected and will not impact the firmware upgrade process.

Appendix B.1.1 Upgrade HP DL380 Server Firmware

10 ☐	Local Work Station: Clean Up	Once the firmware updates have been completed the server will automatically be rebooted. Closing the remote console window will disconnect the Virtual Image and you can close the iLO3/iLO4 Web GUI browser session. If you are using SPP USB media plugged into the server you can now remove it.
11 ☐	Local Work Station: Verify Server Availability	Wait 3 to 5 minutes and verify the server has rebooted and is available by gaining access to the login prompt.
12 ☐	Local Work Station: Update Firmware Errata	Refer to the ProLiant Server Firmware Errata section of [1] to determine if this HP Solutions Firmware Update Pack contains additional firmware errata updates that should be applied to the server at this time.
13 ☐	Repeat for Additional RMS Servers	Repeat this procedure for additional HP DL380 rack mount servers.

Appendix B.2: Oracle X5-2/Netra X5-2/X6-2**Needed Material:**

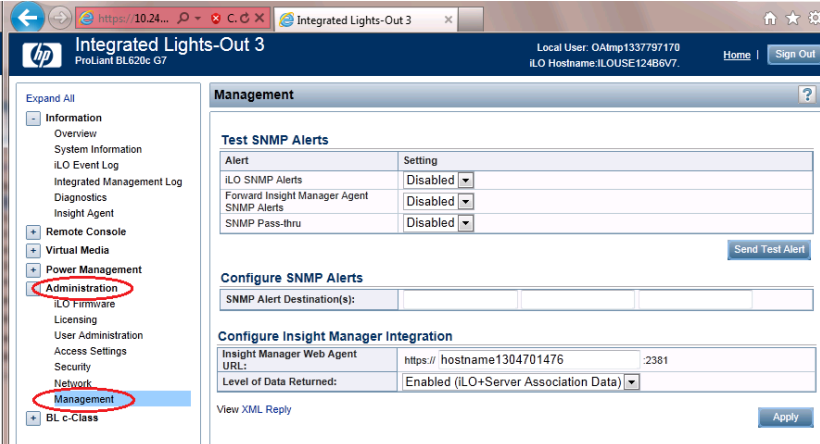
- Oracle Firmware Upgrade Pack 3.x.x
- Oracle Firmware Upgrade Pack 3.x.x Upgrade Guide

Note: The minimum supported Oracle Firmware Upgrade Pack is release 3.1.7. However, when upgrading firmware, it is recommended that the latest release be used. Refer to the Oracle Firmware Upgrade Pack Release Notes for procedures on how to obtain the firmware, and then follow the procedures in the Oracle Firmware Upgrade Pack Upgrade Guide to upgrade the firmware.

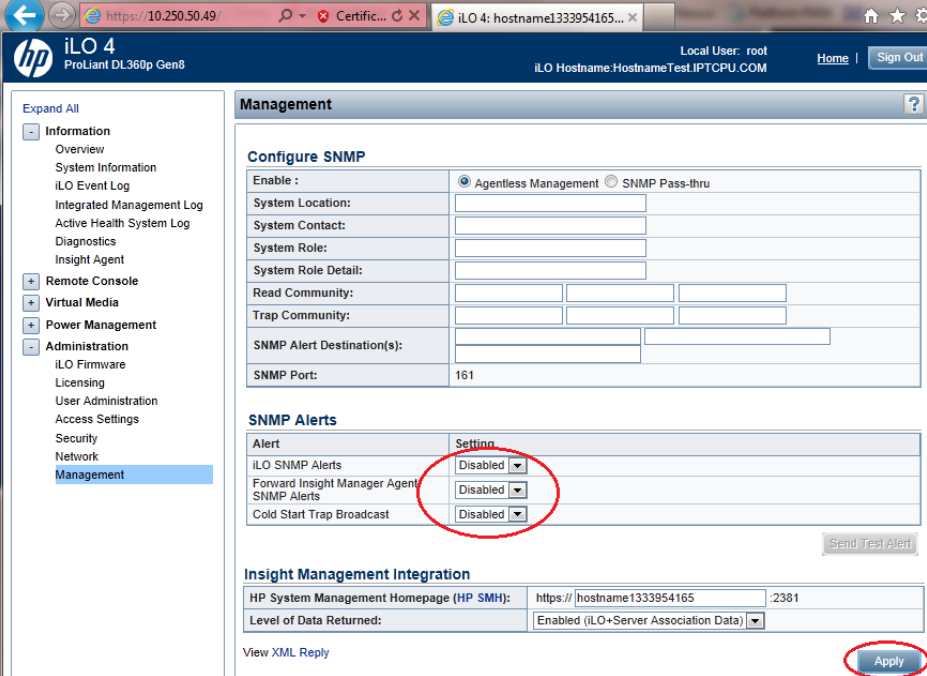
Appendix C: Changing the SNMP Configuration Settings

This procedure provides instructions to change the default SNMP settings for the HP ProLiant iLO4 devices.

Appendix C.1. Changing SNMP Configuration Settings for HP DL 380

STEP #	This procedure explains the steps needed to upgrade the HP DL380 server firmware Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Local Work Station: Login to the iLO web GUI	Access the iLO web GUI. <code>https://<iLO_IP>/</code>  Username = <iLO_admin_user> Password = <iLO_admin_password>
2 ☐	iLO4 GUI: Navigate to Management Screen	Expand the [Administration] menu item in the left hand navigation pane. Select the [Management] sub-menu item to display the Management configuration page. 

Appendix C.1. Changing SNMP Configuration Settings for HP DL 380

3 ☐	iLO4 GUI: Disable SNMP Alerts	From the above screen (Step 2): Select setting [Disabled] for each of the 3 SNMP Alerts options as shown to the right.  Click [Apply] to save the change. Note: To verify the setting changes navigate away from the Management configuration page and then go page back to it to verify the SNMP settings as shown on the right.
4 ☐	iLO4 GUI: Exit	Click [Sign Out] link in upper right corner of page to log out of the iLO GUI.
5 ☐	Repeat for Additional RMS Servers.	Repeat this procedure for additional HP DL 380 rack mount servers.

Appendix D: TVOE iLO/iLOM GUI Access

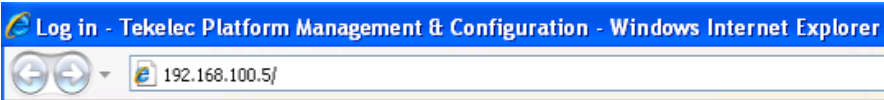
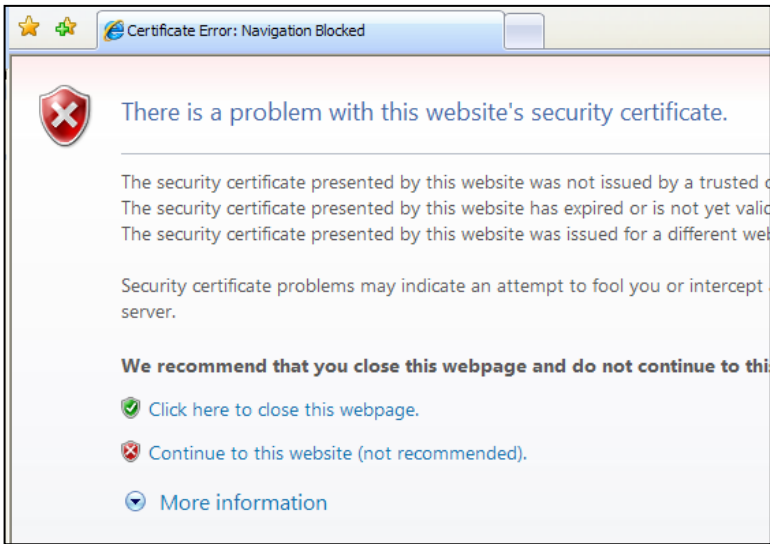
Appendix D.1: iLO GUI Access (HP DL380)

Appendix D.1. TVOE iLO4 GUI Access

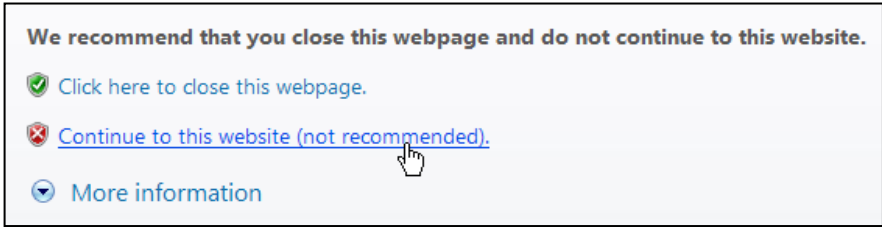
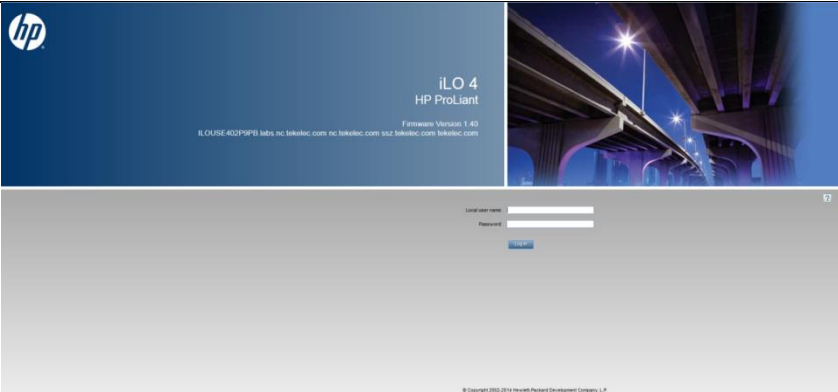
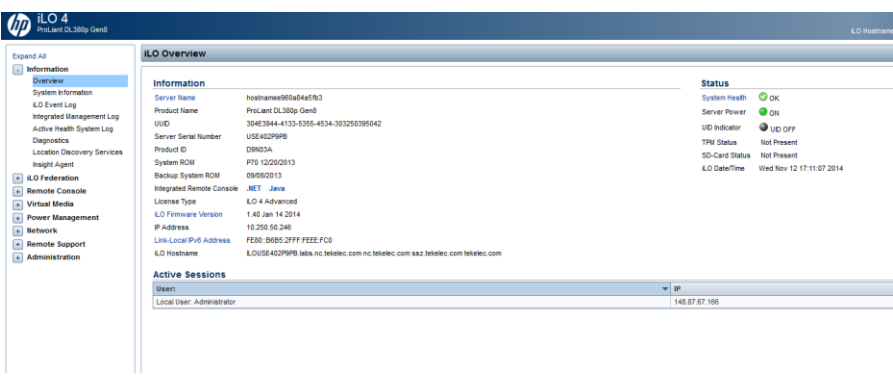
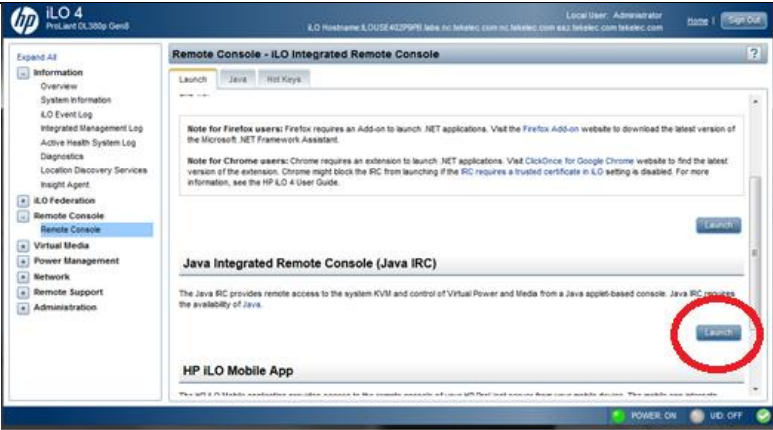
This procedure contains the steps to access the TVOE iLO4 GUI.

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

If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

STEP #	Procedure	Result
1 ☐	Launch Internet Explorer Navigate to 192.168.100.5 (manufacturing default) or customer IP set during installation.	
2 ☐	Internet Explorer may display a warning message regarding the Security Certificate.	

Appendix D.1. TVOE iLO4 GUI Access

3 ☐	Select the option to Continue to the website (not recommended)	
4 ☐	Log in to the iLO4	
5 ☐	The iLO4 Home page is displayed.	
6 ☐	Click on Launch to start the PMAC iLO4 CLI	

Appendix D.2: iLOM GUI Access (Oracle X5-2/Netra X5-2/X6-2)

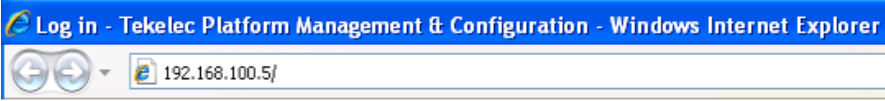
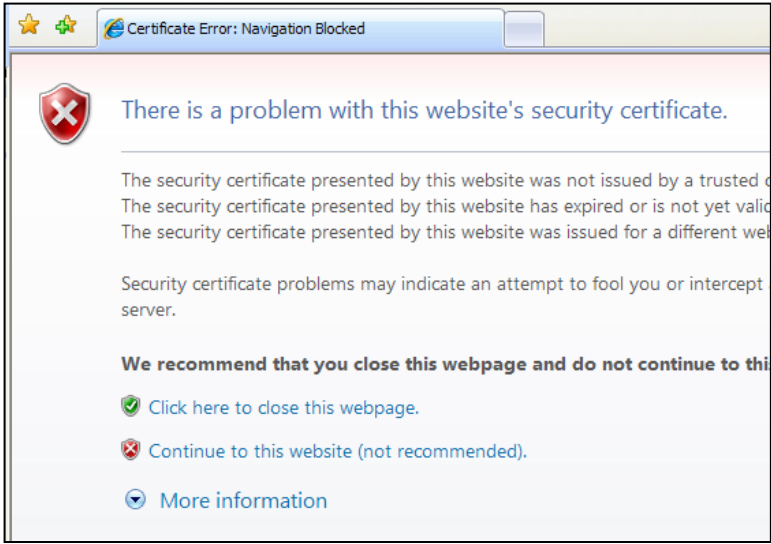
Appendix D.2. TVOE iLOM GUI Access

This procedure contains the steps to set a static IP address on the iLOM and access the TVOE iLOM GUI.

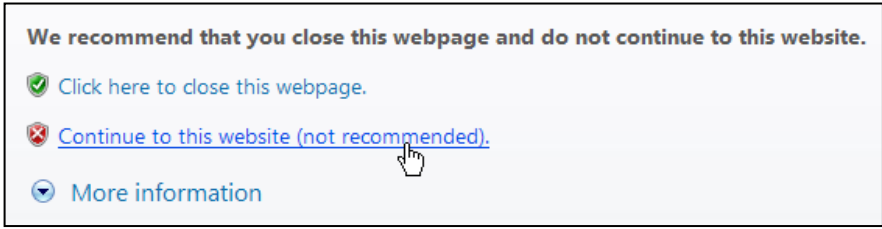
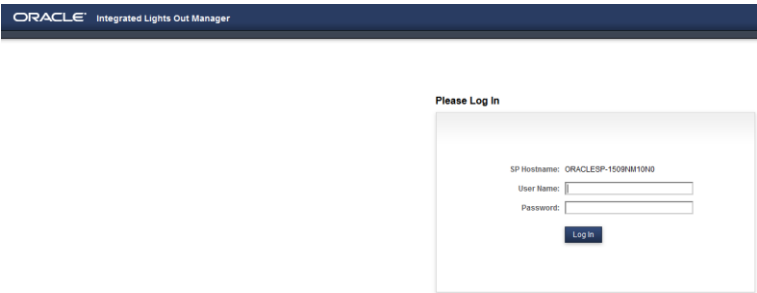
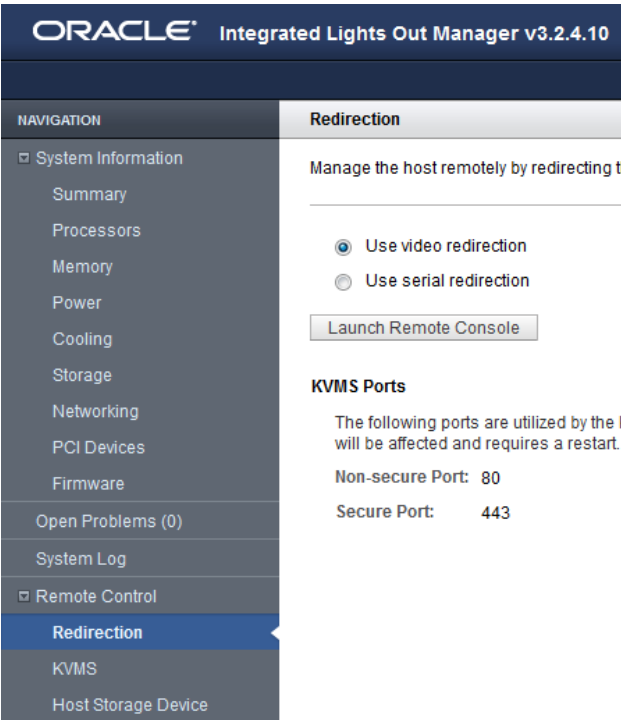
Note: These steps assume Out-of-Box State

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

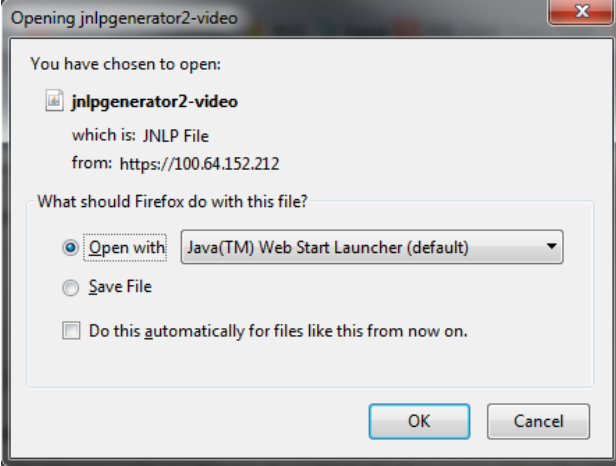
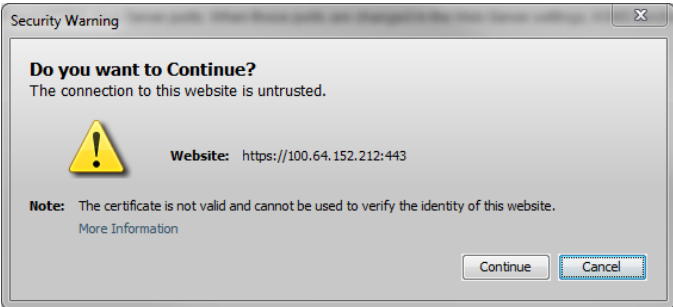
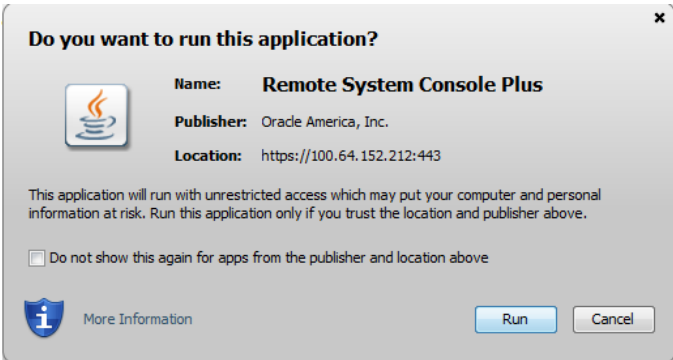
If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

STEP #	Procedure	Result
1 ☐	Launch Internet Explorer Navigate to 192.168.100.5 (manufacturing default) or customer IP set during installation.	
2 ☐	Internet Explorer may display a warning message regarding the Security Certificate.	

Appendix D.2. TVOE iLOM GUI Access

3 ☐	Select the option to Continue to the website (not recommended)	
4 ☐	Oracle X5-2/Netra X5-2/X6-2: Login	Login to the Oracle rack mount server iLOM: 
5 ☐	Oracle X5-2/Netra X5-2/X6-2: Access the Remote Console	Navigate to Remote Control -> Redirection Select Launch Remote Console 

Appendix D.2. TVOE iLOM GUI Access

6 ☐	Oracle X5-2/Netra X5-2/X6-2: Access the Remote Console	Select OK and open with Java Web Start Launcher  Select Continue and Run for any security warning prompts  

Appendix E: Changing the TVOE iLO/iLOM Address

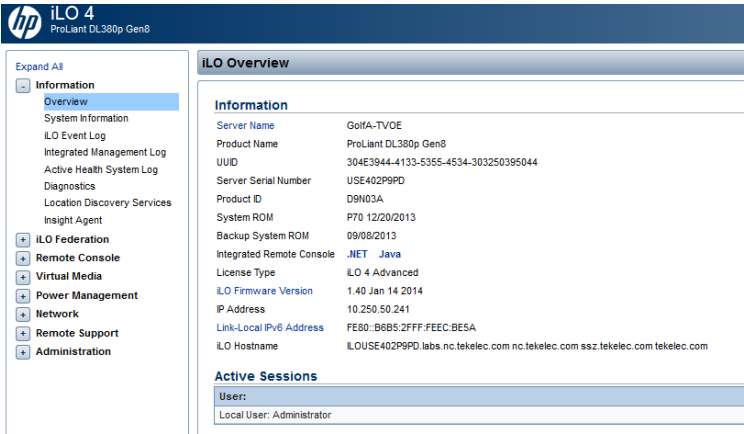
Appendix E.1: HP DL 380 Servers (iLO4)

Appendix E.1. Changing the TVOE iLO Address

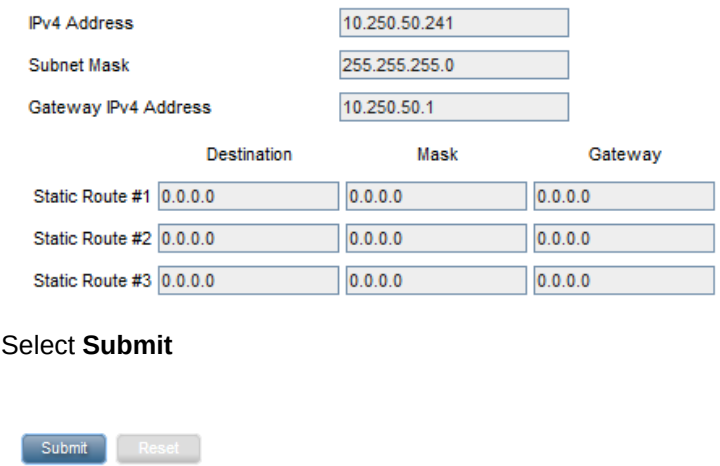
This procedure will set the IP address of the TVOE iLO4 on HP DL380 servers to the customer's network so that it can be accessed by Oracle support.

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

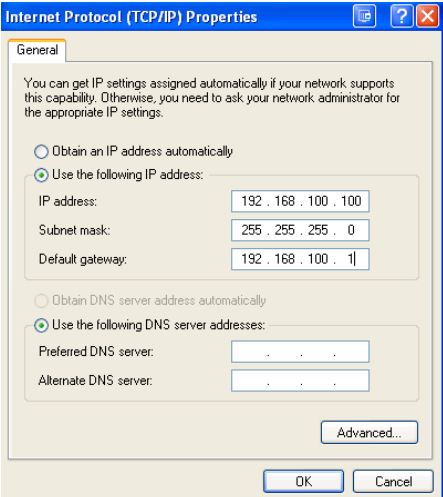
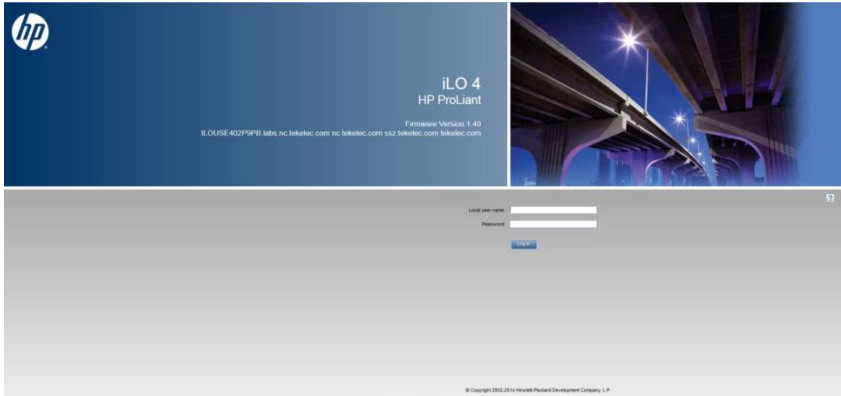
If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

STEP #	Procedure	Result
1 ☐	HP DL 380: Connect to the TVOE iLO GUI	Using the instructions in Appendix D: TVOE iLO/iLOM GUI Access, connect to the iLO4 GUI 

Appendix E.1. Changing the TVOE iLO Address

2 ☐	iLO4 GUI: Navigate to Network Menu	Navigate to Network -> iLO Dedicated Network Port  Select the tab for either IPv4 or IPv6
3 ☐	iLO4 GUI: Change IP information Subnet Mask and Gateway IP Address to the values supplied in the NAPD for the TVOE iLO. Select Apply. Note: You will lose access after you hit the Apply button.	Change the IP address, subnet Mask/prefix, and Gateway address to the values supplied in the NAPD for the TVOE iLO.  Select Submit Note: You will lose access after you hit the Submit button.

Appendix E.1. Changing the TVOE iLO Address

4 ☐	Local Machine: Reset PC's network connection.	Using the instructions found in Appendix G: Configuring for TVOE iLO Access; reset the PC's network connection replacing the Subnet Mask and Gateway with those just used for the TVOE iLO. Use an appropriate IP address for this subnet. 
5 ☐	Local Machine: Connect to the TVOE iLO GUI	Connect to the TVOE iLO GUI using the instructions in Appendix D: TVOE iLO/iLOM GUI Access Note: Use the IP address entered in Step 3 

Appendix E.2: Oracle X5-2/Netra X5-2/X6-2 Servers (Changing iLOM IP address using Keyboard/Monitor)

Appendix E.2. Changing the TVOE Oracle X5-2/Netra X5-2/X6-2 iLOM Address using keyboard/Monitor

This procedure will set the IP address of the TVOE iLOM on Oracle X5-2/Netra X5-2/X6-2 servers to the customer's network so that it can be accessed by Oracle support.

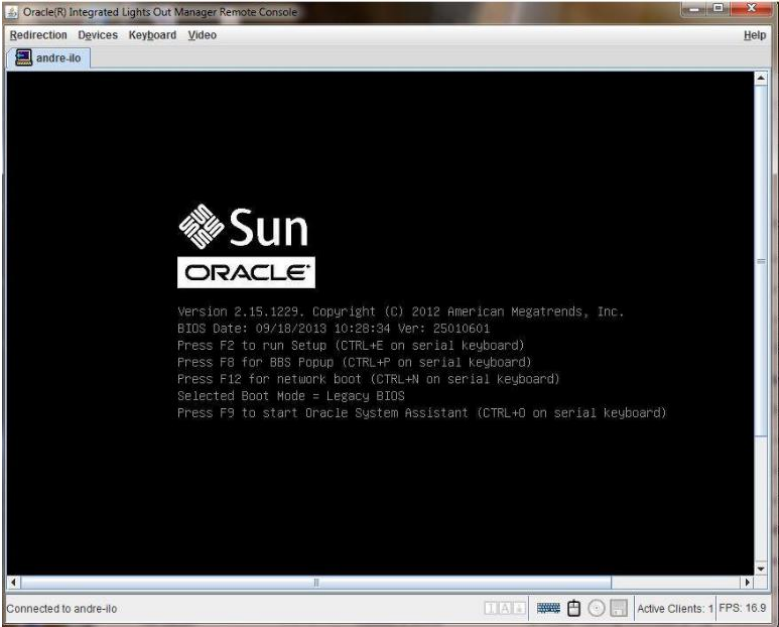
Note: By default the ILOM is configured to get its IP address Dynamically through DHCP. This procedure lists how to statically set the IP address of the ILOM using a keyboard and monitor.

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

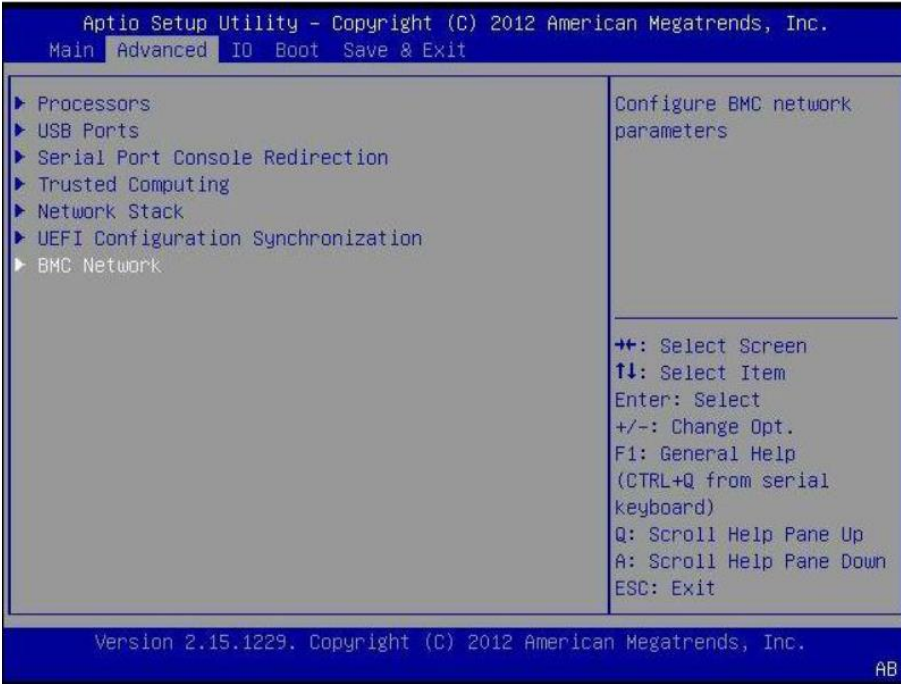
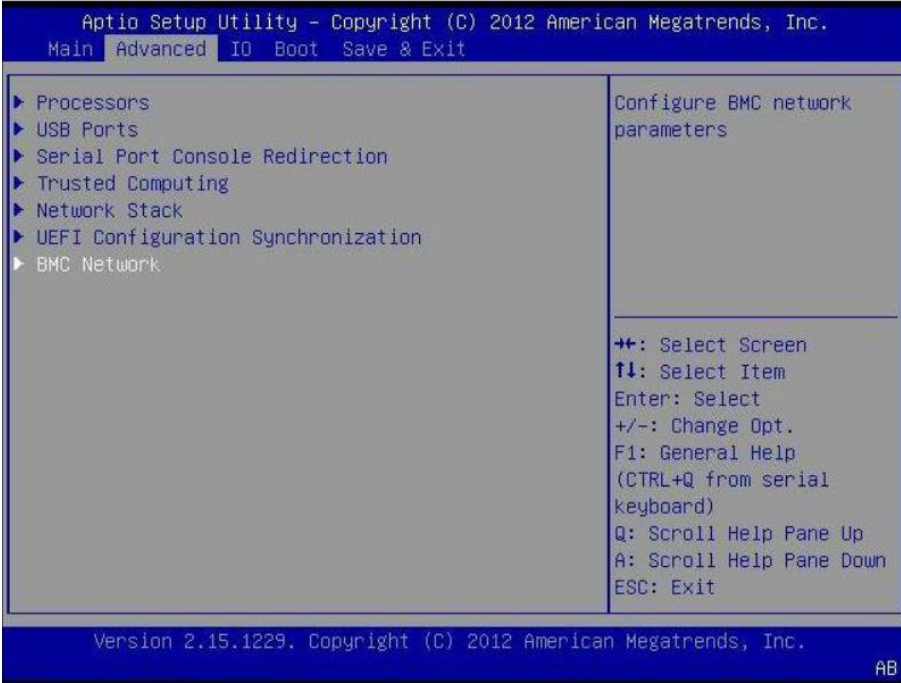
If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

STEP #	Procedure	Result

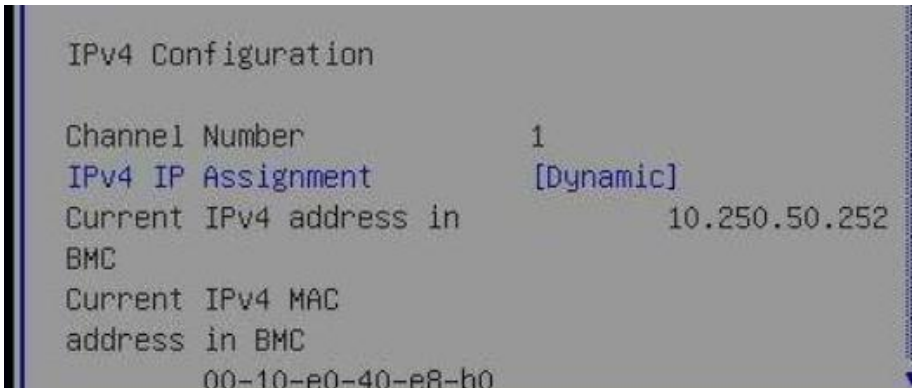
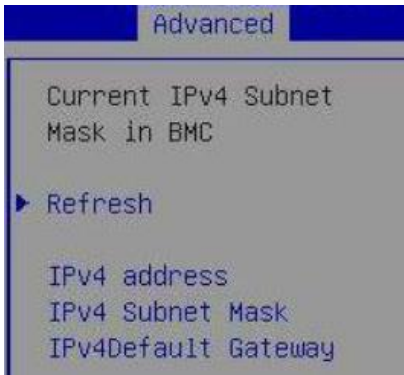
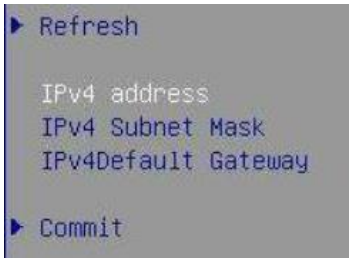
Appendix E.2. Changing the TVOE Oracle X5-2/Netra X5-2/X6-2 iLOM Address using keyboard/Monitor

1 ☐	Oracle X5-2/Netra X5-2/X6-2: Reboot and Access BIOS Configuration Menu	Reboot the Server Press F2 when prompted to enter the BIOS configuration menu:  This action will take you to the Main Menu: 

Appendix E.2. Changing the TVOE Oracle X5-2/Netra X5-2/X6-2 iLOM Address using keyboard/Monitor

2 ☐	Oracle X5-2/Netra X5-2/X6-2: Access the Configuration Menu	Use the arrow keys to navigate to the Advanced menu:  Use the arrow keys to navigate to the BMC Network menu: 

Appendix E.2. Changing the TVOE Oracle X5-2/Netra X5-2/X6-2 iLOM Address using keyboard/Monitor

3 ☐	Oracle X5-2/Netra X5-2/X6-2: Configure Static IPv4 Addresses	Setting Static IPv4 Address, IPv6 Skip this step Use the arrow keys to navigate through the menu to highlight IPv4 IP Assignment:  Press Enter Highlight Static, then press Enter Use the arrow keys to navigate down to highlight IPv4 address, press Enter  Enter the desired IPv4 address, press Enter Repeat for IPv4 Subnet Mask and IPv4 Default Gateway Select the Commit BELOW the IPv4 fields: 

Appendix E.2. Changing the TVOE Oracle X5-2/Netra X5-2/X6-2 iLOM Address using keyboard/Monitor

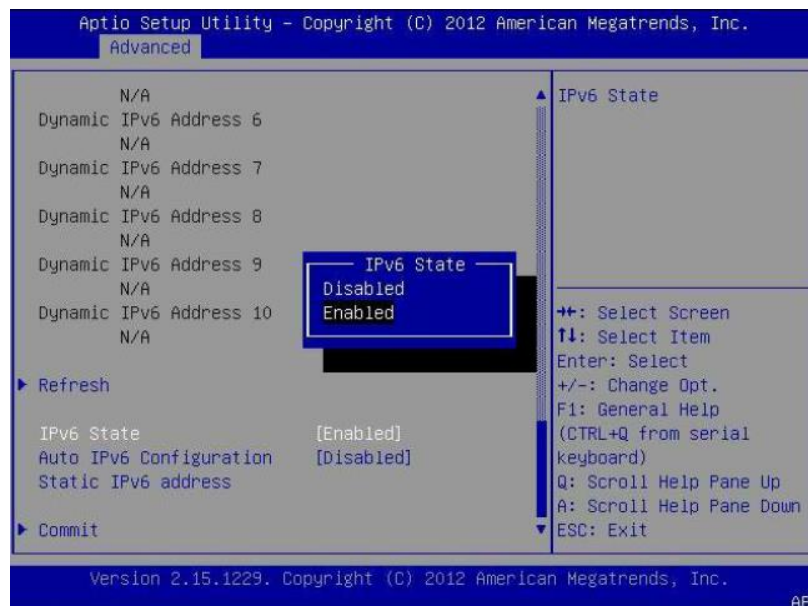
4



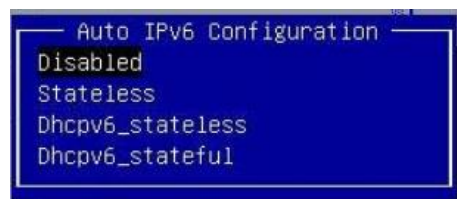
Oracle X5-2/Netra X5-2/X6-2:
Configure Static IPv6 Addresses

Setting Static IPv6 Address

Page down to the IPv6 configuration settings, set **IPv6 State** to **Enabled** and press **Enter**:



Navigate to Auto IPv6 Configuration, set **Auto IPv6 Configuration** to Disabled and press **Enter**

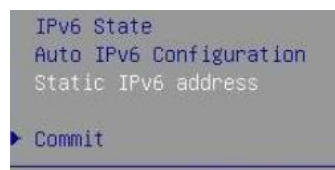


Highlight the **Static IPv6 address** option, press **Enter**

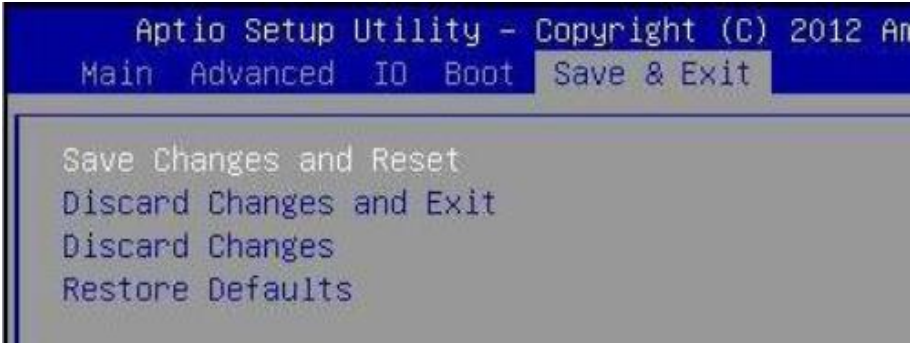
Enter the IPv6 address:



Select the **Commit** BELOW the IPv6 fields:



Appendix E.2. Changing the TVOE Oracle X5-2/Netra X5-2/X6-2 iLOM Address using keyboard/Monitor

5 ☐	Oracle X5-2/Netra X5-2/X6-2: Save and Exit	Exit the BMC Network menu by pressing the escape key Use the arrow keys to navigate through the menu and select the Save & Exit tab:  Select Save Changes and Reset When prompted, select Yes to confirm "Save configuration and reset?" The Server will reboot

Appendix E.3: Oracle X5-2/Netra X5-2/X6-2 Servers (Changing iLOM IP address using Serial Console)

Appendix E.3. Changing the TVOE Oracle X5-2/Netra X5-2/X6-2 iLOM Address using Serial Console

This procedure will set the IP address of the TVOE iLOM on Oracle X5-2/Netra X5-2/X6-2 servers to the customer's network so that it can be accessed by Oracle support.

Note: By default the iLOM is configured to get its IP address Dynamically through DHCP. This procedure lists how to statically set the IP address of the iLOM using the serial console

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

If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

STEP #	Procedure	Result												
1 	Connect to the Serial Management Port of the Oracle X5-2/Netra X5-2/X6-2 Server.	 Serial Management Port The serial management connector (labeled SER MGT) is an RJ-45 connector that can be accessed from the rear panel. This port is the default connection to the server. Use this port <i>only</i> for server management. TABLE 19 Default Serial Connections for Serial Port <table><tr><th>Parameter</th><th>Setting</th></tr><tr><td>Connector</td><td>SER MGT</td></tr><tr><td>Rate</td><td>9600 baud</td></tr><tr><td>Parity</td><td>None</td></tr><tr><td>Stop bits</td><td>1</td></tr><tr><td>Data bits</td><td>8</td></tr></table> Connect a laptop to the serial management (SER MGT) port on the server: 	Parameter	Setting	Connector	SER MGT	Rate	9600 baud	Parity	None	Stop bits	1	Data bits	8
Parameter	Setting													
Connector	SER MGT													
Rate	9600 baud													
Parity	None													
Stop bits	1													
Data bits	8													

Appendix E.3. Changing the TVOE Oracle X5-2/Netra X5-2/X6-2 iLOM Address using Serial Console

2 ☐	Login to the Serial Console	1) Press Enter on the terminal. The Oracle ILOM login prompt appears. 2) Type your Oracle ILOM user name (default user: root), and then press Enter. A password prompt appears. 3) Type the password associated with your user name, press Enter. Oracle ILOM displays the default command prompt (->), indicating that you have successfully logged in.
3 ☐	Configure NET_MGT Network Interface	1) Navigate to the /SP/network target: -> cd /SP/network 2) Ensure that the SP network interface is enabled. -> set state=enabled 3) Configure a static IPv4 address for the SP. -> set pendingipdiscovery=static pendingipaddress=<ip_address> pendingipnetmask=<netmask> pendingipgateway=<gateway> commitpending=true 4) Verify settings. -> show
4 ☐	Connect to the NET_MGT port	Connect a laptop to the network management (NET MGT) port on the server: 

Appendix F: Attaching an ISO Image to a Server using the iLO or iLOM

As an alternative to mounting the ISO image via USB, the user may also mount the ISO via the iLO or iLOM for HP and Oracle rack mount servers.

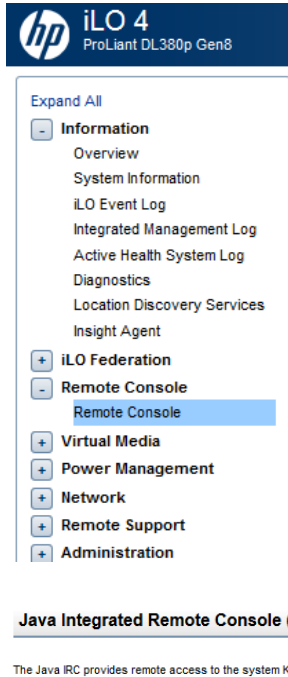
Appendix F.1: HP DL380 Servers (iLO4)

Appendix F.1.1 HP DL380 Servers Mounting the ISO image via iLO4

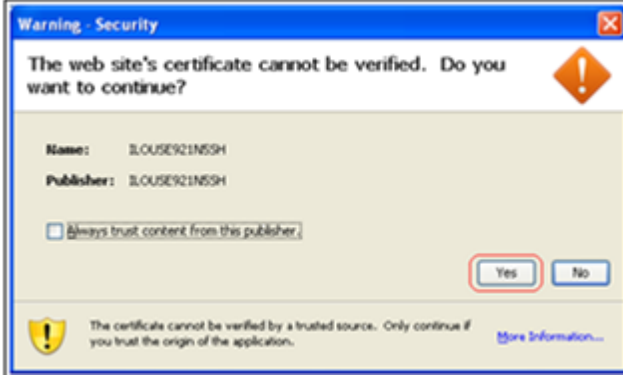
This procedure describes the steps needed to attach an ISO image to a server using the iLO4 for HP DL 380 servers.

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

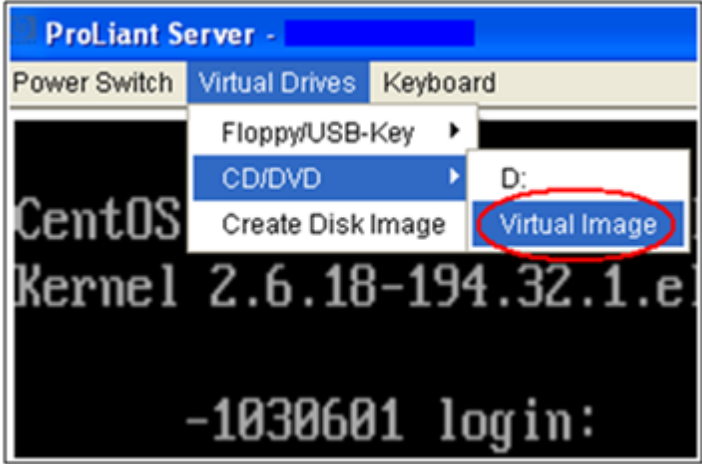
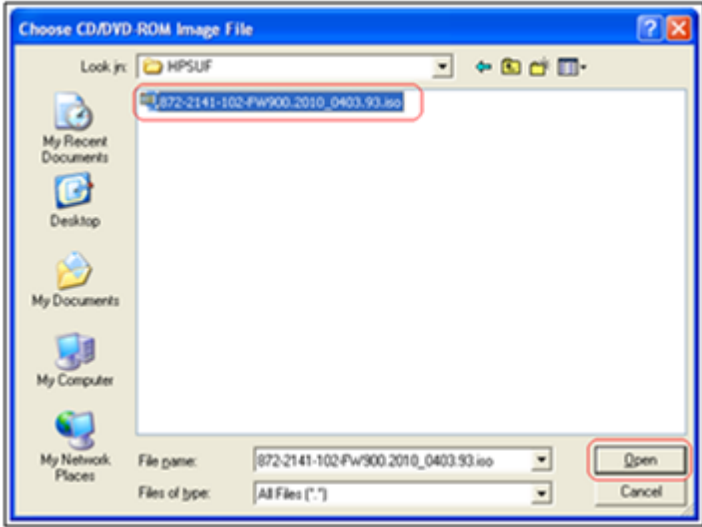
If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

STEP #	Procedure	Result
1 ☐	iLO 4 Web GUI: Launch Remote Console	Launch the Java Integrated Remote Console applet. On the menu to the left navigate to the Remote Console page. Under Java Integrated Remote Console (Java IRC), click Launch 

Appendix F.1.1 HP DL380 Servers Mounting the ISO image via iLO4

2 ☐	iLO 4 Web GUI: Java Security Prompt	Acknowledge Security Warning. If a dialog similar to the one below is presented, click Yes to acknowledge the issue and proceed  The image shows a 'Warning - Security' dialog box. The title bar is blue with a red 'X' icon. The main text says 'The web site's certificate cannot be verified. Do you want to continue?' with an orange diamond warning icon. Below this, it lists 'Name: iLOUSE921NESH' and 'Publisher: iLOUSE921NESH'. There is a checkbox labeled 'Always trust content from this publisher'. At the bottom right are 'Yes' and 'No' buttons, with the 'Yes' button circled in red. At the bottom left is a yellow shield icon with an exclamation mark, and text stating 'The certificate cannot be verified by a trusted source. Only continue if you trust the origin of the application.' with a 'More Information...' link.

Appendix F.1.1 HP DL380 Servers Mounting the ISO image via iLO4

3 ☐		Click on the Virtual Drives drop down menu. Go to CD/DVD, then click on Virtual Image  Navigate to the location of the ISO image file specified by the procedure which referenced this appendix.  Select the desired file and click Open.
4 ☐		Verify Virtual Image Connection. At the bottom of the remote console window, there should now be a green highlighted drive icon and Virtual M written next to it. 

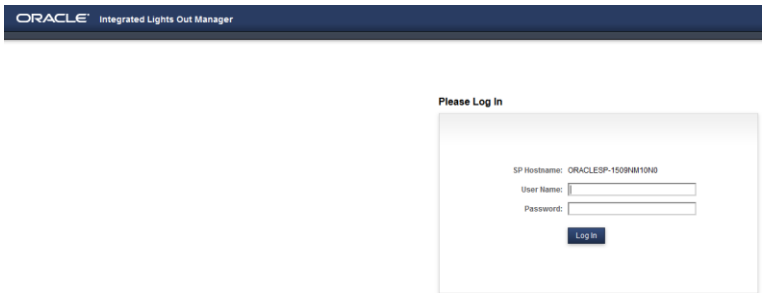
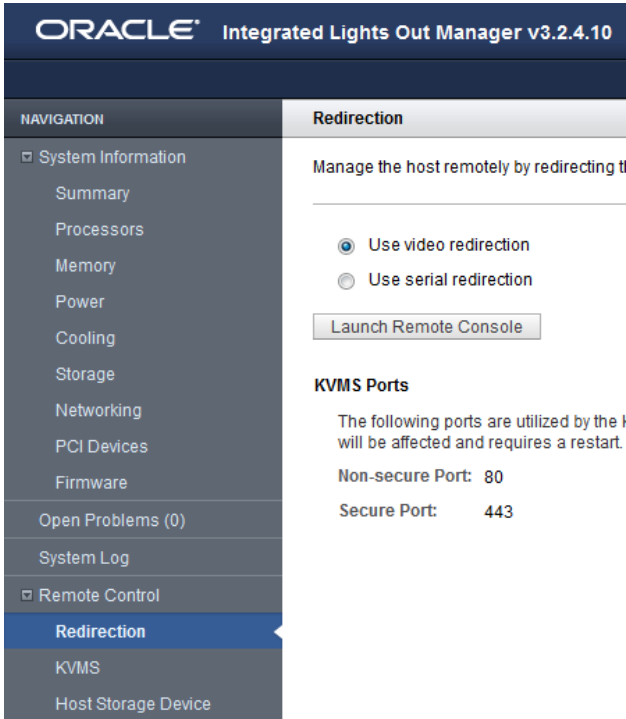
Appendix F.2: Oracle X5-2/Netra X5-2/X6-2 Servers (iLOM)

Appendix F.2.2. Oracle X5-2/Netra X5-2/X6-2 Servers Mounting the ISO image via iLOM

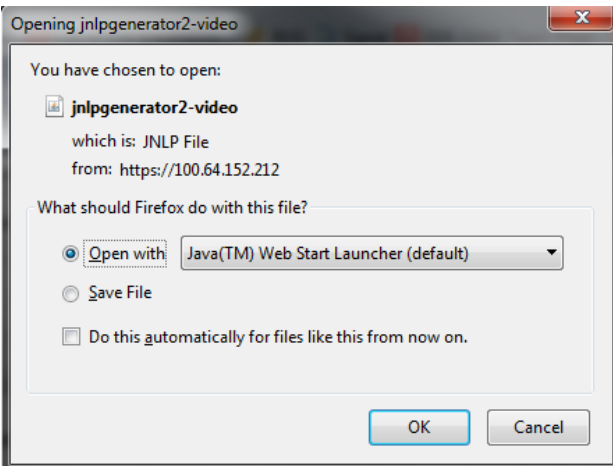
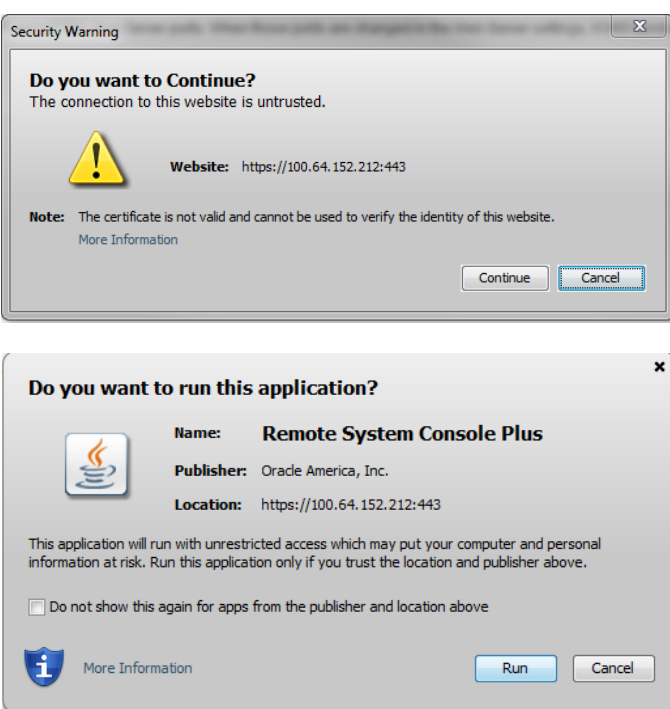
This procedure describes the steps needed to attach an ISO image to a server using the iLOM for Oracle rack mount servers.

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

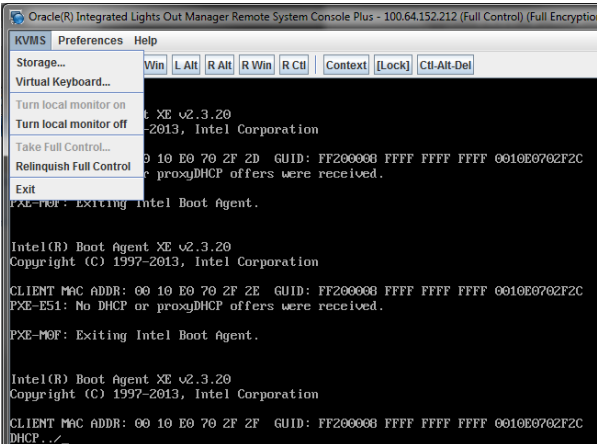
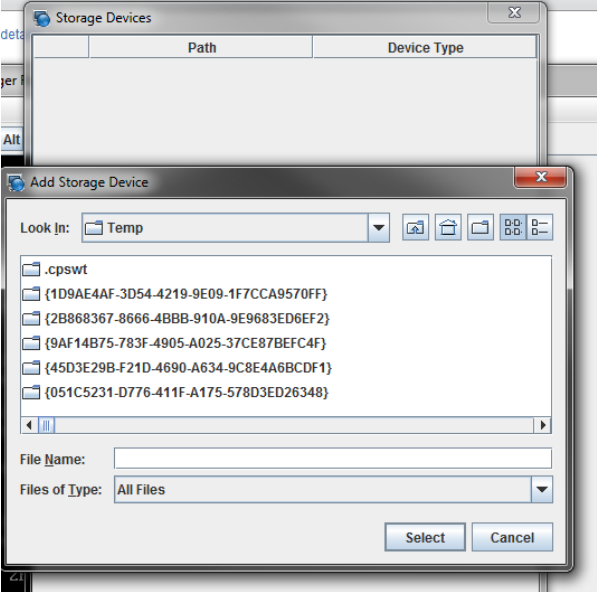
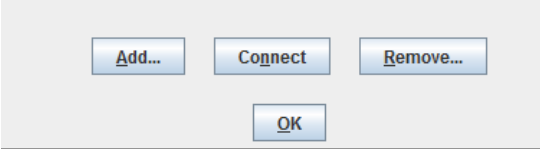
If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

STEP #	Procedure	Result
1 ☐	Oracle X5-2/Netra X5-2/X6-2: Login	Login to the Oracle rack mount server iLOM: 
2 ☐	Oracle X5-2/Netra X5-2/X6-2: Access the Remote Console	Navigate to Remote Control -> Redirection Select Launch Remote Console 

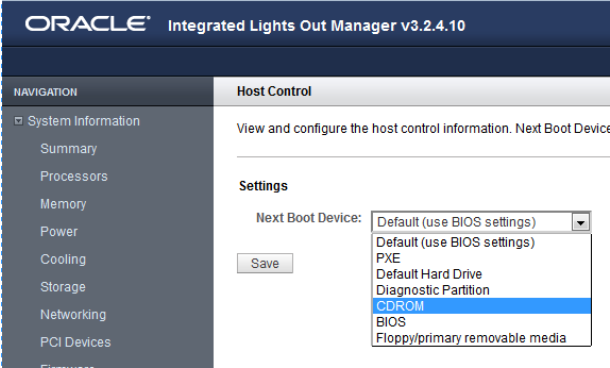
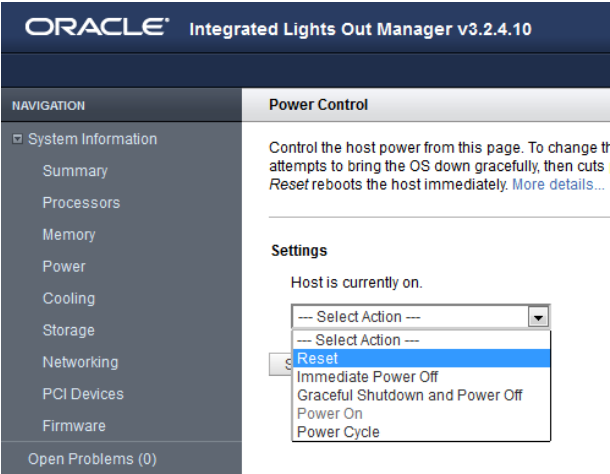
Appendix F.2.2. Oracle X5-2/Netra X5-2/X6-2 Servers Mounting the ISO image via iLOM

3 ☐	Oracle X5-2/Netra X5-2/X6-2: Access the Remote Console	Select OK and open with Java Web Start Launcher  Select Continue and Run for any security warning prompts 

Appendix F.2.2. Oracle X5-2/Netra X5-2/X6-2 Servers Mounting the ISO image via iLOM

4 ☐	Oracle X5-2/Netra X5-2/X6-2: Mount the ISO from the Remote Console	Navigate to KVMS Select Storage  Select Add, browse to the ISO located on the local machine.  Click Select Once the ISO image is selected, now select Connect 

Appendix F.2.2. Oracle X5-2/Netra X5-2/X6-2 Servers Mounting the ISO image via iLOM

5 ☐	Oracle X5-2/Netra X5-2/X6-2: Change the Device for Next Boot	Change the Next Boot Device by navigating to Host Management -> Host Control In the drop down box, select CDROM  Click Save
6 ☐	Oracle X5-2/Netra X5-2/X6-2: Power Cycle	Reboot the rack mount server to start the install by navigating to Host Management -> Power Control From the drop down box, select Reset  Click the Save button Confirm Save

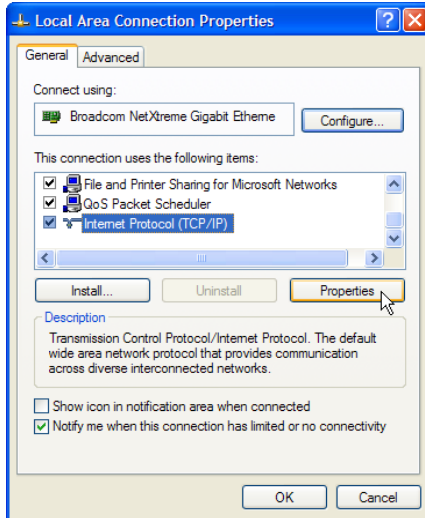
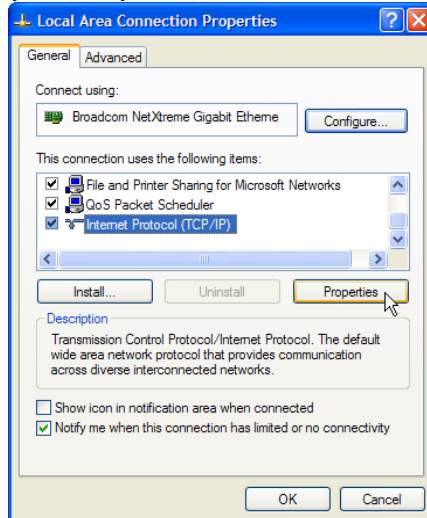
Appendix G: Configuring for TVOE iLO Access

Appendix G.1 Connecting to the TVOE iLO

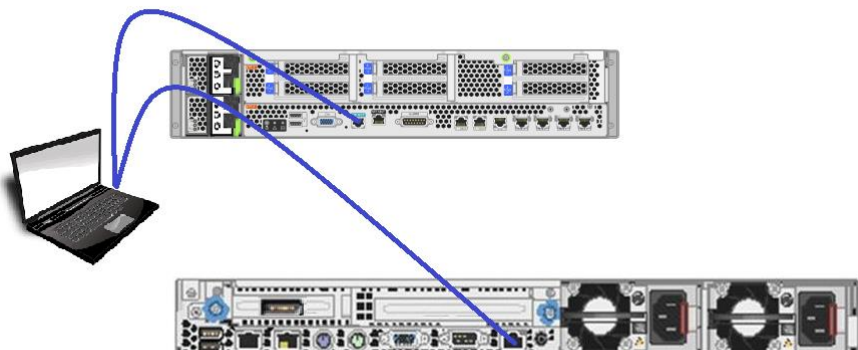
This procedure contains the steps to connect a laptop to the TVOE iLO via a directly cabled Ethernet connection.

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

If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

STEP #	Procedure	Result	
1 ☐	Access the laptop network interface cards TCP/IP Properties screen. NOTE: For this step follow the instruction specific to the laptop's OS (XP or 7).	Windows XP	Windows 7
		- Go to Control Panel - Double-click on Network Connections - Right-click the wired Ethernet Interface icon and select Properties - Select Internet Protocol (TCP/IP) Select Properties 	- Go to Control Panel. - Double-click on Network and Sharing Center - Select Change Adapter Settings (left menu) - Right-click the Local Area Connection icon and select Properties Select Internet Protocol Version 4 (TCP/IPv4) 

Appendix G.1 Connecting to the TVOE iLO

2 ☐	Click Use the following IP address Set the IP address to 192.168.100.100 Set the Subnet mask to 255.255.255.0 Set the Default gateway to 192.168.100.1 Select OK. Select Close from the network interface card's main Properties screen.	Internet Protocol (TCP/IP) Properties General You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. ☐ Obtain an IP address automatically ☒ Use the following IP address: IP address: 192 . 168 . 100 . 100 Subnet mask: 255 . 255 . 255 . 0 Default gateway: 192 . 168 . 100 . 1 ☐ Obtain DNS server address automatically ☒ Use the following DNS server addresses: Preferred DNS server: . . . Alternate DNS server: . . . Advanced... OK Cancel Local Area Connection Properties General Advanced Connect using: Broadcom NetXtreme Gigabit Ethernet Configure... This connection uses the following items: ☒ Client for Microsoft Networks ☒ Deterministic Network Enhancer ☒ Wireless Intermediate Driver ☒ File and Printer Sharing for Microsoft Networks Install... Uninstall Properties Description Allows your computer to access resources on a Microsoft network. ☐ Show icon in notification area when connected ☒ Notify me when this connection has limited or no connectivity Close Cancel
3 ☐	Connect the laptop's Ethernet port directly to the TVOE iLO port using a standard Cat-5 cross-over cable.	

Appendix H: SNMP Configuration

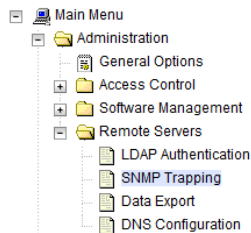
The network-wide plan for SNMP configuration should be decided upon before DSR installation proceeds. This section provides some recommendations for these decisions.

SNMP traps can originate from the following entities in a DSR installation:

- DSR Application Servers (NOAM, SOAM, MPs of all types)
- DSR Auxiliary Components (Switches, TVOE hosts, PMAC)

DSR application servers can be configured to:

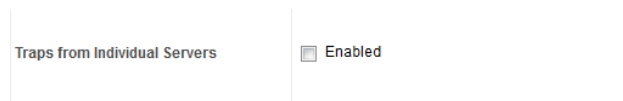
1. Send all their SNMP traps to the NOAM via merging from their local SOAM. All traps will terminate at the NOAMP and be viewable from the NOAMP GUI (entire network) and the SOAM GUI (site specific) if **only** NOAM and SOAM are configured as Manager and **Traps Enabled** checkbox is selected for these managers on **Main Menu > Administration > Remote Servers > SNMP Trapping screen**. This is the default configuration option.



2. Send all their SNMP traps to an external Network Management Station (NMS). The traps will NOT be seen at the SOAM OR at the NOAM. They will be viewable at the configured NMS(s) only if **only** external NMS is configured as Manager and **Traps Enabled** checkbox is selected for this manager on **Main Menu > Administration > Remote Servers > SNMP Trapping screen**.

Manager 1	10.10.10.10
Manager 2	
Manager 3	
Manager 4	
Manager 5	
Enabled Versions	SNMPv3 v
Traps Enabled	☒ Manager 1 ☐ Manager 2 ☐ Manager 3 ☐ Manager 4 ☐ Manager 5

3. Send SNMP traps from individual servers like MPs of all types If **Traps from Individual Servers** check box is selected on **Main Menu > Administration > Remote Servers > SNMP Trapping screen**.



Application server SNMP configuration is done from the NOAM GUI, near the end of DSR installation.

See the procedure list for details.

DSR Auxiliary components must have their SNMP trap destinations set explicitly. Trap destinations can be the NOAM VIP, the SOAM VIP, or an external (customer) NMS.

The recommended configuration is as follows:

The following components:

- PMAC (TVOE)
- PMAC (App)
- Applicable Switch types
- TVOE for DSR Servers

Should have their SNMP trap destinations set to:

1. The local SOAM VIP
2. The customer NMS, if available

Note: All the entities **MUST** use the same Community String during configuration of the NMS server.

Note: SNMP community strings i.e. (Read Only or Read Write SNMP community strings) should be same for all the components like OAM/MP servers, PMACs, TVOE and external NMS.

Appendix I: Application NetBackup Client Installation Procedures

NetBackup is a utility that allows for management of backups and recovery of remote systems. The NetBackup suite is for the purpose of supporting Disaster Recovery at the customer site. The following procedures provides instructions for installing and configuring the NetBackup client software on an application server in two different ways, first using platcfg and second using nbAutoInstall (push Configuration)

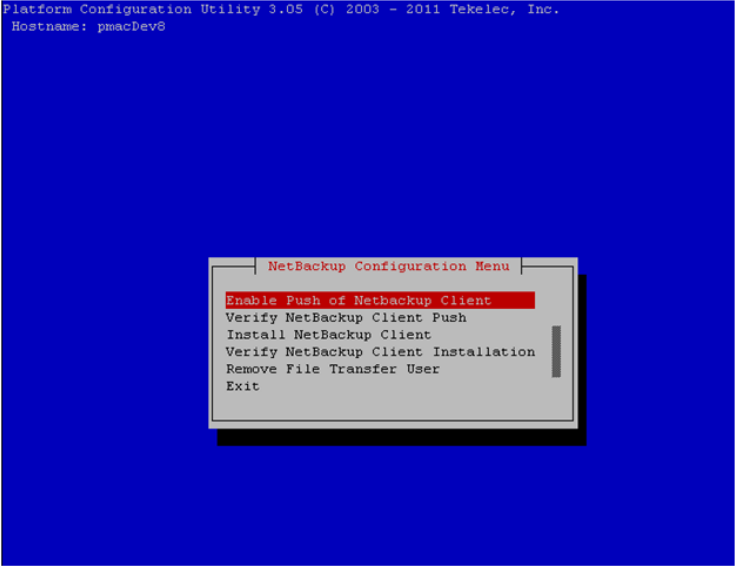
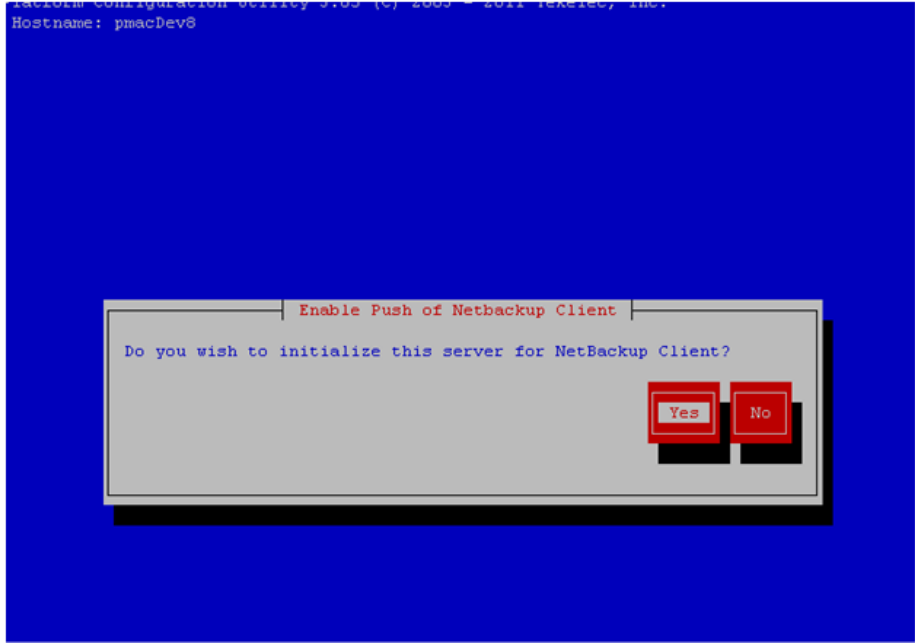
Please note that at the writing of this document, the supported versions of NetBackup are 7.1, 7.5, 7.6, and 7.7

Appendix I.1: NetBackup Client Install using PLATCFG

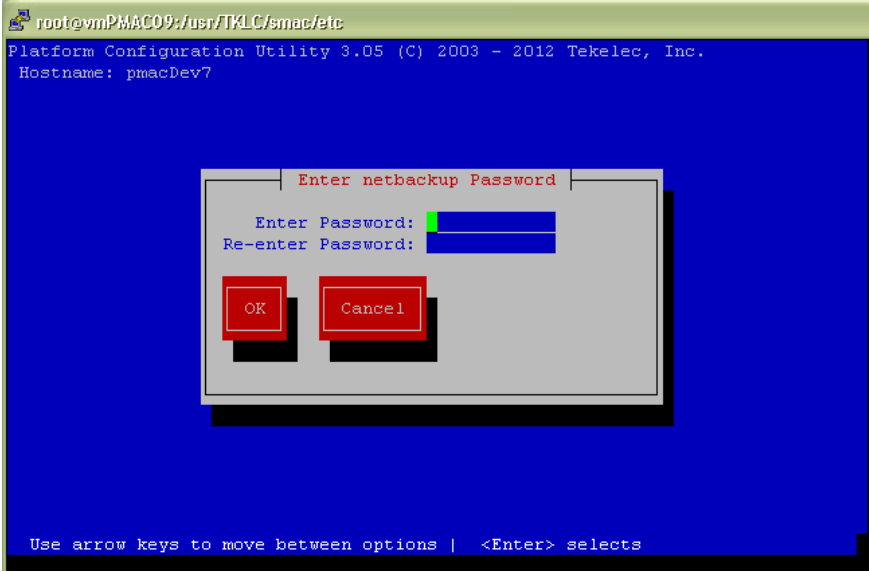
Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

S T E P #	This procedure explains the NetBackup installation using platcfg Prerequisites: • Application server platform installation has been completed. • Site survey has been performed to determine the network requirements for the application server, and interfaces have been configured. • NetBackup server is available to copy, sftp, the appropriate NetBackup Client software to the application server. Note: Execute the following procedure to switch/migrate to having NetBackup installed via platcfg instead of using NBAutoInstall (<i>Push Configuration</i>) Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Application server iLO: Login	Login and launch the integrated remote console SSH to the application Server (PMAC or NOAM) as admusr using the management network for the PMAC or XMI network for the NOAM.

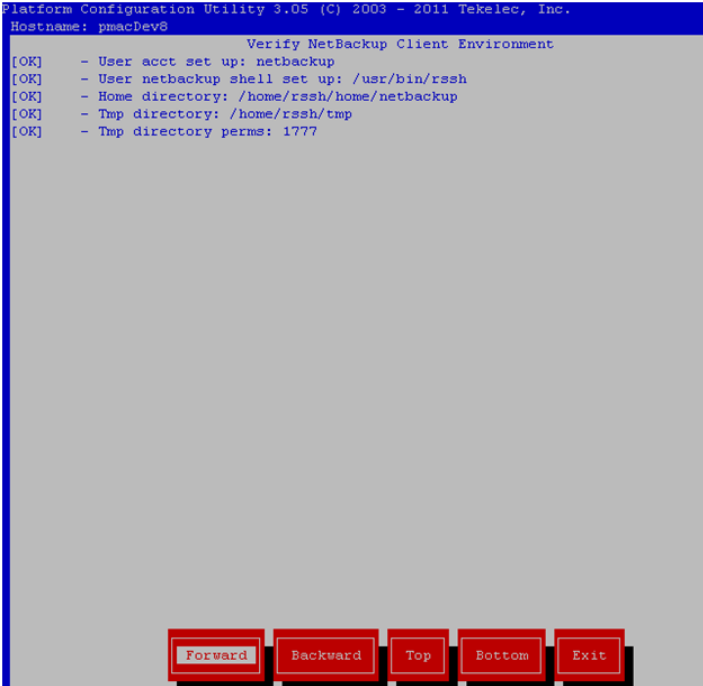
Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

2 ☐	Application server iLO: Navigate to NetBackup Configuration	Configure NetBackup Client on application server <pre>\$ sudo su - platcfg</pre> Navigate to NetBackup -> Configuration 
3 ☐	Application server iLO: Enable Push of NetBackup Client	Navigate to NetBackup Configuration -> Enable Push of NetBackup Client 

Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

4 ☐	Application server iLO: Enter NetBackup password	Enter the NetBackup password:  Select OK Note: If the version of NetBackup is 7.6.0.0 or greater, follow the instructions provided by the OSDC download for the version of NetBackup that is being pushed.

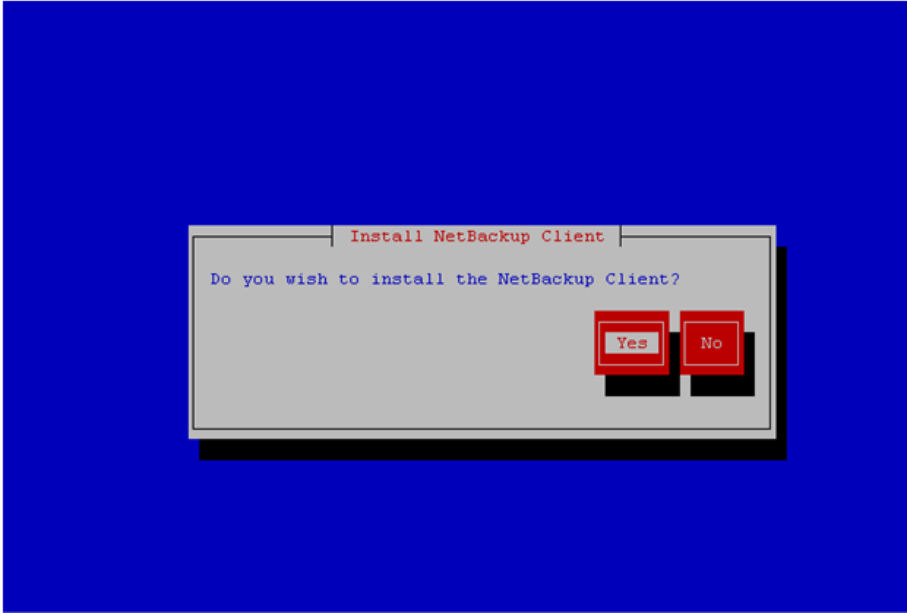
Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

5 ☐	Application server iLO: Verify NetBackup Client software push is enabled.	Navigate to NetBackup Configuration -> Verify NetBackup Client Push  Verify list entries indicate OK for NetBackup client software environment. Select Exit to return to NetBackup Configuration menu.

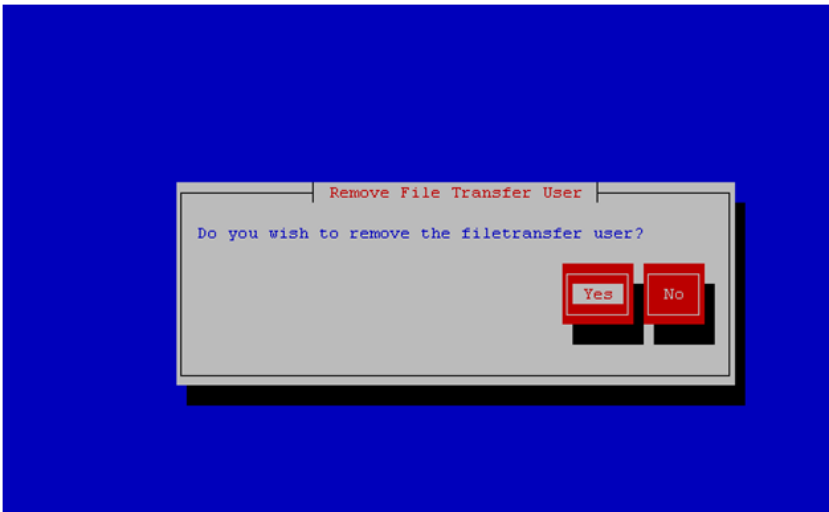
Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

[illegible]

Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

7 ☐	Application server iLO: Install NetBackup Client software on application server.	Execute the command: <pre>\$ sudo chmod 555 /var/TKLC/home/rssh/tmp/client_config</pre> Where NETBACKUP_BIN is the temporary directory where the NetBackup client install programs were copied in step 5. The directory should look similar to the following: "/tmp/bp.XXXX/" Navigate to NetBackup Configuration -> Install NetBackup Client  Verify list entries indicate OK for NetBackup client software installation Select Exit to return to NetBackup Configuration menu

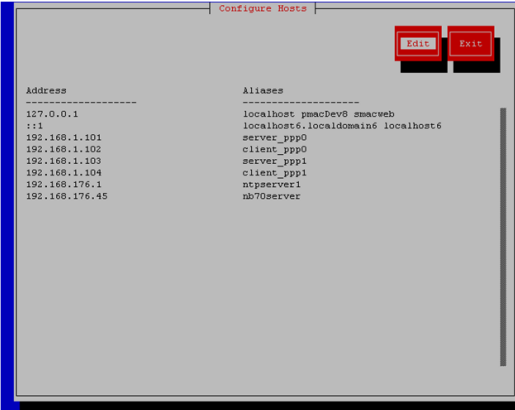
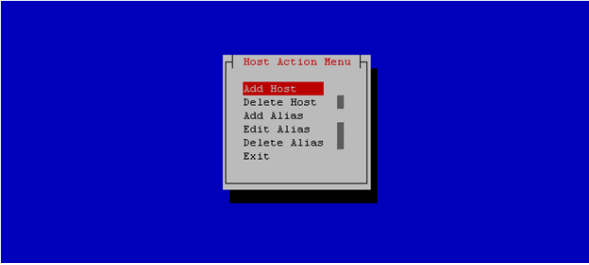
Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

8 ☐	Application server iLO: Verify NetBackup Client software installation on the application server.	Navigate to NetBackup Configuration -> Verify NetBackup Client Installation.  Verify list entries indicate OK for NetBackup Client software installation. Select Exit to return to NetBackup Configuration menu.
9 ☐	Application server iLO: Disable NetBackup Client software transfer to the application server.	Navigate to NetBackup Configuration -> Remove File Transfer User  Select Yes to remove the NetBackup file transfer user from the application server
10 ☐	Application server iLO: Exit platform configuration utility (platcfg)	Exit platform configuration utility (platcfg)

Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

11 ☐	Application server iLO: Verify Server bp.conf file	Verify that the server has been added to the <code>/usr/opensv/NetBackup/bp.conf</code> file: Issue the following command: <pre>\$ sudo cat /usr/opensv/NetBackup/bp.conf CLIENT_NAME = 10.240.34.10 SERVER = NB71server</pre>

Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

12 □	Application server iLO: Use platform configuration utility (platcfg) to modify hosts file with NetBackup server alias.	Note: After the successful transfer and installation of the NetBackup client software the NetBackup servers hostname can be found in the NetBackup "/usr/opensv/NetBackup/bp.conf" file, identified by the SERVER configuration parameter. The NetBackup server hostname and IP address must be added to the application server's host's file. List NetBackup servers hostname: <pre>\$ sudo cat /usr/opensv/NetBackup/bp.conf SERVER = nb70server CLIENT_NAME = pmacDev8</pre> Use platform configuration utility (platcfg) to update application hosts file with NetBackup Server alias. <pre>\$ sudo su - platcfg</pre> Navigate to Network Configuration -> Modify Hosts File  Select Edit, the Host Action Menu will be displayed.  Select Add Host, and enter the appropriate data  Select OK, confirm the host alias add, and exit Platform Configuration Utility

Appendix I.1. Application NetBackup Client Installation (Using Platcfg)

13 □	Application server iLO: Create links to NetBackup client notify scripts on application server where NetBackup expects to find them.	Copy the notify scripts from appropriate path on application server for given application: <pre>\$ sudo ln -s <path>/bpstart_notify /usr/openv/NetBackup/bin/bpstart_notify \$ sudo ln -s <path>/bpend_notify /usr/openv/NetBackup/bin/bpend_notify</pre> An example of <path> is "/usr/TKLC/appworks/sbin"

Appendix I.2: NETBACKUP CLIENT INSTALL/UPGRADE WITH NBAUTOINSTALL

Note: Execute the following procedure to switch/migrate to having NetBackup installed via NBAutoInstall (*Push Configuration*) instead of manual installation using platcfg

Note: Executing this procedure will enable TPD to automatically detect when a NetBackup Client is installed and then complete TPD related tasks that are needed for effective NetBackup Client operation. With this procedure, the NetBackup Client install (pushing the client and performing the install) is the responsibility of the customer and is not covered in this procedure.

Appendix I.2. Application NetBackup Client Installation (NBAUTOINSTALL)

S T E P #	This procedure explains the NetBackup installation with NBAUTOINSTALL Prerequisites: • Application server platform installation has been completed. • Site survey has been performed to determine the network requirements for the application server, and interfaces have been configured. • NetBackup server is available to copy, sftp, the appropriate NetBackup Client software to the application server. Note: If the customer does not have a way to push and install NetBackup Client, then use NetBackup Client Install/Upgrade with platcfg. Note: It is required that this procedure is executed before the customer does the NetBackup Client install. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	Application server iLO: Login Login and launch the integrated remote console. SSH to the application Server (PMAC or NOAM) as admusr using the management network for the PMAC or XMI network for the NOAM.
2 ☐	Application server iLO: Enable nbAutoInstall Execute the following command: <pre>\$ sudo /usr/TKLC/plat/bin/nbAutoInstall --enable</pre>
3 ☐	Application server iLO: Create links to NetBackup client notify scripts on application server where NetBackup expects to find them. Execute the following commands <pre>\$ sudo mkdir -p /usr/openv/NetBackup/bin/ \$ sudo ln -s <path>/bpstart_notify /usr/openv/NetBackup/bin/bpstart_notify \$ sudo ln -s <path>/bpend_notify /usr/openv/NetBackup/bin/bpend_notify</pre> Note: An example of <path> is "/usr/TKLC/plat/sbin"

Appendix I.2. Application NetBackup Client Installation (NBAUTOINSTALL)

4 □	Application server iLO: Verify NetBackup configuration file	Open /usr/opensv/NetBackup/bp.conf and make sure it points to the NetBackup Server using the following command: <pre>\$ sudo vi /usr/opensv/NetBackup/bp.conf</pre> <pre>SERVER = nb75server CLIENT_NAME = 10.240.10.185 CONNECT_OPTIONS = localhost 1 0 2</pre> Note: Verify that the above server name matches the NetBackup Server, and verify that the CLIENT_NAME matches the hostname or IP of the local client machine, if they do not, update them as necessary. Edit /etc/hosts using the following command and add the NetBackup server: <pre>\$ sudo vi /etc/hosts</pre> <pre>e.g.: 192.168.176.45 nb75server</pre> Note: The server will now periodically check to see if a new version of NetBackup Client has been installed and will perform necessary TPD configuration accordingly. At any time, the customer may now push and install a new version of NetBackup Client.

Appendix I.3: Create NetBackup Client Config File

This procedure will copy a NetBackup Client config file into the appropriate location on the TPD based application server. This config file will allow a customer to install previously unsupported versions of NetBackup Client by providing necessary information to TPD.

Appendix I.3. Create NetBackup Client Config File

S T E P #	This procedure will copy a NetBackup Client config file into the appropriate location on the TPD based application server. This config file will allow a customer to install previously unsupported versions of NetBackup Client by providing necessary information to TPD. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Application server iLO: Create NetBackup Config File	Create the NetBackup Client config file on the server using the contents that were previously determined. The config file should be placed in the <i>/usr/TKLC/plat/etc/NetBackup/profiles</i> directory and should follow the following naming conventions: NB\$ver.conf Where \$ver is the client version number with the periods removed. For the 7.5 client the value of \$ver would be 75 and the full path to the file would be: <i>/usr/TKLC/plat/etc/NetBackup/profiles/NB75.conf</i> Note: The config files must start with "NB" and must have a suffix of ".conf". The server is now capable of installing the corresponding NetBackup Client. The server is now capable of installing the corresponding NetBackup Client.
2 ☐	Application server iLO: Create NetBackup Config script	Create the NetBackup Client config script file on the server using the contents that were previously determined. The config script file should be placed in the <i>/usr/TKLC/plat/etc/NetBackup/scripts</i> directory. The name of the NetBackup Client config script file should be determined from the contents of the NetBackup Client config file. As an example for the NetBackup 7.5 client the following is applicable: <u>NetBackup Client config:</u> <i>/usr/TKLC/plat/etc/NetBackup/profiles/NB75.conf</i> <u>NetBackup Client config script:</u> <i>/usr/TKLC/plat/etc/NetBackup/scripts/NB75</i>

Appendix I.4: Configure PMAC Application NetBackup Virtual Disk

Appendix I.4. Configure the PMAC Application Guest NetBackup Virtual Disk

S T E P #	This procedure will configure the PMAC application guest NetBackup Virtual Disk. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1	PMAC GUI: Login Open web browser and navigate to the PMAC GUI, Login as Guiadmin user: https://<pmac_network_ip> 

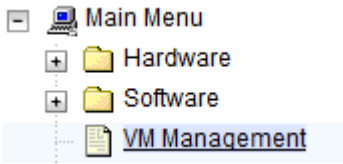
Appendix I.4. Configure the PMAC Application Guest NetBackup Virtual Disk

2

PMAC GUI:

Create NetBackup Virtual Disk

Navigate to **Main Menu -> VM Management**



Edit the PMAC application guest to add the "NetBackup" virtual disk.
Click "Edit" and enter the following data for the new NetBackup virtual disk.

- Size (MB): "2048"
- Host Pool: "vgguests"
- Host Vol Name: "<pmacGuestName>_NetBackup.img"
- Guest Dev Name: "NetBackup"

Edit guest 5010441PMAC

VM Info Software Network Media

Summary Virtual Disks Virtual NICs

Virtual Disks						Add	Delete
Primary	Size (MB)	Host Pool	Host Vol Name	Guest Dev Name			
YES	51200	vgguests	5010441PMAC.img	PRIMARY	...		
NO	10240	vgguests	5010441PMAC_logs.i mg	logs	...		
NO	61440	vgguests	5010441PMAC_imag es.img	images	...		
NO	20480	vgguests	5010441PMAC_isoim ages.img	isoimages	...		
NO	2048	vgguests	NetBackup.img	NetBackup			

Click **Save** to continue.

Save

Cancel

A confirmation dialog will be presented with the message, "Changes to the PMAC guest :<pmacGuestName> will not take effect until after the next power cycle. Do you wish to continue?"

Changes to the PMAC guest 5010441PMAC will not take effect until after the next power cycle.
Do you wish to continue?

OK

Cancel

Click **OK**

Appendix I.4. Configure the PMAC Application Guest NetBackup Virtual Disk

3

PMAC GUI:

Verify

NetBackup

Virtual Disk

Confirm the Edit VM Guest task has completed successfully.

Navigate to **Main Menu -> Task Monitoring**

The screenshot shows a vertical menu with five items: 'Status and Manage' (folder icon), 'Task Monitoring' (document icon, highlighted with a blue selection bar), 'Help' (purple cube icon), 'Legal Notices' (document icon), and 'Logout' (document icon with a speech bubble).

Confirm that the guest edit task has completed successfully.

Main Menu: Task Monitoring

Filter* ▼

	ID	Task	Target	Status
	1459	Edit Guest	RMS: pc5010441 Guest: 5010441PMAC	Guest editing completed (5010441PMAC)

Appendix I.4. Configure the PMAC Application Guest NetBackup Virtual Disk

4 **PMAC GUI:**
Verify “In-Progress” tasks

Navigate to **Main Menu -> Task Monitoring**

If any tasks show as in-progress (blue) then wait for the task to complete prior to going to the next step.

	1455	Backup PM&C		PM&C Backup successful	COMPLETE	N/A	0:00:15	2016-08-10 05:00:02
	1454	Run Script	RMS: pc5010439	Script execution success	COMPLETE		0:00:12	2016-08-09 16:47:03
	1453	File Transfer	RMS: pc5010439	File transfer success	COMPLETE		0:00:03	2016-08-09 16:46:47
	1452	Accept	RMS: pc5010439 Guest: Zombie_SDSQSVR1	Success	COMPLETE	N/A	0:01:04	2016-08-09 16:45:30
	1451	Upgrade	RMS: pc5010439 Guest: Zombie_SDSQSVR1	Success	COMPLETE		0:07:22	2016-08-09 16:36:53
	1450	Accept	RMS: pc5010441 Guest: Zombie_DSRQOAM1	Success	COMPLETE	N/A	0:01:07	2016-08-09 16:22:28
	1449	Accept	RMS: pc5010441 Guest: Zombie_DSRNOAM1	Success	COMPLETE	N/A	0:01:07	2016-08-09 16:22:28
	1448	Accept	RMS: pc5010441 Guest: ZombieDR_DSRDRNOAM1	Success	COMPLETE	N/A	0:01:09	2016-08-09 16:22:27
	1447	Accept	RMS: pc5010441 Guest: 5010441PMAC	Success	COMPLETE	N/A	0:01:07	2016-08-09 16:22:27
	1446	Accept	RMS: pc5010441	Success	COMPLETE	N/A	0:01:09	2016-08-09 16:22:27

Delete Completed

Delete Failed

Delete Selected

Note: If desired, you can delete all of the Complete and Failed tasks using the “Delete Completed” and “Delete Failed” buttons. This will leave only the in-progress tasks.

Appendix I.4. Configure the PMAC Application Guest NetBackup Virtual Disk

5 ☐	Management Server TVOE iLO/iLOM: SSH into the Management Server	Using an SSH client such as putty, ssh to the TVOE host as admusr. Login using virsh, and wait until you see the login prompt : <pre>\$ sudo /usr/bin/virsh list</pre> <pre>Id Name State ----- 1 myTPD running 2 PM&C running</pre> <pre>\$ sudo /usr/bin/virsh console <PM&C></pre> <pre>[Output Removed]</pre> <pre>Starting ntdMgr: [OK] Starting atd: [OK] 'TPD Up' notification(s) already sent: [OK] upstart: Starting tpdProvd... upstart: tpdProvd started. CentOS release 6.2 (Final) Kernel 2.6.32-220.17.1.el6prere16.0.0_80.14.0.x86_64 on an x86_64 PM&Cdev7 login:</pre>
6 ☐	PMAC: Shutdown the PMAC Guest	Assuming no in-progress tasks exists, it is safe to shut down the PMAC guest. Execute the following command: <pre>[admusr@pmac ~]\$ sudo /usr/bin/halt -p</pre> <pre>Broadcast message from root@pmacDev901 (/dev/ttyS0) at 11:20 ... The system is going down for power off NOW! [admusr@pmac ~]\$</pre> Eventually the virsh console session is closed and you are returned to the TVOE host command prompt: <pre>Halting system... Power down. [admusr@tvoe ~]\$</pre>

Appendix I.4. Configure the PMAC Application Guest NetBackup Virtual Disk

7 ☐	Management Server TVOE iLO/iLOM: Verify PMAC Guest is shutdown	From the TVOE host command prompt execute the following command: <pre>[admusr@tvoe ~]\$ sudo /usr/bin/virsh list --all</pre> <pre>Id Name State</pre> <pre>-----</pre> <pre>- pmac shut off</pre> <pre>[admusr@tvoe ~]\$</pre> This should show the guest state as “shut off”. You will want to be sure all guests are in the shut off state as well.
8 ☐	Management Server TVOE iLO/iLOM: Start PMAC Guest	Issue the following command to start the PMAC guest: <pre>\$ sudo /usr/bin/virsh</pre> <pre>virsh # list --all</pre> <pre>Id Name State</pre> <pre>-----</pre> <pre>20 pmacU14-1 shut off</pre> <pre>virsh # start pmacU14-1</pre> <pre>Domain pmacU14-1 started</pre> <pre>virsh # list --all</pre> <pre>Id Name State</pre> <pre>-----</pre> <pre>20 pmacU14-1 running</pre>

Appendix J: List of Frequently used Time Zones

Table 3. Time Zones

Time Zone Value	Description	Universal Time Code (UTC) Offset
UTC	Coordinated Universal Time	UTC-00
America/New_York	Eastern Time	UTC-05
America/Chicago	Central Time	UTC-06
America/Denver	Mountain Time	UTC-07
America/Phoenix	Mountain Standard Time - Arizona	UTC-07
America/Los_Angeles	Pacific Time	UTC-08
America/Anchorage	Alaska Time	UTC-09
Pacific/Honolulu	Hawaii	UTC-10
Africa/Johannesburg		UTC+02
America/Mexico_City	Central Time - most locations	UTC-06
Africa/Monrovia		UTC+00
Asia/Tokyo		UTC+09
America/Jamaica		UTC-05
Europe/Rome		UTC+01
Asia/Hong_Kong		UTC+08
Pacific/Guam		UTC+10
Europe/Athens		UTC+02
Europe/London		UTC+00
Europe/Paris		UTC+01
Europe/Madrid	mainland	UTC+01
Africa/Cairo		UTC+02
Europe/Copenhagen		UTC+01
Europe/Berlin		UTC+01
Europe/Prague		UTC+01
America/Vancouver	Pacific Time - west British Columbia	UTC-08
America/Edmonton	Mountain Time - Alberta, east British Columbia & westSaskatchewan	UTC-07
America/Toronto	Eastern Time - Ontario - most locations	UTC-05
America/Montreal	Eastern Time - Quebec - most locations	UTC-05
America/Sao_Paulo	South & Southeast Brazil	UTC-03
Europe/Brussels		UTC+01
Australia/Perth	Western Australia - most locations	UTC+08
Australia/Sydney	New South Wales - most locations	UTC+10
Asia/Seoul		UTC+09
Africa/Lagos		UTC+01
Europe/Warsaw		UTC+01
America/Puerto_Rico		UTC-04
Europe/Moscow	Moscow+00 - west Russia	UTC+04
Asia/Manila		UTC+08
Atlantic/Reykjavik		UTC+00
Asia/Jerusalem		UTC+02

Appendix K: Upgrade Cisco 4948 PROM

Appendix K.1. Upgrade Cisco 4948 PROM

S T E P #	This procedure explains the procedure to upgrade the Cisco 4948 PROM Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Virtual PMAC: Verify PROM image is on the system	Determine if the PROM image for the 4948E-F is on the system. Execute the following command: <pre>\$ ls /var/TKLC/smac/image/<PROM_image_file></pre> Note: If the file exists, continue with the next step. If the file does not exist, copy the file from the firmware media and ensure the file is specified by the HP Solutions Firmware Upgrade Pack Release Notes [1]
2 ☐	Virtual PMAC: Attach to switch Console	Connect serially to the switch by issuing the following command as admusr on the server: <pre>\$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg switch1A_console Enter platcfg@pmac5000101's password: <platcfg_password> [Enter `^Ec?' for help] Press Enter</pre> If the switch is not already in enable mode ("switch#" prompt) then issue the "enable" command, otherwise continue with the next step. <pre>Switch> enable Switch#</pre>

Appendix K.1. Upgrade Cisco 4948 PROM

3 ☐	4948E-F: Configure ports on the switch	Configure ports on the 4948E-F switch. To ensure connectivity, ping the management server's management vlan ip <pmac_mgmt_ip_address> address from the switch. Execute the following commands: <pre>Switch# conf t Switch(config-if)# switchport mode trunk Switch(config-if)# spanning-tree portfast trunk Switch(config-if)# end Switch# write memory</pre> Now issue ping command: <pre>Switch# ping <pmac_mgmtVLAN_ip_address></pre> Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to <pmac mgmt ip address>, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round trip min/avg/max = 1/1/4 ms If ping is not successful, double check that the procedure was completed correctly by repeating all steps up to this point. If after repeating those steps, ping is still unsuccessful, contact Appendix U: My Oracle Support (MOS).
4 ☐	4948E-F: Upgrade PROM	To upgrade PROM, execute the following commands: <pre>Switch# copy tftp: bootflash: Address or name of remote host []? <pmac_mgmt_ip_address> Source filename []? <PROM_image_file> Destination filename [<PROM_image_file>]? [Enter] Accessing tftp://<pmac_mgmt_ip_address>/<PROM_image_file>... Loading <PROM_image_file> from <pmac_mgmt_ip_address> (via Vlan2): !!!!! [OK- 45606 bytes] 45606 bytes copied in 3.240 secs (140759 bytes/sec) Switch#</pre>
5 ☐	4948E-F: Reload	Reload the switch, execute the following commands: <pre>Switch# reload System configuration has been modified. Save? [yes/no]: no Proceed with reload? [confirm] [Enter] === Boot messages removed ===</pre> Note: Type [Control-C] when “<i>Type control-C to prevent autobooting</i>” is displayed on the screen.

Appendix K.1. Upgrade Cisco 4948 PROM

6 ☐	4948E-F: Initiate PROM Upgrade	Initiate the PROM upgrade by executing the following commands: <pre>rommon 1 > boot bootflash:<PROM_image_file> === PROM upgrade messages removed === System will reset itself and reboot within few seconds....</pre>
7 ☐	4948E-F: Verify PROM Upgrade	The switch will reboot when the firmware upgrade completes. Allow it to boot up. Wait for the following line to be printed: <pre>Press RETURN to get started! Would you like to terminate autoinstall? [yes]: [Enter] Switch> show version include ROM ROM: 12.2(31r)SGA1 System returned to ROM by reload</pre> Note: Review the output and look for the ROM version. Verify that the version is the desired new version. If the switch does not boot properly or has the wrong ROM version, contact Appendix U: My Oracle Support (MOS)
8 ☐	4948E-F: Reset Switch Factory Defaults	Reset switch to factory defaults. Execute the following command: <pre>Switch# write erase Switch# reload</pre> Note: Wait until the switch reloads, then exit from console, enter <ctrl-e><c><. > and you will be returned to the server prompt. Note: There might be messages from the switch, if asked to confirm, press enter. If asked yes or no, type in 'no' and press enter.

Appendix L: Sample Network Element

In order to enter all the network information for a network element, a specially formatted XML file needs to be filled out with the required network information. The network information is needed to configure both the NOAM and any SOAM Network Elements.

It is expected that the maintainer/creator of this file has networking knowledge of this product and the customer site at which it is being installed. The following is an example of a Network Element XML file.

The SOAM Network Element XML file needs to have same network names for the networks as the NOAMP Network Element XML file has. It is easy to accidentally create different network names for NOAMP and SOAM Network Element, and then the mapping of services to networks will not be possible.

Note: In Below Figure 4 **Example Network Element XML File**, IP values are network ID IPs and not host IPs.

Figure 4. Example Network Element XML File

```
<?xml version="1.0"?>
<networkelement>
  <name>NE</name>
  <networks>
    <network>
      <name>INTERNALXMI</name>
      <vlanId>3</vlanId>
      <ip>10.2.0.0</ip>
      <mask>255.255.255.0</mask>
      <gateway>10.2.0.1</gateway>
      <isDefault>true</isDefault>
    </network>
    <network>
      <name>INTERNALIMI</name>
      <vlanId>4</vlanId>
      <ip>10.3.0.0</ip>
      <mask>255.255.255.0</mask>
      <nonRoutable>true</nonRoutable>
    </network>
  </networks>
</networkelement>
```

'nonRoutable' Field: By defining a network as 'nonRoutable' as seen above for INTERNALIMI, this means that the network shall not be routable outside the layer 3 boundary. This allows the user to define the same IP range in each SOAM site, and no duplicate IP check will be performed during server creation.

Appendix M: IDIH Fast Deployment Configuration

The `fdc.cfg` file contains 8 sections. The following is a list of those sections with a short description:

Section	Description
Software Images	A list of the TVOE, TPD, and iDIH application versions.
TVOE RMS	Includes Hardware Type and ILO address of the Rack Mount Server.
TVOE Configuration (Up to 3)	Contains all ip addresses, hostname and network devices for the TVOE host.
Guest Configurations (3)	The guest sections contain network and hostname configuration for the Oracle, Mediation and Application guests.

SOFTWARE IMAGES

Be sure to update the software images section based on software versions you intend to install. The following table outlines typical installation failures caused by incorrect software versions. Use the “`fdconfig dumpsteps -file=`” command to produce output of a Fast Deployment Session.

Software Image	Element	Command Text
TVOE ISO	mgmtsrvrtvoe	IPM Server
TPD ISO	Oracle,tpd Mediation,tpd Application,tpd	IPM Server
iDIH Mediation ISO	Mgmtsrvrtvoe,configExt	Transfer File
iDIH Oracle ISO iDIH Mediation ISO iDIH Application ISO	Oracle,ora Mediation,med Application,app	Upgrade Server

Note: For installation, `oracleGuest-8.1.0.0.0_81.x.x-x86_64.iso` is to be used

TVOE RMS

The TVOE RMS section contains the ILO ip address and Hardware profile. If the ILO IP address is incorrect the PMAC will not be able to discover the Rack Mount Server, server discovery must occur before the installation can begin.

TVOE CONFIGURATION

This section defines the hostname, network ip addresses for the TVOE bridges and it defines the network devices. You can define the devices you intend to use for bonded interfaces and the tagged bonded interfaces you intend to associate with a bridge.

GUEST CONFIGURATION

These sections contain the hostname, IPv4 addresses, IPv4 netmask, IPv4 gateway, and IPv6 addresses. If you do not intend to configure IPv6 addresses then leave those IP addresses commented out. The IPv6 netmask is included in the IPv6 address.

Note: Although the network for the iDIH 'int' network can be changed to a unique value, the IP scheme must follow the below rules:

- db-guest int ip = x.y.z.**n**
- Mediation-guest int ip = x.y.z.**n+1**
- Appserver-guest int ip = x.y.z.**n+2**

Note: this network is a non-routable network, so if the IP range of this network is not required; it is recommended that these values are left unchanged from the fast deployment template.

Below is FDC configuration template included on the mediation ISO:

IPv4 Configuration shown:

Note: IPv6 addresses should be entered into the <address> field in the FDC template. IPv6 prefix should be configured in the '<netmask>' field in the FDC template as only the number of the prefix (i.e 64)

Note: The template below is just an example. It may not always synchronize with the actual template. Please always refer to the actual template file in the delivered iso file.

```
<?xml version="1.0"?>

<!--
- Copyright (C) 2010, 2016, Oracle and/or its affiliates. All rights reserved.
-->

<fdc>
  <infrastructures>
    <infrastructure name="localPMAC">
      <software>
        <image id="ora">
          <name>oracleGuest-8.1.0.0.0_81.16.0-x86_64</name>
        </image>
        <image id="med">
          <name>mediation-8.1.0.0.0_81.16.0-x86_64</name>
        </image>
        <image id="app">
          <name>apps-8.1.0.0.0_81.16.0-x86_64</name>
        </image>
      </software>
      <hardware>
        <cabinet id="1">
          <cabid>1</cabid>
        </cabinet>
        <rms id="mgmtsrvr1">
          <!-- RMS #1 iLO/iLOM address -->
          <rmsOOBIP>10.250.56.201</rmsOOBIP>
          <!-- RMS #1 hostname can be changed here -->
          <rmsname>Sterling-TVOE-3</rmsname>
          <!-- iLO login user/pass -->
          <rmsuser>root</rmsuser>
          <rmpassword>changeme</rmpassword>
        </rms>
      </hardware>
    </infrastructure>
  </infrastructures>
</fdc>
```

```

<rms id="mgmtsrvr2">
  <!-- RMS #2 iLO/iLOM address -->
  <rmsOOBIP>10.250.56.202</rmsOOBIP>
  <!-- RMS #2 hostname can be changed here -->
  <rmsname>Sterling-TVOE-4</rmsname>
  <!--iLO login user/pass -->
  <rmsuser>root</rmsuser>
  <rmspassword>changeme</rmspassword>
</rms>
<rms id="mgmtsrvr3">
  <!-- RMS #3 iLO/iLOM address -->
  <rmsOOBIP>10.250.56.203</rmsOOBIP>
  <!-- RMS #3 hostname can be changed here -->
  <rmsname>Sterling-TVOE-5</rmsname>
  <!--iLO login user/pass -->
  <rmsuser>root</rmsuser>
  <rmspassword>changeme</rmspassword>
</rms>
</hardware>
<tvoehost id="mgmtsrvrtvoel">
  <hardware>
    <!--rmshwid must match rms id above -->
    <rmshwid>mgmtsrvr1</rmshwid>
  </hardware>
</tvoehost>
<tvoehost id="mgmtsrvrtvoe2">
  <hardware>
    <!--rmshwid must match rms id above -->
    <rmshwid>mgmtsrvr2</rmshwid>
  </hardware>
</tvoehost>
<tvoehost id="mgmtsrvrtvoe3">
  <hardware>
    <!--rmshwid must match rms id above -->
    <rmshwid>mgmtsrvr3</rmshwid>
  </hardware>
</tvoehost>
</infrastructure>
</infrastructures>
<servers>
  <tvoeguest id="ORA">
    <infrastructure>localPMAC</infrastructure>
    <!--Specify which Rack Mount Server TVOE Host the Oracle server will be placed -->
    <tvoehost>mgmtsrvrtvoel</tvoehost>
    <name>ORA</name>
    <cpus>4</cpus>
    <memory>8192</memory>
    <watchdog>ON</watchdog>
    <vnics>
      <vnic>
        <hostbridge>control</hostbridge>
        <guestdevname>control</guestdevname>
      </vnic>
      <vnic>
        <hostbridge>int</hostbridge>
        <guestdevname>int</guestdevname>
      </vnic>
      <vnic>
        <hostbridge>xmi</hostbridge>
        <guestdevname>xmi</guestdevname>
      </vnic>
    </vnics>
    <vdisks>
      <vdisk>
        <hostvolname>ORA.img</hostvolname>
        <hostpool>vgguests</hostpool>
        <size>81920</size>
        <primary>yes</primary>
        <guestdevname>PRIMARY</guestdevname>
      </vdisk>
      <vdisk>
        <hostvolname>ORA_sdb.img</hostvolname>
        <hostpool>vgguests</hostpool>
        <size>51200</size>
        <primary>no</primary>
        <guestdevname>sdb</guestdevname>
      </vdisk>
      <vdisk>
        <hostvolname>ORA_sdc.img</hostvolname>
        <hostpool>vgguests</hostpool>
        <size>51200</size>

```

```

    <primary>no</primary>
    <guestdevname>sdc</guestdevname>
  </vdisk>
</vdisk>
</vdisk>
<archive>
  <image>ora</image>
  <name>idih-ora</name>
</archive>
<tpdnetworking>
  <tpdinterfaces>
    <tpdinterface id="int">
      <device>int</device>
      <type>Ethernet</type>
      <onboot>yes</onboot>
      <bootproto>none</bootproto>
      <address>10.254.254.2</address>
      <netmask>255.255.255.224</netmask>
    </tpdinterface>
    <tpdinterface id="xmi">
      <device>xmi</device>
      <type>Ethernet</type>
      <onboot>yes</onboot>
      <bootproto>none</bootproto>
      <!--Specify xmi IP address -->
      <address>10.240.30.204</address>
      <!--Specify xmi subnet -->
      <netmask>255.255.255.128</netmask>
    </tpdinterface>
  </tpdinterfaces>
  <tpdroutes>
    <tpdroute id="xmi_default">
      <type>default</type>
      <device>xmi</device>
      <!--Specify default gateway of xmi network-->
      <gateway>10.240.30.129</gateway>
    </tpdroute>
  </tpdroutes>
</tpdnetworking>
<serverinfo>
  <!--Specify Oracle server hostname-->
  <hostname>Sterling-IDIH-ora</hostname>
</serverinfo>
<scripts>
  <postsrvapp>
    <scriptfile id="oraPostImageInstall">
      <filename>/usr/bin/sudo</filename>
      <arguments>/opt/xIH/oracle/utills/post_image_install.sh</arguments>
      <timeout>1500</timeout>
    </scriptfile>
  </postsrvapp>
  <postdeploy>
    <scriptfile id="oraHealthcheck">
      <filename>/usr/bin/sudo</filename>
      <arguments>/usr/TKLC/xIH/plat/bin/analyze_server.sh -i > /tmp/analyze_server.sh</arguments>
    </scriptfile>
  </postdeploy>
</scripts>
</tvoeguest>
<tvoeguest id="APP">
  <infrastructure>localPMAC</infrastructure>
  <!--Specify which Rack Mount Server TVOE Host the Application server will be placed -->
  <tvoehost>mgmtsrvrtvoe3</tvoehost>
  <name>APP</name>
  <cpus>4</cpus>
  <memory>8192</memory>
  <watchdog>ON</watchdog>
  <vnics>
    <vnic>
      <hostbridge>control</hostbridge>
      <guestdevname>control</guestdevname>
    </vnic>
    <vnic>
      <hostbridge>int</hostbridge>
      <guestdevname>int</guestdevname>
    </vnic>
    <vnic>
      <hostbridge>xmi</hostbridge>
      <guestdevname>xmi</guestdevname>
    </vnic>
  </vnics>
</tvoeguest>
</vdisk>

```

```

<vdisk>
  <hostvolname>APP.img</hostvolname>
  <hostpool>vgguests</hostpool>
  <size>65536</size>
  <primary>yes</primary>
  <guestdevname>PRIMARY</guestdevname>
</vdisk>
</vdisks>
<archive>
  <image>app</image>
  <name>idih-app</name>
</archive>
<tpdnetworking>
  <tpdinterfaces>
    <tpdinterface id="int">
      <device>int</device>
      <type>Ethernet</type>
      <onboot>yes</onboot>
      <bootproto>none</bootproto>
      <address>10.254.254.4</address>
      <netmask>255.255.255.224</netmask>
    </tpdinterface>
    <tpdinterface id="xmi">
      <device>xmi</device>
      <type>Ethernet</type>
      <onboot>yes</onboot>
      <bootproto>none</bootproto>
      <!--Specify xmi IP address -->
      <address>10.240.30.202</address>
      <!--Specify xmi subnet mask -->
      <netmask>255.255.255.128</netmask>
    </tpdinterface>
  </tpdinterfaces>
  <tpdroutes>
    <tpdroute id="xmi_default">
      <type>default</type>
      <device>xmi</device>
      <!--Specify default gateway of xmi network-->
      <gateway>10.240.30.129</gateway>
    </tpdroute>
  </tpdroutes>
</tpdnetworking>
<serverinfo>
  <!--Specify Application server hostname-->
  <hostname>Sterling-IDIH-app</hostname>
</serverinfo>
<scripts>
  <postdeploy>
    <scriptfile id="appPreSleep">
      <filename>/bin/sleep</filename>
      <arguments>200</arguments>
    </scriptfile>
    <scriptfile id="appPostImageInstall">
      <filename>/usr/bin/sudo</filename>
      <arguments>/opt/xIH/apps/post image install.sh</arguments>
    </scriptfile>
    <scriptfile id="appSleep">
      <filename>/bin/sleep</filename>
      <arguments>60</arguments>
    </scriptfile>
    <scriptfile id="appHealthcheck">
      <filename>/usr/bin/sudo</filename>
      <arguments>/usr/TKLC/xIH/plat/bin/analyze server.sh -i > /tmp/analyze server.log</arguments>
    </scriptfile>
  </postdeploy>
</scripts>
</tvoeguest>
<tvoeguest id="MED">
  <infrastructure>localPMAC</infrastructure>
  <!--Specify which Rack Mount Server TVOE Host the Mediation server will be placed -->
  <tvoehost>mgmtsrvrtvoe2</tvoehost>
  <name>MED</name>
  <cpus>4</cpus>
  <memory>8192</memory>
  <watchdog>ON</watchdog>
  <vnics>
    <vnic>
      <hostbridge>control</hostbridge>
      <guestdevname>control</guestdevname>
    </vnic>
  </vnics>

```

```

    <hostbridge>int</hostbridge>
    <guestdevname>int</guestdevname>
  </vnic>
  <vnic>
    <hostbridge>xmi</hostbridge>
    <guestdevname>xmi</guestdevname>
  </vnic>
  <vnic>
    <hostbridge>imi</hostbridge>
    <guestdevname>imi</guestdevname>
  </vnic>
</vnics>
<vdisks>
  <vdisk>
    <hostvolname>MED.img</hostvolname>
    <hostpool>vgguests</hostpool>
    <size>65536</size>
    <primary>yes</primary>
    <guestdevname>PRIMARY</guestdevname>
  </vdisk>
</vdisks>
<archive>
  <image>med</image>
  <name>idih-med</name>
</archive>
<tpdnetworking>
  <tpdinterfaces>
    <tpdinterface id="imi">
      <device>imi</device>
      <type>Ethernet</type>
      <onboot>yes</onboot>
      <bootproto>none</bootproto>
      <!--Specify imi IP address -->
      <address>192.168.201.139</address>
      <!--Specify imi subnet mask -->
      <netmask>255.255.255.0</netmask>
    </tpdinterface>
    <tpdinterface id="int">
      <device>int</device>
      <type>Ethernet</type>
      <onboot>yes</onboot>
      <bootproto>none</bootproto>
      <address>10.254.254.3</address>
      <netmask>255.255.255.224</netmask>
    </tpdinterface>
    <tpdinterface id="xmi">
      <device>xmi</device>
      <type>Ethernet</type>
      <onboot>yes</onboot>
      <bootproto>none</bootproto>
      <!--Specify xmi IP address -->
      <address>10.240.30.203</address>
      <!--Specify xmi subnet mask -->
      <netmask>255.255.255.128</netmask>
    </tpdinterface>
  </tpdinterfaces>
  <tpdroutes>
    <tpdroute id="xmi_default">
      <type>default</type>
      <device>xmi</device>
      <!--Specify default gateway of xmi network-->
      <gateway>10.240.30.129</gateway>
    </tpdroute>
  </tpdroutes>
</tpdnetworking>
<serverinfo>
  <!--Specify Mediation server hostname-->
  <hostname>Sterling-IDIH-med</hostname>
</serverinfo>
<scripts>
  <postdeploy>
    <scriptfile id="medPreSleep">
      <filename>/bin/sleep</filename>
      <arguments>200</arguments>
    </scriptfile>
    <scriptfile id="medPostImageInstall">
      <filename>/usr/bin/sudo</filename>
      <arguments>/opt/xIH/mediation/post_image_install.sh</arguments>
    </scriptfile>
    <scriptfile id="medSleep">
      <filename>/bin/sleep</filename>

```

```

        <arguments>60</arguments>
      </scriptfile>
      <scriptfile id="medHealthcheck">
        <filename>/usr/bin/sudo</filename>
        <arguments>/usr/TKLC/xIH/plat/bin/analyze_server.sh -i > /tmp/analyze_server.log</arguments>
      </scriptfile>
    </postdeploy>
  </scripts>
</tvoeguest>
</servers>
</fdc>

```

Appendix N: Creating a Bootable USB Drive on Linux

Appendix P.1. Creating a Bootable USB Drive on Linux

S T E P #		This procedure will create a Bootable USB drive from a .usb file on a Linux Machine Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	Insert USB Media	Insert the USB Media into the USB Port. It should automatically be mounted under /media Obtain the path of the USB drive by running: \$ ls /media The output should be similar to the following: sdb1 Note down the path without the partition number (in this case, it would be /dev/sdb)
2 ☐	Linux Machine	Obtain the TVOE .iso file and copy it onto the local Linux machine (e.g. under /var/TKLC/upgrade)
3 ☐	Copy the .USB file onto the USB drive	Use the dd command to copy the .usb file onto the USB drive Note: Make sure you do not use the partition number when copying the file \$ sudo dd if=<path_to_iso> of=/dev/sdb bs=4M oflag=direct

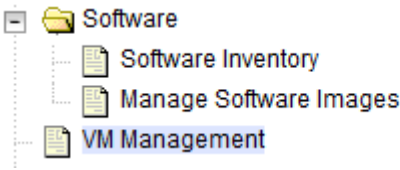
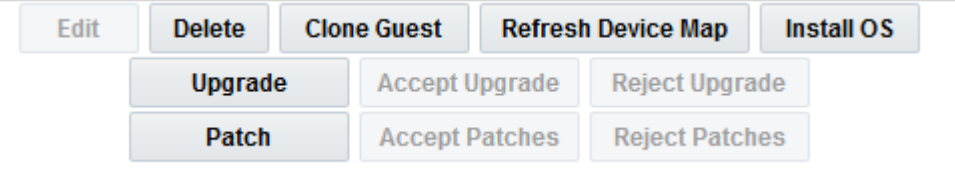
Appendix O: IDIH External Drive Removal

This procedure should only be run if the user intends to do a fresh installation on an existing IDIH.

Appendix O.2. IDIH External Drive Removal

S T E P #	This procedure will destroy all of the data in the Oracle Database. Warning: Do not perform this procedure on an IDIH system unless you intent to do a fresh TVOE installation. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PMAC GUI: Login Open web browser and enter: <a href="https://<PMAC_Mgmt_Network_IP>">https://<PMAC_Mgmt_Network_IP> Login as guiadmin user:  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.

Appendix O.2. IDIH External Drive Removal

2 ☐	PMAC GUI: Delete VMs if Needed	Before a re-installation can be performed, the IDIH VMs must be removed first. Navigate to Main Menu -> VM Management  Select each of the IDIH VMs and select the Delete button. 
3 ☐	IDIH TVOE HOST: Login	Establish an SSH session to the TVOE host, login as admusr
4 ☐	IDIH TVOE HOST: Verify External Drive Exists	Execute the following command to verify the external drive exists: HP DL380: <pre>\$ sudo hpssacli ctrl slot=2 Id all show</pre>

Appendix O.2. IDIH External Drive Removal

5 ☐	IDIH TVOE HOST: Remove the External Drive and Volume Group	Execute the following command to remove the external drive and volume group: HP DL380: <pre>\$ sudo /usr/TKLC/plat/sbin/storageClean hpdisk --slot=2</pre> Oracle X5-2/Netra X5-2/X6-2: Logon to TVOE host as root user and execute the virsh commands as show below to manually delete the image files. Make sure that storage pool other than vgguests are also cleaned. <pre>[root@hellcat~]# virsh vol-list vgguests Name Path ----- application.img /dev/vgguests/application.img mediation.img /dev/vgguests/mediation.img oracle.img /dev/vgguests/oracle.img pmac.img /dev/vgguests/pmac.img pmac_images.img /dev/vgguests/pmac_images.img pmac_isoimages.img /dev/vgguests/pmac_isoimages.img pmac_logs.img /dev/vgguests/pmac_logs.img [root@hellcat~]# virsh vol-delete --vol=oracle.img --pool=vgguests Vol oracle.img deleted [root@hellcat~]# virsh vol-delete --vol=mediation.img --pool=vgguests Vol mediation.img deleted [root@hellcat~]# virsh vol-delete --vol=application.img --pool=vgguests Vol application.img deleted</pre> <pre>[root@hellcat~]# virsh pool-list Name State Autostart ----- external1 active yes external2 active yes external3 active yes vgguests active yes [root@hellcat~]# virsh vol-list external1 Name Path ----- [root@hellcat~]# virsh vol-list external2 Name Path ----- [root@hellcat~]# virsh vol-list external3 Name Path -----</pre>

Appendix P: Growth/De-Growth/Re-Shuffle (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)

For scenarios where growth or de-growth is required, it may be necessary to delete or re-shuffle VM guests, SDS, and DSR servers. Appendix T.1 will explain how to add individual VMs and add various DSR/SDS servers. Appendix T.2 will explain how to delete individual VMs and move or remove various DSR/SDS servers.

Appendix P.1: Growth (X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)

For growth scenarios where it is necessary to add DSR/SDS servers, the following sequence of steps should be followed:

Step	Procedure(s)
Perform Backups	Appendix P.1.1
Perform system health check	Appendix P.1.2
Identify Servers which will be affected by the Growth: • DR-NOAM • SOAM Spares • DSR MP (SBR, SS7MP, IPFE)/ SDS DP • Query Server	
Add new rack mount server	Appendix P.1.3
Create and Configure the VMs on the new Rack Mount Servers	
Configure Servers in new VM locations	NOAM/DR-NOAM (DSR/SDS): Appendix P.1.4 SOAM (DSR/SDS): Appendix P.1.5 MP/DP (DSR/SDS): Appendix P.1.6 Query Server (SDS): Appendix P.1.7
Post Growth Health Check	Appendix P.1.8
Post Growth Backups	Appendix P.1.9

Appendix P.1.1 Perform Backups

S T E P #	This procedure will reference steps to backup all necessary items before a growth scenario. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Backup TVOE	Backup all TVOE host configurations by executing Section 4.17.6 Backup TVOE Configuration
2 ☐	Backup PMAC	Backup the PMAC application by executing Section 4.17.7 Backup PMAC Application
3 ☐	Backup NOAM/SOAM databases	Backup the NOAM and SOAM Databases by executing Sections 4.17.8 Backup NOAM Database and 4.17.9 Backup SOAM Database Note: Database backup on SDS SOAMs not required

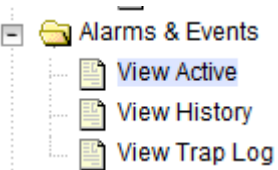
Appendix P.1.2 Perform Health Check

S T E P #	This procedure will provide steps verify system status and log all alarms. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: 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: <code>http://<Primary_NOAM_VIP_IP_Address></code> Login as the <i>guiadmin</i> user: 

Appendix P.1.2 Perform Health Check

2	NOAM VIP GUI: Verify Server Status	Navigate to Main Menu -> Status & Manage -> Server Status & Manage Network Elements Server HA Database KPIs Processes Verify all Server Status is Normal (Norm) for: Alarm (Alm), Database (DB), Replication Status, and Processes (Proc). <table><tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr></table> Do not proceed to with Growth/De-Growth if any of the above states are not Norm. If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the feature activation. If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed. If there are Major or Critical alarms present, these alarms should be analyzed prior to proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms	Appl State	Alm	DB	Reporting Status	Proc	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm
Appl State	Alm	DB	Reporting Status	Proc																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
3	NOAM VIP GUI: Verify Server Configuration	Navigate to Main Menu -> Configuration -> Server Groups Configuration Networking Servers Server Groups Resource Domains Places Place Associations Verify the configuration data is correct for your network.																									

Appendix P.1.2 Perform Health Check

4 ☐	NOAM VIP GUI: Log Current Alarms	Navigate to Main Menu -> Alarms & Events -> View Active  Click on the Report button Save or Print this report, keep copies for future reference.
5 ☐	SOAM VIP GUI: Repeat For SOAM	Repeat Steps 1-4 for the SOAM

Appendix P.1.3 Adding a new TVOE Server/VMs

S T E P #	This procedure will provide steps to add a new rack mount server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Add/Configure Additional Rack Mount Servers	Follow the steps in the following sections to install and configure TVOE on additional rack mount servers. 1. Section Add Rack Mount Server to PMAC 2. Section Install TVOE on Additional Rack Mount Servers 3. Section Configure TVOE on Additional Rack Mount Servers
2 ☐	Add/Configure New VMs	1. Determine CPU placement and pinning information by referring to Section Determine VM Placement and Socket Pinning 2. Create new virtual Machines by following Section Virtual Machine/Network Fast Deployment 3. Perform CPU Pinning by following Section CPU Pinning

Appendix P.1.4 Growth: DR-NOAM

S T E P #	This procedure will reference steps to configure a DR-NOAM on the new virtual machine for VM Growth scenarios. Prerequisites: - NEW Virtual Machine Created - TPD/DSR software installed Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	NOAM VIP GUI: Configure the DR-NOAM	Configure the DR-NOAM by executing the steps referenced in the following procedures: <u>DSR DR-NOAM:</u> Section 4.14.3 DSR Configuration: Disaster Recovery NOAM (Optional) <u>SDS DR-NOAM:</u> Section 4.15.3 SDS Configuration: Disaster Recovery SDS NOAM (Optional)
2 ☐	DR-NOAM: Activate Optional Features (DSR Only)	DSR DR-NOAMs ONLY, SDS DR-NOAMs SKIP THIS STEP If there are any optional features currently activated, the feature activation procedures will need to be run again. Refer to Section Optional Features
3 ☐	DR-NOAM VIP: Login	Establish an SSH to the DR-NOAM VIP address, login as admusr .
4 ☐	DR-NOAM VIP: Transfer Optimization Script from the Primary NOAM	Execute the following commands to transfer and set permissions of the optimization script from the primary NOAM: <pre>\$ sudo scp -r admusr@<Primary NOAM XMI VIP>:/usr/TKLC/dsr/bin/rmsNoamConfig.sh /usr/TKLC/dsr/bin</pre> <pre>\$ sudo chmod 777 /usr/TKLC/dsr/bin/rmsNoamConfig.sh</pre>
5 ☐	NOAM VIP: Execute the Optimization Script on the Active NOAM	Execute the following commands to execute the performance optimization script on the active NOAM: <pre>\$ cd /usr/TKLC/dsr/bin/</pre> <pre>\$ sudo ./rmsNoamConfig.sh</pre> Note: Configuration Successful output should be given.

Appendix P.1.4 Growth: DR-NOAM

6 ☐	NOAM VIP: Execute the key revocation Script on the Active NOAM (RADIUS)	If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator) Execute the following commands to execute the key revocation script on active NOAM server to copy key file to new NOAM server created: <pre>\$ cd /usr/TKLC/dsr/bin/ \$./sharedKrevo -synchronize -server <new_NOAM_hostname></pre> Note: Key transfer successful output should be given.

Appendix P.1.5 Growth: SOAM spare (DSR/PCA Only)

S T E P #	This procedure will reference steps to configure an SOAM spare on the new virtual machine for VM growth scenarios. Prerequisites: • NEW Virtual Machine Created • TPD/DSR software installed Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	NOAM VIP GUI: Configure the SOAM spare	Configure the SOAM spare by executing the steps referenced in the following procedures: <u>DSR SOAM spare:</u> • Procedure 24 • Procedure 25 • Procedure 26 (Steps 1,4,6, and 9)
2 ☐	NOAM GUI: Activate Optional Features	If there are any optional features currently activated, the feature activation procedures will need to be run again. Refer to Section Optional Features

Appendix P.1.5 Growth: SOAM spare (DSR/PCA Only)

3 ☐	NOAM VIP: Execute the key revocation Script on the Active NOAM (RADIUS)	If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator) Execute the following commands to execute the key revocation script on active NOAM server to copy key file to new SOAM server created: <pre>\$ cd /usr/TKLC/dsr/bin/ \$./sharedKrevo -synchronize -server <new_SOAM_hostname></pre> Note: Key transfer successful output should be given.

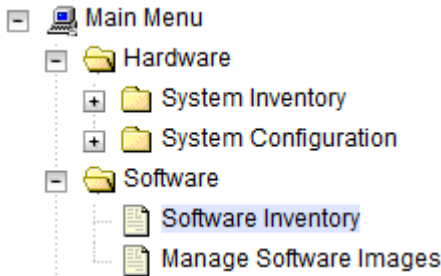
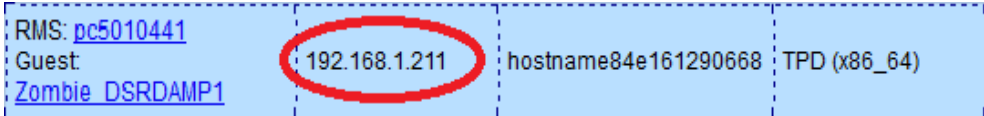
Appendix P.1.6 Growth: MP/DP

S T E P #	This procedure will reference steps to configure an MP/DP on the new virtual machine for growth scenarios. Prerequisites: • NEW Virtual Machine Created • TPD/DSR software installed Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	NOAM VIP GUI: Configure the MP/DP Configure the MP/DP by executing the steps referenced in the following procedures: • <u>DSR MP:</u> Procedure 30 (Steps 1-2, 7-14, 15-16(Optional), 17) Procedure 31 Procedure 32 Procedure 64 • <u>SDS DP:</u> Procedure 49 Procedure 50 Procedure 64

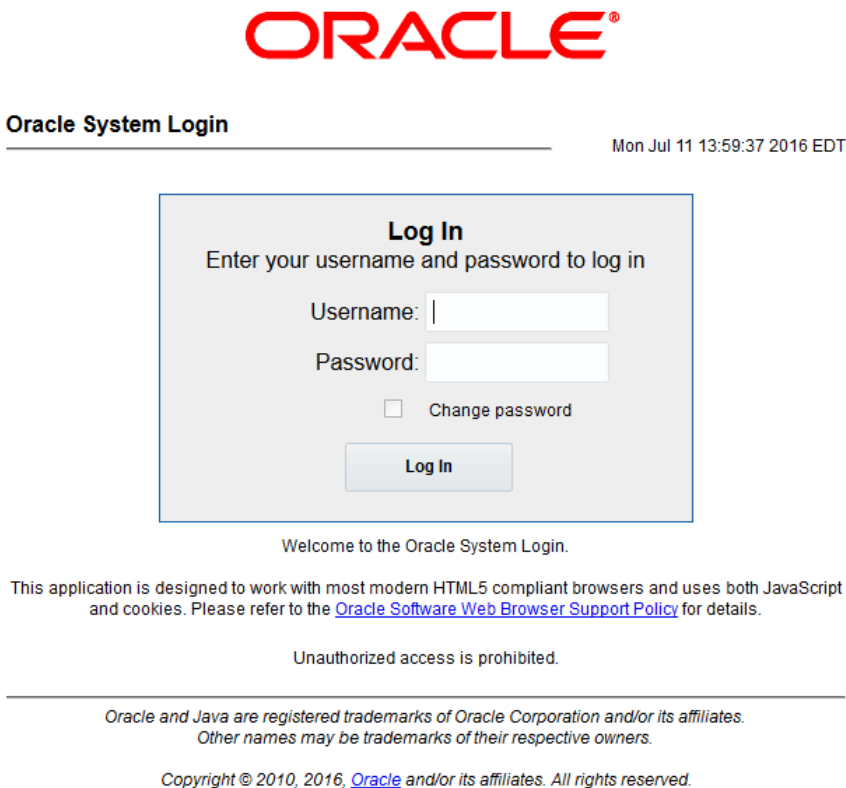
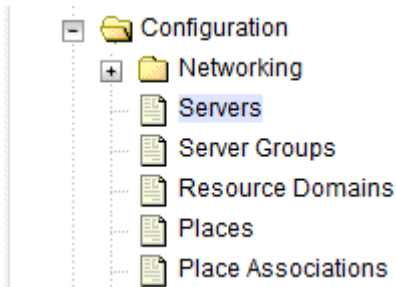
Appendix P.1.6 Growth: MP/DP

2 ☐	NOAM VIP: Execute the key revocation Script on the Active NOAM (RADIUS)	If the RADIUS key has never been revoked, skip this step (If RADIUS was never configured on any site in the network, the RADIUS key would have most likely never been revoked. Check with your system administrator) Execute the following commands to execute the key revocation script on active NOAM server to copy key file to new MP server created: <pre>\$ cd /usr/TKLC/dsr/bin/ \$./sharedKrevo -synchronize -server <new_MP_hostname></pre> Note: Key transfer successful output should be given.

Appendix P.1.6.1 Growth: MP (7.x to 8.x upgraded system)

STEP #	This procedure should be executed ONLY to configure an MP on the new virtual machine for growth scenarios for 7.x to 8.x upgraded system Prerequisites: - NEW Virtual Machine Created - TPD/DSR software installed Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PMAC: Exchange SSH keys between MP site's local PMAC and the MP server Use the MP site's PMAC GUI to determine the Control Network IP address of the server that is to be an MP server. From the MP site's PMAC GUI, navigate to Main Menu -> Software -> Software Inventory.   Note the IP address for an MP server. Login to the MP site's PMAC terminal as the admusr. From a terminal window connection on the MP site's PMAC as the admusr.

Appendix P.1.6.1 Growth: MP (7.x to 8.x upgraded system)

		Exchange SSH keys for admusr between the PMAC and the MP server using the keyexchange utility, using the Control network IP address for the MP server. <pre>\$ keyexchange admusr@<MP_Control_IP Address></pre> When prompted for the password, enter the password for the admusr user of the MP server.
2 ☐	PRIMARY NOAM VIP GUI: Login	Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of < NOAM_XMI_VIP_IP_Address >: Login as the guiadmin user: 
3 ☐	NOAM VIP GUI: Insert the MP server (Part 1)	Navigate to Main Menu->Configuration->Servers 

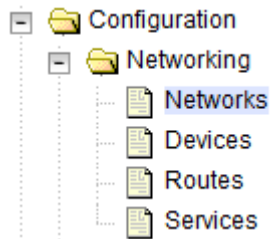
Appendix P.1.6.1 Growth: MP (7.x to 8.x upgraded system)

		Select the Insert button to insert the new MP server into servers table. Insert Edit Delete Export Report Fill out the following values: Hostname:<Hostname> Role: MP Network Element: [Choose Network Element] Hardware Profile: DSR TVOE Guest Location: <enter an optional location description> The interface configuration form will now appear. • For the XMI network, enter the MP's XMI IP address. Select the xmi interface. • For the IMI network, enter the MP's IMI IP address. Select the imi interface.				
4	☐ NOAM VIP GUI: Insert the MP server (Part 2)	Next, add the following NTP servers: <table><tr><th>NTP Server</th><th>Preferred?</th></tr><tr><td><MP-RMS-TVOE-IP-Address></td><td>Yes</td></tr></table> Select OK when all fields are filled in to finish MP server insertion.	NTP Server	Preferred?	<MP-RMS-TVOE-IP-Address>	Yes
NTP Server	Preferred?					
<MP-RMS-TVOE-IP-Address>	Yes					
5	☐ NOAM VIP GUI: Export the Configuration	Navigate to Main Menu -> Configuration -> Servers. Configuration Networking Servers Server Groups Resource Domains Places Place Associations From the GUI screen, select the MP server and then select Export to generate the initial configuration data for that server. Insert Edit Delete Export Report				

Appendix P.1.6.1 Growth: MP (7.x to 8.x upgraded system)

6 ☐	NOAM VIP: Copy Configuration File to MP Server	Obtain a terminal session to the NOAM VIP as the admusr user. Use the awpushcfg utility to copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the NOAM to the MP server, using the Control network IP address for the MP server. The configuration file will have a filename like “TKLCConfigData.<hostname>.sh”. <pre>\$ sudo awpushcfg</pre> The awpushcfg utility is interactive, so the user will be prompted for the following: • IP address of the local PMAC server: Use the management 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 MP server). • Hostname of the target server: Enter the server name configured in step 1
7 ☐	MP Server: Verify awpushcfg was called and Reboot the Configured Server	Obtain a terminal window connection on the MP server console by establishing an ssh session from the PMAC of the MP. <pre>\$ ssh admusr@<MP_Control_IP></pre> Login as the admusr user. Verify awpushcfg was called by checking the following file: <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> Verify no errors are present and that the following message is displayed: <pre>[SUCCESS] script completed successfully!</pre> Note: The script may return success even when errors are reported in the log file. Go through the entire install.log file to verify no errors are present. Reboot the sever: <pre>\$ sudo init 6</pre> Proceed to the next step once the Server finished rebooting, The server is done rebooting once the login prompt is displayed.
8 ☐	MP Server: Login	After the reboot, login as admusr.
9 ☐	MP Server: Verify Server	Execute the following command on the server and make sure that no errors are returned:

Appendix P.1.6.1 Growth: MP (7.x to 8.x upgraded system)

	Health	<pre>\$ sudo syscheck Running modules in class hardware...OK Running modules in class disk...OK Running modules in class net...OK Running modules in class system...OK Running modules in class proc...OK LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>
10 ☐	MP Server: Delete Auto-Configured Default Route on MP and Replace it with a Network Route via the XMI Network-Part1 (Optional)	Note: THIS STEP IS OPTIONAL AND SHOULD ONLY BE EXECUTED IF YOU PLAN TO CONFIGURE A DEFAULT ROUTE ON YOUR MP THAT USES A SIGNALING (XSI) NETWORK INSTEAD OF THE XMI NETWORK. (Not executing this step will mean that a default route will not be configurable on this MP and you will have to create separate network routes for each signaling network destination.) Login into the site's PMAC then SSH to the MP's control address (<i>Alternatively you can login to the TVOE host and access the MP via virsh console <MP VM></i>) Determine <XMI_Gateway_IP> from your SO site network element info. Gather the following items: • <NO_XMI_Network_Address> • <NO_XMI_Network_Netmask> • <DR_NO_XMI_Network_Addres> • <DR_NO_XMI_Network_Netmask> • <TVOE_Mgmt_XMI_Network_Address> • <TVOE_Mgmt_XMI_Network_Netmask> Note: You can either consult the XML files you imported earlier, or go to the NO GUI and view these values from the Main Menu -> Configuration -> Networking -> Networking screen.  Proceed to the next step to modify the default routes on the MP servers.
11 ☐	MP Server: Delete Auto-Configured Default Route on MP and Replace it with a Network	After gathering the network information from step 14, proceed with modifying the default routes on the MP server. Establish a connection to the MP server, login as admusr. Create network routes to the NO's XMI(OAM) network:

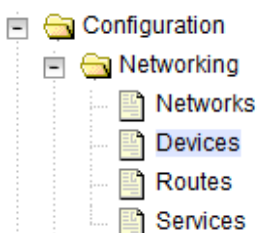
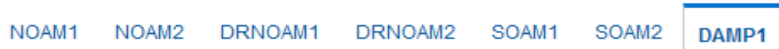
Appendix P.1.6.1 Growth: MP (7.x to 8.x upgraded system)

	Route via the XMI Network-Part2 (Optional)	Note: If your NOAM XMI network is exactly the same as your MP XMI network, then you should skip this command and only configure the DR NO route. <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --address=<NO_Site_Network_ID> --netmask=<NO_Site_Network_Netmask> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface> Route to <MP_XMI_Interface> added.</pre> Create network routes to the DR NO's XMI(OAM) network: <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --address=<DR-NO_Site_Network_ID> --netmask=<DR-NO_Site_Network_Netmask> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface> Route to <MP_XMI_Interface> added.</pre> Create network routes to the Management Server TVOE XMI(OAM) network for NTP: <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --address=<TVOE_Mgmt_XMI_Network_Address> --netmask=<TVOE_Mgmt_XMI_Network_Netmask> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface> Route to <MP_XMI_Interface> added.</pre> (Optional) If Sending SNMP traps from individual servers, create host routes to customer SNMP trap destinations on the XMI network: <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=host --address=<Customer_NMS_IP> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface> Route to <MP_XMI_Interface> added.</pre> (Repeat for any existing customer NMS stations) Delete the existing default route: 1. Login to the PRIMARY NOAM VIP GUI 2. Navigate to Configuration->Networking->Networks 3. Select the specific SO tab. 4. Select the XMI network and click 'Unlock'. Click OK to confirm 5. Go to Configuration->Networking->Routes 6. Select the Specific MP XMI route and click 'Delete'. 7. Click OK to confirm. 8. Repeat the above steps for all required MPs to delete the XMI routes 9. Select Configuration->Networking->Networks 10. Select the respective SOAM tab. 11. Select the XMI network and click 'Lock'. Click OK to confirm
12 ☐	MP Server: Verify	After steps 10 -11 have been executed, verify network connectivity. Establish a connection to the MP server, login as admusr.

Appendix P.1.6.1 Growth: MP (7.x to 8.x upgraded system)

	connectivity	Ping active NO XMI IP address to verify connectivity: <pre>\$ ping <ACTIVE_NO_XMI_IP_Address> PING 10.240.108.6 (10.240.108.6) 56(84) bytes of data. 64 bytes from 10.240.108.6: icmp_seq=1 ttl=64 time=0.342 ms 64 bytes from 10.240.108.6: icmp_seq=2 ttl=64 time=0.247 ms</pre> (Optional) Ping Customer NMS Station(s): <pre>\$ ping <Customer_NMS_IP> PING 172.4.116.8 (172.4.116.8) 56(84) bytes of data. 64 bytes from 172.4.116.8: icmp_seq=1 ttl=64 time=0.342 ms 64 bytes from 172.4.116.8: icmp_seq=2 ttl=64 time=0.247 ms</pre> If you do not get a response, then verify your network configuration. If you continue to get failures then halt the installation and contact Oracle customer support.
13 ☐	Repeat for remaining MPs	Repeat the above steps (1-12) for all remaining MP (SS7-MP, DA-MP, SBR and IPFE) servers.
14 ☐	Configure the MP	Execute the following procedures: • Procedure 31 Configure Places and Assign MP Servers to Places (PCA & DCA ONLY) • Procedure 32 Configure the MP Server Group(s) and Profile(s)
<i>The following steps (15-18) are to configure the Signaling Interfaces for the newly added MPs</i>		
15 ☐	Newly created MP Server console: Manually configure signaling interface	1. Login to iLO/iLOM, follow Appendix D: TVOE iLO/iLOM GUI Access for instructions on how to access the iLO/iLOM GUI. <pre>https://<management_server_iLO_ip></pre> 2. Login to the newly added MP Console 3. Execute the below netAdm commands to configure the Signaling interfaces <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --onboot=yes --netmask=<netmask> --device=xsil --address=<ip address> Interface xsil added.</pre> 4. Repeat step 3 to configure the required number of Signaling interfaces 5. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.

Appendix P.1.6.1 Growth: MP (7.x to 8.x upgraded system)

		<pre>\$ sudo init 6</pre>																					
16	Primary NOAM VIP GUI: Take ownership of the Signaling interfaces and make it Deployed	Navigate to Main Menu->Configuration->Networking-> Devices.  You should see several tabs each representing a server in the system. Click on the tab representing the newly created MP.  Select all newly configured Signaling Ethernet devices which are having “Discovered” as their Configuration Status. <table><tr><td>xmi</td><td>Ethernet</td><td>MTU = 1500 bootProto = none onboot = yes hwAddr = 02:4D:0D:8A:D0:E7</td><td>10.240.32.27 (INTERNALXMI) 2606:b400:605:b821:4d:dff:fe8a:d0e7 (/64) fe80::4d:dff:fe8a:d0e7 (/64)</td><td>Deployed</td></tr><tr><td>imi</td><td>Ethernet</td><td>MTU = 1500 bootProto = none onboot = yes hwAddr = 02:17:A2:37:DB:45</td><td>192.168.100.22 (INTERNALIMI) fe80::17:a2ff:fe37:db45 (/64)</td><td>Deployed</td></tr><tr><td>xsi1</td><td>Ethernet</td><td>MTU = 1500 bootProto = none hwAddr = 02:82:C3:DC:2F:A0 onboot = no</td><td>192.168.3.205 (XSI1) fe80::f816:3eff:feed:81cd (/64)</td><td>Discovered</td></tr><tr><td>xsi2</td><td>Ethernet</td><td>MTU = 1500 bootProto = none hwAddr = 02:82:C3:DC:2F:A0 onboot = no</td><td>192.168.4.205 (XSI2) fe80::f816:3eff:feb0:645 (/64)</td><td>Discovered</td></tr></table> Next, press the Take Ownership button.  Converts a discovered device to a configured one. After a brief moment, the selected devices should now show a Configuration Status of “Deployed”.	xmi	Ethernet	MTU = 1500 bootProto = none onboot = yes hwAddr = 02:4D:0D:8A:D0:E7	10.240.32.27 (INTERNALXMI) 2606:b400:605:b821:4d:dff:fe8a:d0e7 (/64) fe80::4d:dff:fe8a:d0e7 (/64)	Deployed	imi	Ethernet	MTU = 1500 bootProto = none onboot = yes hwAddr = 02:17:A2:37:DB:45	192.168.100.22 (INTERNALIMI) fe80::17:a2ff:fe37:db45 (/64)	Deployed	xsi1	Ethernet	MTU = 1500 bootProto = none hwAddr = 02:82:C3:DC:2F:A0 onboot = no	192.168.3.205 (XSI1) fe80::f816:3eff:feed:81cd (/64)	Discovered	xsi2	Ethernet	MTU = 1500 bootProto = none hwAddr = 02:82:C3:DC:2F:A0 onboot = no	192.168.4.205 (XSI2) fe80::f816:3eff:feb0:645 (/64)	Discovered	
xmi	Ethernet	MTU = 1500 bootProto = none onboot = yes hwAddr = 02:4D:0D:8A:D0:E7	10.240.32.27 (INTERNALXMI) 2606:b400:605:b821:4d:dff:fe8a:d0e7 (/64) fe80::4d:dff:fe8a:d0e7 (/64)	Deployed																			
imi	Ethernet	MTU = 1500 bootProto = none onboot = yes hwAddr = 02:17:A2:37:DB:45	192.168.100.22 (INTERNALIMI) fe80::17:a2ff:fe37:db45 (/64)	Deployed																			
xsi1	Ethernet	MTU = 1500 bootProto = none hwAddr = 02:82:C3:DC:2F:A0 onboot = no	192.168.3.205 (XSI1) fe80::f816:3eff:feed:81cd (/64)	Discovered																			
xsi2	Ethernet	MTU = 1500 bootProto = none hwAddr = 02:82:C3:DC:2F:A0 onboot = no	192.168.4.205 (XSI2) fe80::f816:3eff:feb0:645 (/64)	Discovered																			
17	Repeat for remaining MPs and IPFES	Repeat Steps 15-16 for any newly created remaining MP servers.																					
18	Configure comagent connection	Execute Procedure 62 Configure ComAgent Connections (DSR + SDS Only)																					

Appendix P.1.7 Growth: Query Server (SDS Only)

S T E P #	This procedure will reference steps to configure a query server on the new virtual machine for growth scenarios. Prerequisites: • NEW Virtual Machine Created • TPD/DSR software installed Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	SDS NOAM VIP GUI: Configure the query server	Configure the query server by executing the steps referenced in the following procedures: <u>SDS query server</u>: Section 4.15.4

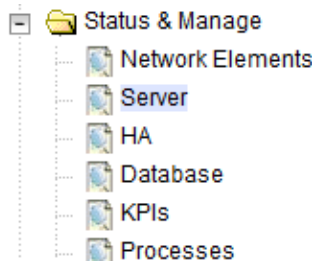
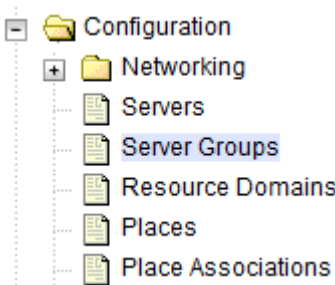
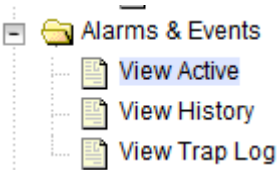
Appendix P.1.8 Post Growth Health Check

S T E P #	This procedure will provide steps verify system status and log all alarms after Growth/De-growth. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

Appendix P.1.8 Post Growth Health Check

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: <code>http://<Primary_NOAM_VIP_IP_Address></code> Login as the guiadmin user: 

Appendix P.1.8 Post Growth Health Check

2	NOAM VIP GUI: Verify Server Status	Navigate to Main Menu -> Status & Manage -> Server  Verify all Server Status is Normal (Norm) for: Alarm (Alm), Database (DB), Replication Status, and Processes (Proc). <table><tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr></table>	Appl State	Alm	DB	Reporting Status	Proc	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm
Appl State	Alm	DB	Reporting Status	Proc																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
3	NOAM VIP GUI: Verify Server Configuration	Navigate to Main Menu -> Configuration -> Server Groups  Verify the configuration data is correct for your network.																									
4	NOAM VIP GUI: Log Current Alarms	Navigate to Main Menu -> Alarms & Events -> View Active  Click on the Report button Export Report Clear Selections Save or Print this report, keep copies for future reference. Print Save Back Compare this alarm report with those gathered in procedure Appendix Q.2.1																									

Appendix P.1.8 Post Growth Health Check

4 ☐	SOAM VIP GUI: Repeat	Repeat Steps 1-3 for the SOAM

Appendix P.1.9 Post Growth Backups

S T E P #	This procedure will reference steps to backup all necessary items after a growth scenario. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Backup TVOE	Backup all TVOE host configurations by executing Section 4.17.6 Backup TVOE Configuration
2 ☐	Backup PMAC	Backup the PMAC application by executing Section 4.17.7 Backup PMAC Application
3 ☐	Backup NOAM/SOAM databases	Backup the NOAM and SOAM Databases by executing Sections 4.17.8 Backup NOAM Database and 4.17.9 Backup SOAM Database Note: Database backup on SDS SOAMs not required

Appendix P.2: De-Growth (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)

For De-growth scenarios where it is necessary to remove/delete DSR/SDS MP(SBR, SS7, IPFE)/DP servers, the following sequence of steps should be followed:

Step	Procedure(s)
Perform Backups	Appendix P.2.1
Perform system health check	Appendix P.2.2
Identify Servers which will be affected by the De-growth: DSR MP (SBR, SS7MP, IPFE)/ SDS DP	
Remove identified servers from Server Group	Appendix P.2.3
Shutdown and remove the identified server's VM.	Appendix P.2.4
Post De-Growth Health Check	Appendix P.2.5
Post De-Growth Backups	Appendix P.2.6

Appendix P.2.1 Perform Backups

S T E P #	This procedure will reference steps to backup all necessary items before a growth scenario. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Backup TVOE	Backup all TVOE host configurations by executing Section 4.17.6 Backup TVOE Configuration
2 ☐	Backup PMAC	Backup the PMAC application by executing Section 4.17.7 Backup PMAC Application
3 ☐	Backup NOAM/SOAM databases	Backup the NOAM and SOAM Databases by executing Sections 4.17.8 Backup NOAM Database and 4.17.9 Backup SOAM Database Note: Database backup on SDS SOAMs not required

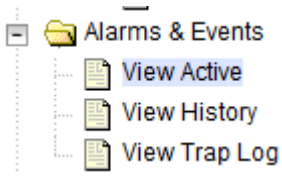
Appendix P.2.2 Perform Health Check

S T E P #	This procedure will provide steps verify system status and log all alarms. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: 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: <code>http://<Primary_NOAM_VIP_IP_Address></code> Login as the <i>guiadmin</i> user:  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.

Appendix P.2.2 Perform Health Check

2	NOAM VIP GUI: Verify Server Status	Navigate to Main Menu -> Status & Manage -> Server Status & Manage Network Elements Server HA Database KPIs Processes Verify all Server Status is Normal (Norm) for: Alarm (Alm), Database (DB), Replication Status, and Processes (Proc). <table><tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr></table> Do not proceed to with Growth/De-Growth if any of the above states are not Norm. If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the feature activation. If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed. If there are Major or Critical alarms present, these alarms should be analyzed prior to proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms	Appl State	Alm	DB	Reporting Status	Proc	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm
Appl State	Alm	DB	Reporting Status	Proc																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
3	NOAM VIP GUI: Verify Server Configuration	Navigate to Main Menu -> Configuration -> Server Groups Configuration Networking Servers Server Groups Resource Domains Places Place Associations Verify the configuration data is correct for your network.																									

Appendix P.2.2 Perform Health Check

4 ☐	NOAM VIP GUI: Log Current Alarms	Navigate to Main Menu -> Alarms & Events -> View Active  Click on the Report button  Save or Print this report, keep copies for future reference. 
5 ☐	SOAM VIP GUI: Repeat For SOAM	Repeat Steps 1-4 for the SOAM

Appendix P.2.3 Removing Server from Server Group

S T E P #	Once the server's that will be deleted have been identified, the server will first need to be removed from its server group. The following procedure will provide steps to remove a server from a server group. Warning: It is recommended that no more than one server from each server group be removed from a server group at a time. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	SOAM VIP GUI: Login Execute this step if Removing SS7MP, otherwise skip to step 10 Establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of: <code>http://<Primary_SOAM_VIP_IP_Address></code> Login as the <i>guiadmin</i> user: 

Appendix P.2.3 Removing Server from Server Group

2 ☐	SOAM VIP GUI: Disable SS7-MP Links	Execute this step if Removing SS7MP, otherwise skip to step 10 Navigate to Main Menu -> SS7/Sigtran -> Maintenance -> Links <pre> graph TD A[Main Menu] --> B[SS7/Sigtran] B --> C[Configuration] B --> D[Maintenance] D --> E[Local SCCP Users] D --> F[Remote Signaling Points] D --> G[Remote MTP3 Users] D --> H[Linksets] D --> I[Links] </pre> Disable the associated links of the identified SS7-MP: <table border="1"> <thead> <tr> <th rowspan="2">Signaling Network Element Name</th> <th rowspan="2">Link Name</th> <th rowspan="2">Link Set</th> <th rowspan="2">MP Server Hostname</th> <th rowspan="2">Admin State</th> <th colspan="2">Operational</th> <th rowspan="2">MP Server HA Status</th> </tr> <tr> <th>Status</th> <th>Reason</th> </tr> </thead> <tbody> <tr> <td>ZombieSOAM</td> <td>L1</td> <td>LS1</td> <td>ZombieSS7MP 1</td> <td>Disabled</td> <td>Down</td> <td>Disabled</td> <td>Active</td> </tr> <tr> <td>ZombieSOAM</td> <td>L10</td> <td>LS10</td> <td>ZombieSS7MP 2</td> <td>Disabled</td> <td>Down</td> <td>Disabled</td> <td>Active</td> </tr> <tr> <td>ZombieSOAM</td> <td>L11</td> <td>LS11</td> <td>ZombieSS7MP 1</td> <td>Disabled</td> <td>Down</td> <td>Disabled</td> <td>Active</td> </tr> <tr> <td>ZombieSOAM</td> <td>L12</td> <td>LS12</td> <td>ZombieSS7MP 2</td> <td>Disabled</td> <td>Down</td> <td>Disabled</td> <td>Active</td> </tr> <tr> <td>ZombieSOAM</td> <td>L13</td> <td>LS13</td> <td>ZombieSS7MP 1</td> <td>Disabled</td> <td>Down</td> <td>Disabled</td> <td>Active</td> </tr> </tbody> </table>	Signaling Network Element Name	Link Name	Link Set	MP Server Hostname	Admin State	Operational		MP Server HA Status	Status	Reason	ZombieSOAM	L1	LS1	ZombieSS7MP 1	Disabled	Down	Disabled	Active	ZombieSOAM	L10	LS10	ZombieSS7MP 2	Disabled	Down	Disabled	Active	ZombieSOAM	L11	LS11	ZombieSS7MP 1	Disabled	Down	Disabled	Active	ZombieSOAM	L12	LS12	ZombieSS7MP 2	Disabled	Down	Disabled	Active	ZombieSOAM	L13	LS13	ZombieSS7MP 1	Disabled	Down	Disabled	Active
Signaling Network Element Name	Link Name	Link Set						MP Server Hostname	Admin State		Operational		MP Server HA Status																																							
			Status	Reason																																																
ZombieSOAM	L1	LS1	ZombieSS7MP 1	Disabled	Down	Disabled	Active																																													
ZombieSOAM	L10	LS10	ZombieSS7MP 2	Disabled	Down	Disabled	Active																																													
ZombieSOAM	L11	LS11	ZombieSS7MP 1	Disabled	Down	Disabled	Active																																													
ZombieSOAM	L12	LS12	ZombieSS7MP 2	Disabled	Down	Disabled	Active																																													
ZombieSOAM	L13	LS13	ZombieSS7MP 1	Disabled	Down	Disabled	Active																																													

Appendix P.2.3 Removing Server from Server Group

3

SOAM VIP GUI:
Disable SS7-MP SCCP Users

Execute this step if Removing SS7MP, otherwise skip to step 10

Navigate to **Main Menu -> SS7/Sigtran -> Maintenance -> Local SCCP Users**

SS7/Sigtran

Configuration

Maintenance

Local SCCP Users

Remote Signaling Points

Remote MTP3 Users

Linksets

Links

Disable the associated local SCCP users of the identified SS7-MP:

Signaling Network Element Name	SSN	Local Signaling Point		Application Name	SSN Status	Up/Down Since
		Point Code	SS7 Domain			
ZombieSOAM	248	100-100-100	ANSI	MAPIWF	Disabled	2016-08-10 13:06:31 EDT
ZombieSOAM	249	111-111-111	ANSI	MAPIWF	Disabled	2016-08-10 13:06:54 EDT
ZombieSOAM	250	1-100-1	ITUI	MAPIWF	Disabled	2016-08-10 13:07:09 EDT
ZombieSOAM	251	1-101-1	ITUI	MAPIWF	Disabled	2016-08-10 13:07:17 EDT

Appendix P.2.3 Removing Server from Server Group

4

SOAM VIP GUI:
Delete SS7-MP Routes

Execute this step if Removing SS7MP, otherwise skip to step 10

Navigate to Main Menu -> SS7/Sigtran -> Configuration -> Routes

SS7/Sigtran

Configuration

Adjacent Server Groups

Local Signaling Points

Local SCCP Users

Remote Signaling Points

Remote MTP3 Users

Link Sets

Links

Routes

SCCP Options

MTP3 Options

M3UA Options

Local Congestion Options

Capacity Constraint Options

Delete the associated routes of the identified SS7-MP:

Signaling Network Element Name	SS7 Domain	Remote Point Code	Link Set	Adjacent Point Code	Relative Cost	Route Name
ZombieSOAM	ANSI	200-200-200	LS1	200-200-200	20	R1
ZombieSOAM	ANSI	200-200-200	LS2	200-200-200	20	R2
ZombieSOAM	ANSI	201-201-201	LS3	201-201-201	20	R3
ZombieSOAM	ANSI	201-201-201	LS4	201-201-201	20	R4
ZombieSOAM	ANSI	202-202-202	LS5	202-202-202	20	R5
ZombieSOAM	ANSI	202-202-202	LS6	202-202-202	20	R6
ZombieSOAM	ANSI	202-202-202	LS7	202-202-202	20	R7

DSR-8.0/8.1

434

February 2018

Appendix P.2.3 Removing Server from Server Group

5

☐

**SOAM
VIP GUI:**
Delete
SS7-MP
Links

Execute this step if Removing SS7MP, otherwise skip to step 10

Navigate to **Main Menu -> SS7/Sigtran -> Configuration -> Links**

SS7/Sigtran

Configuration

Adjacent Server Groups

Local Signaling Points

Local SCCP Users

Remote Signaling Points

Remote MTP3 Users

Link Sets

Links

Routes

SCCP Options

MTP3 Options

M3UA Options

Local Congestion Options

Capacity Constraint Options

Delete the associated links of the identified SS7-MP:

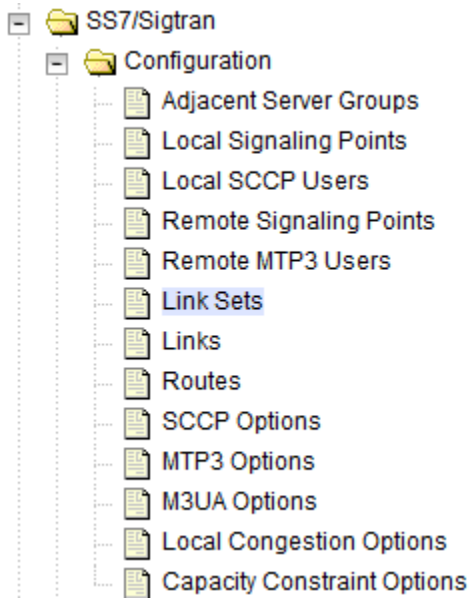
Signaling Network Element Name	Link Name	Link Set	Association
ZombieSOAM	L1	LS1	pc9111729_046
ZombieSOAM	L2	LS2	pc9111729_0461
ZombieSOAM	L3	LS3	pc9111729_0462
ZombieSOAM	L4	LS4	pc9111729_0463
ZombieSOAM	L5	LS5	pc9111729_1
ZombieSOAM	L6	LS6	pc9111729_11

DSR-8.0/8.1

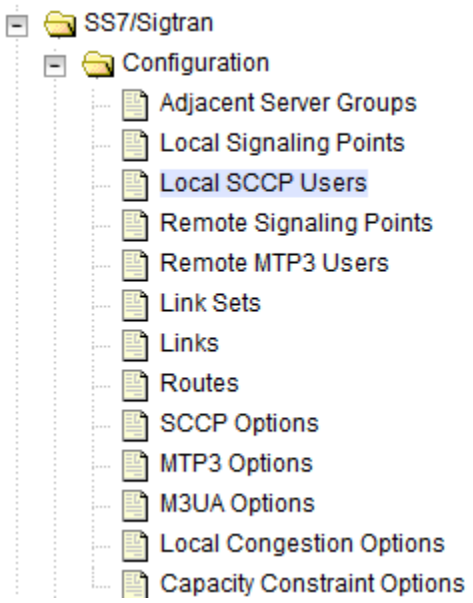
435

February 2018

Appendix P.2.3 Removing Server from Server Group

6 ☐	SOAM VIP GUI: Delete SS7-MP Link Sets	Execute this step if Removing SS7MP, otherwise skip to step 10 Navigate to Main Menu -> SS7/Sigtran -> Configuration -> Link Sets  Delete the associated link sets of the identified SS7-MP: <table border="1"> <thead> <tr> <th>Signaling Network Element Name</th> <th>Link Set Name</th> <th>Mode</th> <th>Local Signaling Point</th> <th>SS7 Domain</th> <th>LSP Point Code</th> <th>Adjacent Remote Point Code</th> <th>Routing Context</th> </tr> </thead> <tbody> <tr> <td>ZombieSOAM</td> <td>LS1</td> <td>AS->SG</td> <td>ANSI_100_100_100</td> <td>ANSI</td> <td>All</td> <td>200-200-200</td> <td>----</td> </tr> <tr> <td>ZombieSOAM</td> <td>LS2</td> <td>AS->SG</td> <td>ANSI_111_111_111</td> <td>ANSI</td> <td>All</td> <td>200-200-200</td> <td>----</td> </tr> <tr> <td>ZombieSOAM</td> <td>LS3</td> <td>AS->SG</td> <td>ANSI_100_100_100</td> <td>ANSI</td> <td>All</td> <td>201-201-201</td> <td>----</td> </tr> <tr> <td>ZombieSOAM</td> <td>LS4</td> <td>AS->SG</td> <td>ANSI_111_111_111</td> <td>ANSI</td> <td>All</td> <td>201-201-201</td> <td>----</td> </tr> <tr> <td>ZombieSOAM</td> <td>LS5</td> <td>AS->SG</td> <td>ANSI_100_100_100</td> <td>ANSI</td> <td>All</td> <td>202-202-202</td> <td>----</td> </tr> <tr> <td>ZombieSOAM</td> <td>LS6</td> <td>AS->SG</td> <td>ANSI_111_111_111</td> <td>ANSI</td> <td>All</td> <td>202-202-202</td> <td>----</td> </tr> </tbody> </table>	Signaling Network Element Name	Link Set Name	Mode	Local Signaling Point	SS7 Domain	LSP Point Code	Adjacent Remote Point Code	Routing Context	ZombieSOAM	LS1	AS->SG	ANSI_100_100_100	ANSI	All	200-200-200	----	ZombieSOAM	LS2	AS->SG	ANSI_111_111_111	ANSI	All	200-200-200	----	ZombieSOAM	LS3	AS->SG	ANSI_100_100_100	ANSI	All	201-201-201	----	ZombieSOAM	LS4	AS->SG	ANSI_111_111_111	ANSI	All	201-201-201	----	ZombieSOAM	LS5	AS->SG	ANSI_100_100_100	ANSI	All	202-202-202	----	ZombieSOAM	LS6	AS->SG	ANSI_111_111_111	ANSI	All	202-202-202	----
		Signaling Network Element Name	Link Set Name	Mode	Local Signaling Point	SS7 Domain	LSP Point Code	Adjacent Remote Point Code	Routing Context																																																	
ZombieSOAM	LS1	AS->SG	ANSI_100_100_100	ANSI	All	200-200-200	----																																																			
ZombieSOAM	LS2	AS->SG	ANSI_111_111_111	ANSI	All	200-200-200	----																																																			
ZombieSOAM	LS3	AS->SG	ANSI_100_100_100	ANSI	All	201-201-201	----																																																			
ZombieSOAM	LS4	AS->SG	ANSI_111_111_111	ANSI	All	201-201-201	----																																																			
ZombieSOAM	LS5	AS->SG	ANSI_100_100_100	ANSI	All	202-202-202	----																																																			
ZombieSOAM	LS6	AS->SG	ANSI_111_111_111	ANSI	All	202-202-202	----																																																			

Appendix P.2.3 Removing Server from Server Group

7 ☐	SOAM VIP GUI: Delete SS7-MP Local SCCP Users	Execute this step if Removing SS7MP, otherwise skip to step 10 Navigate to Main Menu -> SS7/Sigtran -> Configuration -> Local SCCP Users  Delete the associated Local SCCP Users from the identified SS7-MP: <table border="1" data-bbox="397 1050 1421 1396"> <thead> <tr> <th rowspan="2">Signaling Network Element Name</th> <th rowspan="2">SSN</th> <th colspan="2">Local Signaling Point</th> <th rowspan="2">Application Name</th> </tr> <tr> <th>SS7 Domain</th> <th>Point Code</th> </tr> </thead> <tbody> <tr> <td>ZombieSOAM</td> <td>248</td> <td>ANSI</td> <td>100-100-100</td> <td>MAPIWF</td> </tr> <tr> <td>ZombieSOAM</td> <td>249</td> <td>ANSI</td> <td>111-111-111</td> <td>MAPIWF</td> </tr> <tr> <td>ZombieSOAM</td> <td>250</td> <td>ITUI</td> <td>1-100-1</td> <td>MAPIWF</td> </tr> <tr> <td>ZombieSOAM</td> <td>251</td> <td>ITUI</td> <td>1-101-1</td> <td>MAPIWF</td> </tr> </tbody> </table>	Signaling Network Element Name	SSN	Local Signaling Point		Application Name	SS7 Domain	Point Code	ZombieSOAM	248	ANSI	100-100-100	MAPIWF	ZombieSOAM	249	ANSI	111-111-111	MAPIWF	ZombieSOAM	250	ITUI	1-100-1	MAPIWF	ZombieSOAM	251	ITUI	1-101-1	MAPIWF
Signaling Network Element Name	SSN	Local Signaling Point			Application Name																								
		SS7 Domain	Point Code																										
ZombieSOAM	248	ANSI	100-100-100	MAPIWF																									
ZombieSOAM	249	ANSI	111-111-111	MAPIWF																									
ZombieSOAM	250	ITUI	1-100-1	MAPIWF																									
ZombieSOAM	251	ITUI	1-101-1	MAPIWF																									

Appendix P.2.3 Removing Server from Server Group

8

SOAM VIP GUI:

Delete SS7-MP Local Signaling Points

Execute this step if Removing SS7MP, otherwise skip to step 10

Navigate to Main Menu -> SS7/Sigtran -> Configuration -> Local Signaling Points

SS7/Sigtran

Configuration

Adjacent Server Groups

Local Signaling Points

Local SCCP Users

Remote Signaling Points

Remote MTP3 Users

Link Sets

Links

Routes

SCCP Options

MTP3 Options

M3UA Options

Local Congestion Options

Capacity Constraint Options

Delete the associated Local signaling points from the identified SS7-MP:

Signaling Network Element Name	Local Signaling Point Name	SS7 Domain	MTP True Point Code	MTP Capability Point Code(s)	ServerGroup(s)
ZombieSOAM	ANSI_100_100_100	ANSI	100-100-100	----	ZombieSS7SG
ZombieSOAM	ANSI_111_111_111	ANSI	111-111-111	----	ZombieSS7SG
ZombieSOAM	ITUI_1_100_1	ITUI	1-100-1	----	ZombieSS7SG
ZombieSOAM	ITUI_1_101_1	ITUI	1-101-1	----	ZombieSS7SG

9

SOAM VIP GUI:

Disable SS7-MP transports

Execute this step if Removing SS7MP, otherwise skip to step 10

Navigate to Main Menu -> Transport Manager -> Maintenance -> Transport

Transport Manager

Configuration

Maintenance

Transport

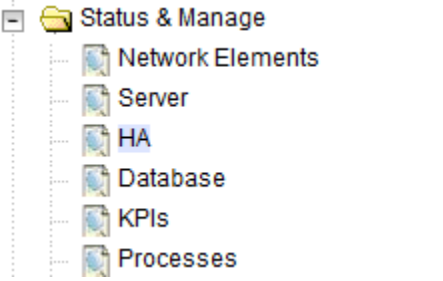
Disable the associated transports from the identified SS7-MP:

Signaling Network Element Name	MP Server Hostname	Adapter	Transport Name	Transport Protocol	Transport Type	Adjacent Node	Admin State	Operational Status	Operational Reason	Up/Down Since
ZombieSOAM	ZombieSS7MP1	M3UA	pc9111729_046	SCTP	Initiator	pc9111729_net046	Disabled	Down	Disabled	2016-08-10 09:57:25 EDT
ZombieSOAM	ZombieSS7MP2	M3UA	pc9111729_0461	SCTP	Initiator	pc9111729_net0461	Disabled	Down	Disabled	2016-08-10 10:02:36 EDT

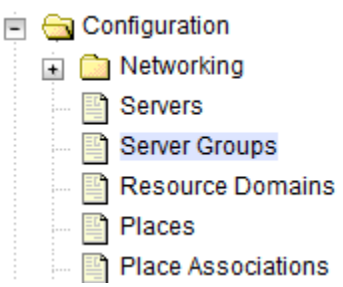
Appendix P.2.3 Removing Server from Server Group

10 ☐	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: <code>http://<Primary_NOAM_VIP_IP_Address></code> Login as the <i>guiadmin</i> user: 

Appendix P.2.3 Removing Server from Server Group

11	NOAM VIP GUI: Set Server to OOS	Navigate to Main Menu -> Status & Manage -> HA  Click Edit Set the server's <i>Max Allowed HA Role</i> to OOS Click Ok

Appendix P.2.3 Removing Server from Server Group

12 ☐	NOAM VIP GUI: Remove Server From Server Group	Navigate to Main Menu -> Configuration -> Server Groups  Select the server group for which the server from step 2 that was placed OOS. Click Edit Insert Edit Delete Report Uncheck the server from step 2 from the <i>SG Inclusion</i> column: <table border="1"> <tr> <td>Server Group Name *</td> <td>ZombieSS7SG1</td> <td>Unique identifier used to label a with a digit.] [A value is required.]</td> </tr> <tr> <td>Level *</td> <td>C</td> <td>Select one of the Levels support</td> </tr> <tr> <td>Parent *</td> <td>ZombieSOAM</td> <td>Select an existing Server Group [</td> </tr> <tr> <td>Function *</td> <td>SS7-IWF</td> <td>Select one of the Functions supp</td> </tr> <tr> <td>WAN Replication Connection Count</td> <td>1</td> <td>Specify the number of TCP conn</td> </tr> <tr> <td colspan="3"> ZombieSOAM ☐ Prefer Network Element as spare </td> </tr> <tr> <td>Server</td> <td>SG Inclusion</td> <td>Preferred HA Role</td> </tr> <tr> <td>ZombieSS7MP1</td> <td>☐ Include in SG</td> <td>☐ Prefer server as spare</td> </tr> <tr> <td colspan="3">VIP Assianment</td> </tr> </table> Click Ok Ok Apply Cancel	Server Group Name *	ZombieSS7SG1	Unique identifier used to label a with a digit.] [A value is required.]	Level *	C	Select one of the Levels support	Parent *	ZombieSOAM	Select an existing Server Group [	Function *	SS7-IWF	Select one of the Functions supp	WAN Replication Connection Count	1	Specify the number of TCP conn	ZombieSOAM ☐ Prefer Network Element as spare			Server	SG Inclusion	Preferred HA Role	ZombieSS7MP1	☐ Include in SG	☐ Prefer server as spare	VIP Assianment		
Server Group Name *	ZombieSS7SG1	Unique identifier used to label a with a digit.] [A value is required.]																											
Level *	C	Select one of the Levels support																											
Parent *	ZombieSOAM	Select an existing Server Group [																											
Function *	SS7-IWF	Select one of the Functions supp																											
WAN Replication Connection Count	1	Specify the number of TCP conn																											
ZombieSOAM ☐ Prefer Network Element as spare																													
Server	SG Inclusion	Preferred HA Role																											
ZombieSS7MP1	☐ Include in SG	☐ Prefer server as spare																											
VIP Assianment																													

Appendix P.2.4 Deleting Server/Server Group

S T E P #	Once the server has been removed from the server group, it is now safe to delete the server. The server group can also be deleted if there are no more servers associated with it. The following procedure will provide steps to delete a server, and delete a server group. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: 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: <code>http://<Primary_NOAM_VIP_IP_Address></code> Login as the <i>guiadmin</i> user: 

Appendix P.2.4 Deleting Server/Server Group

2

☐

NOAM VIP GUI:
Delete the Server

Navigate to **Main Menu -> Configuration -> Servers**

Select the server that has been previously removed from the server group

ZombieSOAM2	System OAM	
ZombieDAMP1	MP	
ZombieDAMP2	MP	
ZombieSS7MP1	MP	
ZombieSS7MP2	MP	
ZombieIPFE1	MP	
ZombieIPFE2	MP	

Select **Delete**

Confirm Deletion

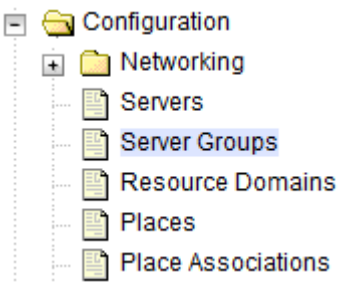
Delete Server(s) : ZombieSS7MP1?

3

**NOAM
VIP GUI:**
Delete
Server
Group

If all servers have been removed from a server group, it is now safe to delete the server group.

Navigate to **Main Menu -> Configuration -> Server Groups**



Select the empty server group

Main Menu: Configuration -> Server Groups

Server Group Name	Level	Parent	Function	Connection Count	Servers						
SS7MP	C	ZombieSOAM	SS7-IWF	1							
ZombieDAMP	C	ZombieSOAM	DSR (multi-active cluster)	1	Network Element: Zombie <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Server</th> <th style="width: 50%;">Node</th> </tr> </thead> <tbody> <tr> <td>ZombieDAMP1</td> <td></td> </tr> <tr> <td>ZombieDAMP2</td> <td></td> </tr> </tbody> </table>	Server	Node	ZombieDAMP1		ZombieDAMP2	
Server	Node										
ZombieDAMP1											
ZombieDAMP2											

Select **Delete**

Insert
Edit
Delete
Report

Confirm Deletion

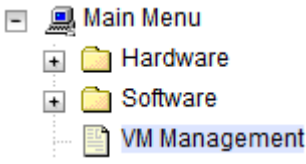
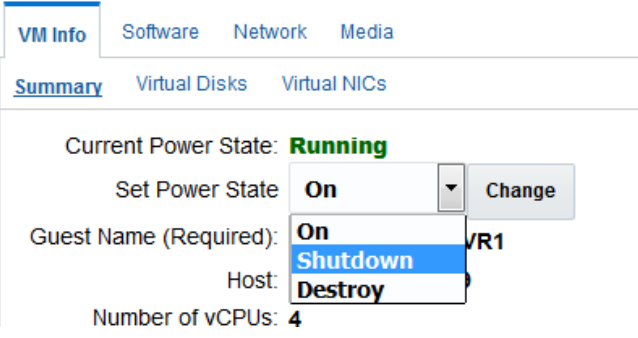
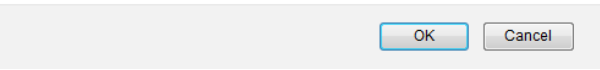
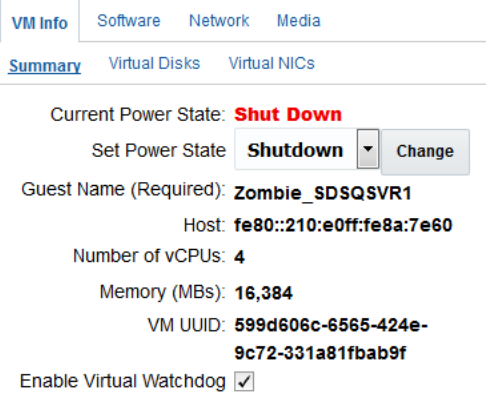
Delete Server Group : SS7MP?

OK
Cancel

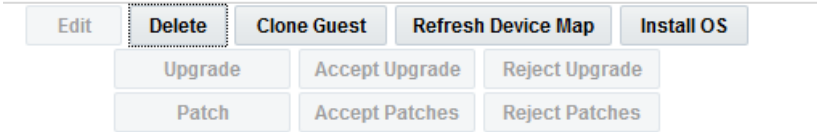
Appendix P.2.5 Deleting the server VM

S T E P #	Once the server's that are being deleted have been identified, placed in OOS, and removed the from the server group. It is now safe to shut down and delete the VM for which the server is located. The following procedure will provide steps to remove a VM from a TVOE Host Warning: It is recommended that a careful approach be taken with this procedure and that the server to VM mapping be confirmed before proceeding. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PMAC GUI: Login Open web browser and navigate to the PMAC GUI, Login as Guiadmin user: <code>https://<pmac_network_ip></code> 

Appendix P.2.5 Deleting the server VM

2 ☐	PMAC GUI: Shutdown the VM	Navigate to Main Menu -> VM Management  Expand the view (<i>if needed</i>) of the Rack Mount Server for which the server you are moving/deleting is located. Shutdown the VM by setting the <i>Current Power State</i> to Shutdown: View guest Zombie_SDSQSVR1  Click Change Select OK for the following prompt: It may not always be possible to shutdown a guest or to do so in a timely manner. You may monitor the power state and opt to destroy the guest rather than shut it down. Are you sure you want to attempt to shutdown this guest?  The <i>Current Power State</i> should now display Shutdown: View guest Zombie_SDSQSVR1 

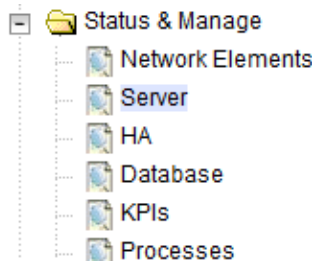
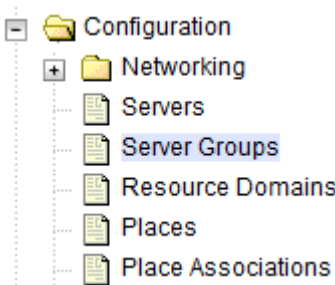
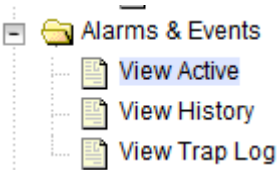
Appendix P.2.5 Deleting the server VM

3 ☐	PMAC GUI: Delete the VM	Once the server has been shutdown, select the VM from step 2. Verify the <i>current power state</i> is Shutdown as listed in step 2. Select Delete  Click OK to confirm deletion Are you sure you want to delete guest Zombie_SDSQSVR1? 

Appendix P.2.6 Post De-Growth Health Check

S T E P #	This procedure will provide steps verify system status and log all alarms after De-growth. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: 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: <code>http://<Primary_NOAM_VIP_IP_Address></code> Login as the guiadmin user: 

Appendix P.2.6 Post De-Growth Health Check

2	NOAM VIP GUI: Verify Server Status	Navigate to Main Menu -> Status & Manage -> Server  Verify all Server Status is Normal (Norm) for: Alarm (Alm), Database (DB), Replication Status, and Processes (Proc). <table><tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr></table>	Appl State	Alm	DB	Reporting Status	Proc	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm
Appl State	Alm	DB	Reporting Status	Proc																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
3	NOAM VIP GUI: Verify Server Configuration	Navigate to Main Menu -> Configuration -> Server Groups  Verify the configuration data is correct for your network.																									
4	NOAM VIP GUI: Log Current Alarms	Navigate to Main Menu -> Alarms & Events -> View Active  Click on the Report button Export Report Clear Selections Save or Print this report, keep copies for future reference. Print Save Back Compare this alarm report with those gathered in procedure Appendix P.2.2																									

Appendix P.2.6 Post De-Growth Health Check

5 ☐	SOAM VIP GUI: Repeat	Repeat Steps 1-4 for the SOAM

Appendix P.2.7 Post De-Growth Backups

S T E P #	This procedure will reference steps to backup all necessary items after a De-growth scenario. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Backup TVOE	Backup all TVOE host configurations by executing Section 4.17.6 Backup TVOE Configuration
2 ☐	Backup PMAC	Backup the PMAC application by executing Section 4.17.7 Backup PMAC Application
3 ☐	Backup NOAM/SOAM databases	Backup the NOAM and SOAM Databases by executing Sections 4.17.8 Backup NOAM Database and 4.17.9 Backup SOAM Database Note: Database backup on SDS SOAMs not required

Appendix P.3: Re-Shuffle (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)

For Growth/De-growth scenarios where it is necessary to move or re-shuffle DSR/SDS servers to different TVOE hosts, the following sequence of steps should be followed:

Step	Procedure(s)
Perform Backups	Appendix P.3.1
Perform system health check	Appendix P.3.2
Add new rack mount server if necessary (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)	Appendix P.3.3
Identify Servers which will be affected by the Growth: • NOAM • SOAM • DSR MP (SBR, SS7MP, IPFE)/ SDS DP • Query Server • PMAC	
Remove identified servers from Server Group	Appendix P.3.4
Shutdown and remove the identified server's VM.	Appendix P.3.5
Identify the new Rack Mount Server for which the previously removed server will be placed.	
Create and Configure the VMs on the new Rack Mount Servers	Appendix P.3.6
Configure Servers in new VM locations	NOAM/DR-NOAM (DSR/SDS): Appendix P.3.7 SOAM (DSR/SDS): Appendix P.3.8 MP/DP (DSR/SDS): Appendix P.3.9 Query Server (SDS): Appendix P.3.10 iDIH: Appendix P.3.11 PMAC: Appendix P.3.12 Redundant PMAC: Appendix P.3.13
Post Move/Re-Shuffle Health Check	Appendix P.3.14
Post Move/Re-Shuffle Backups	Appendix P.3.15

Appendix P.3.1 Perform Backups

S T E P #	This procedure will reference steps to backup all necessary items before a Re-Shuffle scenario. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Backup TVOE	Backup all TVOE host configurations by executing Section 4.17.6 Backup TVOE Configuration
2 ☐	Backup PMAC	Backup the PMAC application by executing Section 4.17.7 Backup PMAC Application
3 ☐	Backup NOAM/SOAM databases	Backup the NOAM and SOAM Databases by executing Sections 4.17.8 Backup NOAM Database and 4.17.9 Backup SOAM Database Note: Database backup on SDS SOAMs not required

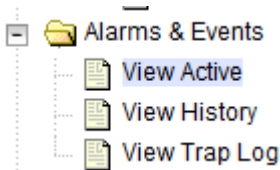
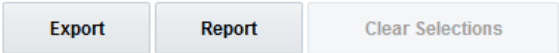
Appendix P.3.2 Perform Health Check

S T E P #	This procedure will provide steps verify system status and log all alarms. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: 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: <code>http://<Primary_NOAM_VIP_IP_Address></code> Login as the <i>guiadmin</i> user: 

Appendix P.3.2 Perform Health Check

2	NOAM VIP GUI: Verify Server Status	Navigate to Main Menu -> Status & Manage -> Server Status & Manage Network Elements Server HA Database KPIs Processes Verify all Server Status is Normal (Norm) for: Alarm (Alm), Database (DB), Replication Status, and Processes (Proc). <table><tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr></table> Do not proceed to with Growth/De-Growth if any of the above states are not Norm. If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the feature activation. If the Alarm (Alm) status is not Norm but only Minor alarms are present, it is acceptable to proceed. If there are Major or Critical alarms present, these alarms should be analyzed prior to proceeding with the feature activation. The activation may be able to proceed in the presence of certain Major or Critical alarms	Appl State	Alm	DB	Reporting Status	Proc	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm
Appl State	Alm	DB	Reporting Status	Proc																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
3	NOAM VIP GUI: Verify Server Configuration	Navigate to Main Menu -> Configuration -> Server Groups Configuration Networking Servers Server Groups Resource Domains Places Place Associations Verify the configuration data is correct for your network.																									

Appendix P.3.2 Perform Health Check

4 ☐	NOAM VIP GUI: Log Current Alarms	Navigate to Main Menu -> Alarms & Events -> View Active  Click on the Report button  Save or Print this report, keep copies for future reference. 
5 ☐	SOAM VIP GUI: Repeat For SOAM	Repeat Steps 1-4 for the SOAM

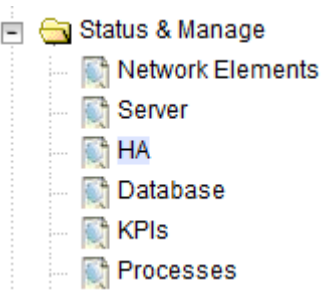
Appendix P.3.3 Adding a new TVOE Server

S T E P #	This procedure will provide steps to add a new rack mount server if necessary. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Add/Configure Additional Rack Mount Servers	Follow the steps in Section Install TVOE on Additional Rack Mount Servers and Section Configure TVOE on Additional Rack Mount Servers to install and configure TVOE on additional rack mount servers.

Appendix P.3.4 Placing Server in OOS

S T E P #	Once the server's that will be moved has been identified, the server will first need to be placed in HA OOS. This procedure will provide steps to place the server in OOS HA state. Warning: It is recommended that no more than one server from each server be placed in OOS at a time. Warning: For NOAM and SOAM servers, during the process of moving/"Re-Shuffling"; these servers are done one at a time. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: 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: <code>http://<Primary_NOAM_VIP_IP_Address></code> Login as the guiadmin user: 

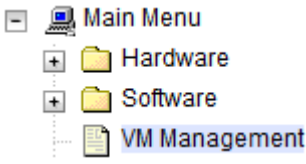
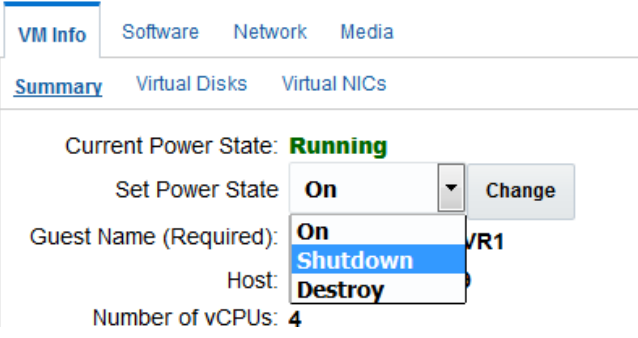
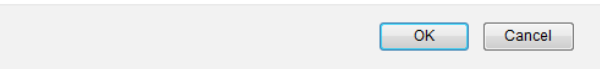
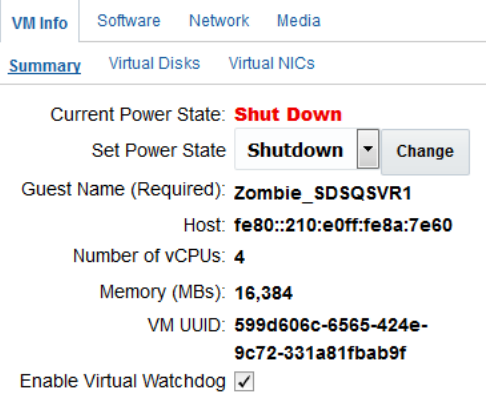
Appendix P.3.4 Placing Server in OOS

2 ☐	NOAM VIP GUI: Set Server to OOS	Navigate to Main Menu -> Status & Manage -> HA  Click Edit Set the server's <i>Max Allowed HA Role</i> to OOS <table border="1" data-bbox="483 751 1393 1039"> <thead> <tr> <th>Hostname</th> <th>Max Allowed HA Role</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ZombieNOAM1</td> <td>Active</td> <td>The maximum desired HA Role for ZombieNOAM1</td> </tr> <tr> <td>ZombieNOAM2</td> <td>Active</td> <td>The maximum desired HA Role for ZombieNOAM2</td> </tr> </tbody> </table> Click Ok Ok Cancel	Hostname	Max Allowed HA Role	Description	ZombieNOAM1	Active	The maximum desired HA Role for ZombieNOAM1	ZombieNOAM2	Active	The maximum desired HA Role for ZombieNOAM2
Hostname	Max Allowed HA Role	Description									
ZombieNOAM1	Active	The maximum desired HA Role for ZombieNOAM1									
ZombieNOAM2	Active	The maximum desired HA Role for ZombieNOAM2									

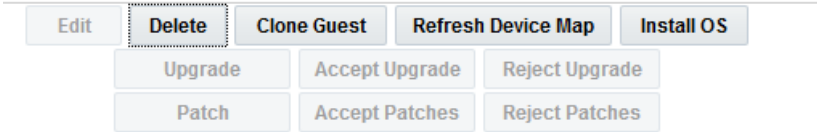
Appendix P.3.5 Deleting the server VM

S T E P #	Once the server's that are being deleted or moved have been identified, and placed in OOS. It is now safe to shut down and delete the VM for which the server is located. The following procedure will provide steps to remove a VM from a TVOE Host Warning: It is recommended that a careful approach be taken with this procedure and that the server to VM mapping be confirmed before proceeding. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PMAC GUI: Login Open web browser and navigate to the PMAC GUI, Login as Guiadmin user: <a href="https://<pmac_network_ip>">https://<pmac_network_ip> 

Appendix P.3.5 Deleting the server VM

2 ☐	PMAC GUI: Shutdown the VM	Navigate to Main Menu -> VM Management  Expand the view (<i>if needed</i>) of the Rack Mount Server for which the server you are moving/deleting is located. Shutdown the VM by setting the <i>Current Power State</i> to Shutdown: View guest Zombie_SDSQSVR1  Click Change Select OK for the following prompt: It may not always be possible to shutdown a guest or to do so in a timely manner. You may monitor the power state and opt to destroy the guest rather than shut it down. Are you sure you want to attempt to shutdown this guest?  The <i>Current Power State</i> should now display Shutdown: View guest Zombie_SDSQSVR1 

Appendix P.3.5 Deleting the server VM

3 ☐	PMAC GUI: Delete the VM	Once the server has been shutdown, select the VM from step 2. Verify the <i>current power state</i> is Shutdown as listed in step 2. Select Delete  Click OK to confirm deletion Are you sure you want to delete guest Zombie_SDSQSVR1? 

Appendix P.3.6 Moving/Re-Shuffle: Creating/Configuring Virtual Machines

S T E P #	Before starting this procedure, it is assumed the server has been identified, placed in OOS, and its corresponding VM deleted. This procedure will reference steps to create the new VM, load the software, and configure the server. Note: Before beginning this procedure, it is recommended that proper VM mapping has been determined to maintain performance efficiency as mentioned in Section 4.10. Note: It is assumed that the PMAC already contains the needed TPD, DSR, and SDS ISO software. If necessary, execute Procedure 14. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	PMAC GUI: Create Virtual Machine	To create a virtual machine for all applicable servers, follow the steps outlined in Section Virtual Machine/Network Fast Deployment
2 ☐	TVOE HOST: Execute CPU Pinning	Execute Section CPU Pinning to allocate CPU resources on each new VM added.

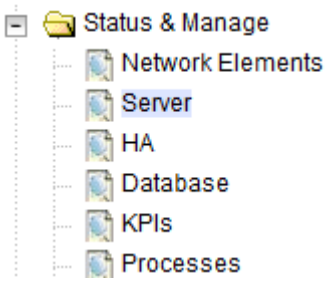
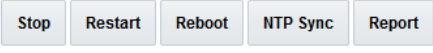
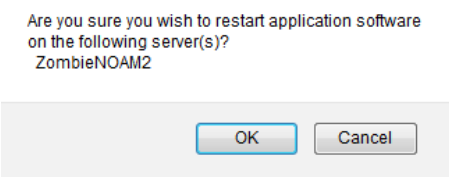
Appendix P.3.7 Moving/Re-Shuffle: NOAM/DR-NOAM

S T E P #	This procedure will reference steps to configure an NOAM/DR-NOAM on the new virtual machine for VM re-shuffling scenarios. Prerequisites: • NOAM/DR-NOAM has been Identified • Placed in OOS • OLD Virtual Machine Deleted • NEW Virtual Machine Created • TPD/DSR software installed Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	NOAM VIP GUI: Configure the 2nd NOAM/DR-NOAM Configure the 2nd NOAM/DR-NOAM by executing the steps referenced in the following procedures: <u>DSR NOAM</u>: Procedure 17 4: Steps 1-2, 4-7, 8(<i>Optional-NetBackup</i>), 9 <u>DSR DR-NOAM</u>: Procedure 253: Steps 4-8, 9(<i>Optional-NetBackup</i>), 10 <u>SDS NOAM</u>: Procedure 37 : Steps 1-2, 4-7, 8(<i>Optional-NetBackup</i>), 9 <u>SDS DR-NOAM</u>: Procedure 43: Steps 4-8, 9(<i>Optional-NetBackup</i>), 10

Appendix P.3.7 Moving/Re-Shuffle: NOAM/DR-NOAM

2 ☐	NOAM VIP: Establish GUI Session	Establish a GUI session on the NOAM by using the XMI VIP address: https://<NOAM_VIP_IP_Address> Login as user guiadmin.  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.
3 ☐	NOAM VIP: Wait for Remote Database Alarm to Clear	Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding. Navigate to Main menu->Alarms & Events->View Active

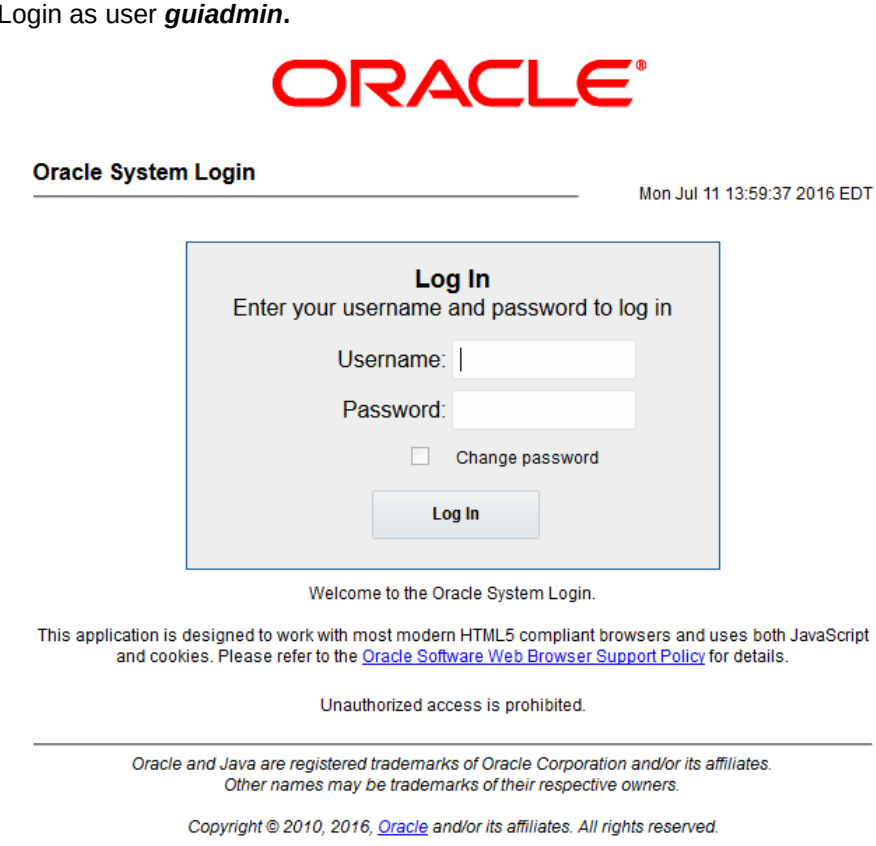
Appendix P.3.7 Moving/Re-Shuffle: NOAM/DR-NOAM

4 ☐	NOAM GUI: Restart 2nd NOAM/DR- NOAM Server	Navigate to Main menu -> Status & Manage -> Server  Select the 2nd NOAM/DR-NOAM server. Select the Restart button.  Answer OK to the confirmation popup. 
5 ☐	NOAM GUI: Activate Optional Features	If there are any optional features currently activated, the feature activation procedures will need to be run again. Refer to Section Optional Features

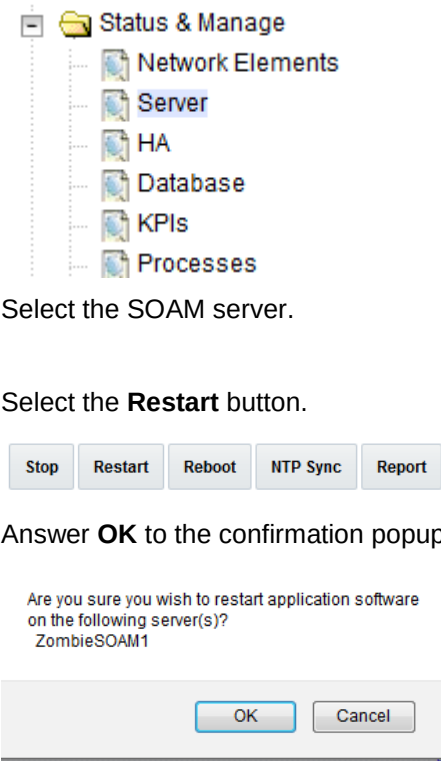
Appendix P.3.8 Moving/Re-Shuffle: SOAM

S T E P #	This procedure will reference steps to configure an SOAM on the new virtual machine for VM re-shuffling scenarios. Prerequisites: • SOAM has been Identified • Placed in OOS • OLD Virtual Machine Deleted • NEW Virtual Machine Created • TPD/DSR software installed Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1	NOAM VIP GUI: Configure the SOAM	Configure the SOAM by executing the steps referenced in the following procedures: <u>DSR SOAM: Procedure 25:</u> Steps 1-3, 5-9, 11(<i>Optional-NetBackup</i>) <u>SDS DP SOAM: Procedure 47:</u> Steps 1-3, 5-9

Appendix P.3.8 Moving/Re-Shuffle: SOAM

2 ☐	NOAM VIP: Establish GUI Session	Establish a GUI session on the NOAM by using the XMI VIP address: https://<NOAM_VIP_IP_Address> Login as user guiadmin.  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.
3 ☐	NOAM VIP: Wait for Remote Database Alarm to Clear	Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding. Navigate to Main menu->Alarms & Events->View Active

Appendix P.3.8 Moving/Re-Shuffle: SOAM

4 ☐	NOAM GUI: Restart the SOAM Server	Navigate to Main menu -> Status & Manage -> Server  Select the SOAM server. Select the Restart button. Answer OK to the confirmation popup.
5 ☐	NOAM GUI: Activate Optional Features	If there are any optional features currently activated, the feature activation procedures will need to be run again. Refer to Section Optional Features.

Appendix P.3.9 Moving/Re-Shuffle: MP/DP

S T E P #	This procedure will reference steps to configure an MP/DP on the new virtual machine for VM re-shuffling scenarios. Prerequisites: • MP/DP has been Identified • Placed in OOS • OLD Virtual Machine Deleted • NEW Virtual Machine Created • TPD/DSR software installed Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	NOAM VIP GUI: Configure the MP/DP	Configure the MP/DP by executing the steps referenced in the following procedures: <u>DSR MP</u>: Procedure 30: Steps 1-2, 7, 9, 10-12, 13-14(Optional), 15 <u>SDS DP</u>: Procedure 49: Steps 1-2, 5-9

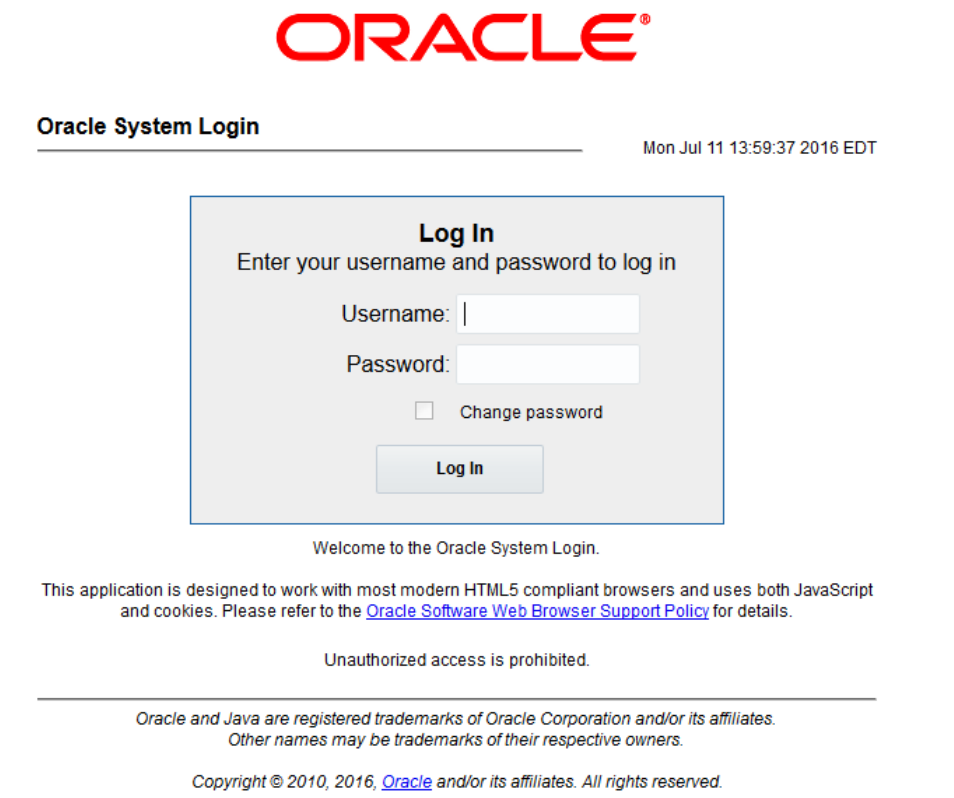
Appendix P.3.9 Moving/Re-Shuffle: MP/DP

2 ☐	NOAM VIP: Establish GUI Session	Establish a GUI session on the NOAM by using the XMI VIP address: <code>https://<NOAM_VIP_IP_Address></code> Login as user guiadmin. 

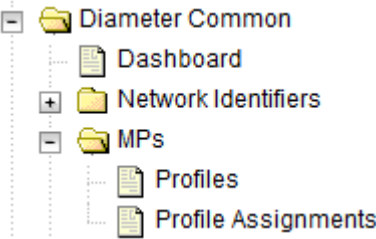
Appendix P.3.9 Moving/Re-Shuffle: MP/DP

3 ☐	NOAM VIP GUI: [PCA / DCA ONLY] Edit the MP Server Group and add Preferred Spares for Site Redundancy (Optional)	If Two Site Redundancy for the Policy and Charging SBR Server Group OR Session Binding Repository is wanted, add a MP server that is physically located in a separate site (location) to the Server Group by clicking the Include in SG checkbox and also check the Preferred Spare checkbox. <table border="1" data-bbox="493 432 1427 562"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>ZombieSBRsp</td><td>☒ Include in SG</td><td>☒ Prefer server as spare</td></tr> </tbody> </table> If Three Site Redundancy for the SBR MP Server Group is wanted, add two SBR MP servers that are both physically located in separate sites (<i>location</i>) to the Server Group by clicking the Include in SG checkbox and also check the Preferred Spare checkbox for both servers. Note: The Preferred Spare servers should be different sites from the original server and should not be in the same site. There should be servers from three separate sites (locations). Note: There must first be Non-Preferred spare present the server group before adding the preferred spare. For more information about Site Redundancy for Policy and Charging SBR Server Groups/ Session Binding Repository Server Groups, see the Terminology section. Select OK to save	Server	SG Inclusion	Preferred HA Role	ZombieSBRsp	☒ Include in SG	☒ Prefer server as spare
Server	SG Inclusion	Preferred HA Role						
ZombieSBRsp	☒ Include in SG	☒ Prefer server as spare						
4 ☐	NOAM VIP: Wait for Remote Database Alarm to Clear	Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding. Navigate to Main menu->Alarms & Events->View Active						

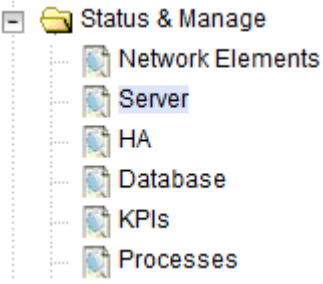
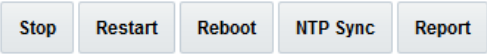
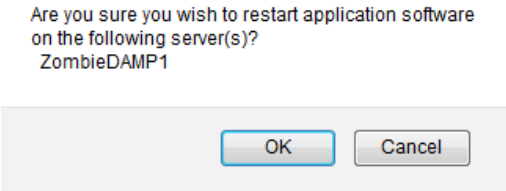
Appendix P.3.9 Moving/Re-Shuffle: MP/DP

5 ☐	SOAM VIP GUI: Login	If not already done, establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of: <code>https://<Primary_SOAM_VIP_IP_Address></code> Login to the SOAM GUI as the <i>guiadmin</i> user: 

Appendix P.3.9 Moving/Re-Shuffle: MP/DP

6 ☐	SOAM VIP GUI: Assign Profiles to DA-MPs from SOAM GUI.	Navigate to Main Menu -> Diameter Common ->MPs -> Profiles Assignments  Refer to the DA-MP section. (If the site has both DSR and MAP-IWF server groups, you will see both a DA-MP section and an SS7-MP section) Main Menu: Diameter Common -> MPs -> Profile Assignments <table border="1"> <thead> <tr> <th>DA-MP</th> <th>MP Profile</th> <th>current value</th> </tr> </thead> <tbody> <tr> <td>ZombieDAMP1</td> <td>VM:10K_MPS</td> <td>The current MP Profile for ZombieDAMP1 is VM:10K_MPS. Virtualized DA-MP rated at 10K MPS for all configurations [A value is required.]</td> </tr> <tr> <td>ZombieDAMP2</td> <td>VM:10K_MPS</td> <td>The current MP Profile for ZombieDAMP2 is VM:10K_MPS. Virtualized DA-MP rated at 10K MPS for all configurations [A value is required.]</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>SS7-MP</th> <th>MP Profile</th> <th>current value</th> </tr> </thead> <tbody> <tr> <td>ZombieSS7MP1</td> <td>VM:MD-IWF</td> <td>The current MP Profile for ZombieSS7MP1 is VM:MD-IWF. Virtualized SS7-MP running MD-IWF application [A value is required.]</td> </tr> <tr> <td>ZombieSS7MP2</td> <td>VM:MD-IWF</td> <td>The current MP Profile for ZombieSS7MP2 is VM:MD-IWF. Virtualized SS7-MP running MD-IWF application [A value is required.]</td> </tr> </tbody> </table> Assign Cancel For each MP, select the proper profile assignment based on the function each MP will serve: <table border="1"> <thead> <tr> <th>Profile Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>VM:10K_MPS (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)</td> <td>Virtualized DA-MP on TVOE Guest running relay, session, and database applications</td> </tr> <tr> <td>VM:MD-IWF</td> <td>Virtualized SS7-MP on TVOE Guest running MD-IWF applications</td> </tr> </tbody> </table> When finished, press the Assign button	DA-MP	MP Profile	current value	ZombieDAMP1	VM:10K_MPS	The current MP Profile for ZombieDAMP1 is VM:10K_MPS . Virtualized DA-MP rated at 10K MPS for all configurations [A value is required.]	ZombieDAMP2	VM:10K_MPS	The current MP Profile for ZombieDAMP2 is VM:10K_MPS . Virtualized DA-MP rated at 10K MPS for all configurations [A value is required.]	SS7-MP	MP Profile	current value	ZombieSS7MP1	VM:MD-IWF	The current MP Profile for ZombieSS7MP1 is VM:MD-IWF . Virtualized SS7-MP running MD-IWF application [A value is required.]	ZombieSS7MP2	VM:MD-IWF	The current MP Profile for ZombieSS7MP2 is VM:MD-IWF . Virtualized SS7-MP running MD-IWF application [A value is required.]	Profile Name	Description	VM:10K_MPS (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)	Virtualized DA-MP on TVOE Guest running relay, session, and database applications	VM:MD-IWF	Virtualized SS7-MP on TVOE Guest running MD-IWF applications
DA-MP	MP Profile	current value																								
ZombieDAMP1	VM:10K_MPS	The current MP Profile for ZombieDAMP1 is VM:10K_MPS . Virtualized DA-MP rated at 10K MPS for all configurations [A value is required.]																								
ZombieDAMP2	VM:10K_MPS	The current MP Profile for ZombieDAMP2 is VM:10K_MPS . Virtualized DA-MP rated at 10K MPS for all configurations [A value is required.]																								
SS7-MP	MP Profile	current value																								
ZombieSS7MP1	VM:MD-IWF	The current MP Profile for ZombieSS7MP1 is VM:MD-IWF . Virtualized SS7-MP running MD-IWF application [A value is required.]																								
ZombieSS7MP2	VM:MD-IWF	The current MP Profile for ZombieSS7MP2 is VM:MD-IWF . Virtualized SS7-MP running MD-IWF application [A value is required.]																								
Profile Name	Description																									
VM:10K_MPS (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Only)	Virtualized DA-MP on TVOE Guest running relay, session, and database applications																									
VM:MD-IWF	Virtualized SS7-MP on TVOE Guest running MD-IWF applications																									

Appendix P.3.9 Moving/Re-Shuffle: MP/DP

7	NOAM GUI: Restart the MP/DP Server	Navigate to Main menu -> Status & Manage -> Server  Select the MP/DP server. Select the Restart button.  Answer OK to the confirmation popup. 

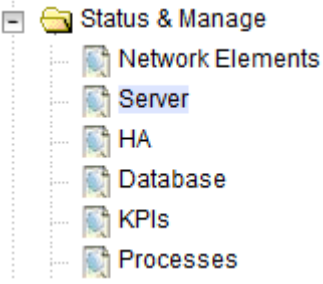
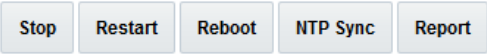
Appendix P.3.10 Moving/Re-Shuffle: Query Server (SDS Only)

S T E P #	This procedure will reference steps to configure a query server on the new virtual machine for VM re-shuffling scenarios. Prerequisites: • Query server has been Identified • Placed in OOS • OLD Virtual Machine Deleted • NEW Virtual Machine Created • TPD/DSR software installed Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	SDS NOAM VIP GUI: Configure the query server	Configure the query server by executing the steps referenced in the following procedures: <u>SDS query server:</u>Procedure 50: Steps 1-2, 4-8

Appendix P.3.10 Moving/Re-Shuffle: Query Server (SDS Only)

2 ☐	SDS NOAM VIP: Establish GUI Session	Establish a GUI session on the NOAM by using the XMI VIP address: https://<NOAM_VIP_IP_Address> Login as user guiadmin. 
3 ☐	SDS NOAM VIP GUI: Wait for Remote Database Alarm to Clear	Wait for the alarm Remote Database re-initialization in progress to be cleared before proceeding. Navigate to Main menu->Alarms & Events->View Active

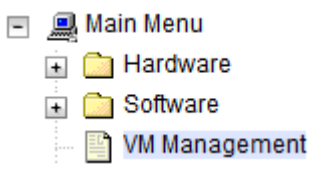
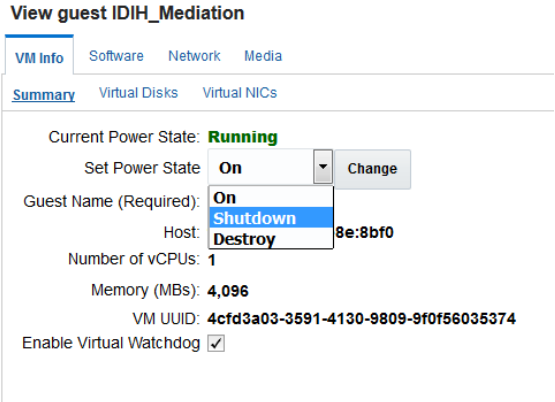
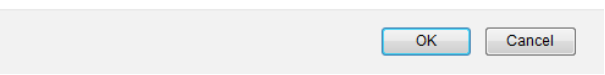
Appendix P.3.10 Moving/Re-Shuffle: Query Server (SDS Only)

4 ☐	SDS NOAM VIP GUI: Restart query server	Navigate to Main menu->Status & Manage->Server.  Select the query server. Select the Restart button.  Answer OK to the confirmation popup. Wait for restart to complete.

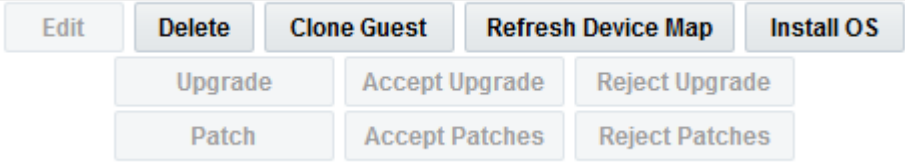
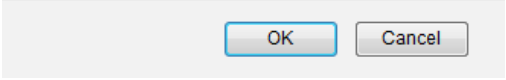
Appendix P.3.11 Moving/Re-Shuffle: iDIH

S T E P #	This procedure will reference steps to configure/Re-deploy iDIH on a set of new virtual machines for VM re-shuffling sceneries. IMPORTANT: If moving/Re-shuffling the Oracle VM/Server, it is important to note that doing so will remove all historical trace data. However, moving/Re-Shuffling of the Application and mediation VMs can be done without affecting historical trace data. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	PMAC GUI: Login Open web browser and navigate to the PMAC GUI, Login as Guiadmin user: <code>https://<pmac_network_ip></code>  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.

Appendix P.3.11 Moving/Re-Shuffle: iDIH

2 ☐	PMAC GUI: Shutdown the VM	Navigate to Main Menu -> VM Management  Expand the view (<i>if needed</i>) of the Rack Mount Server for which the server you are moving/deleting is located. Shutdown the VM by setting the <i>Current Power State</i> to Shutdown: View guest IDIH_Mediation  Click Change Select OK for the following prompt: It may not always be possible to shutdown a guest or to do so in a timely manner. You may monitor the power state and opt to destroy the guest rather than shut it down. Are you sure you want to attempt to shutdown this guest?  The <i>Current Power State</i> should now display Shutdown:

Appendix P.3.11 Moving/Re-Shuffle: iDIH

3 ☐	PMAC GUI: Delete the VM	Once the server has been shutdown, select the VM from step 2. Verify the <i>current power state</i> is Shutdown as listed in step 2. Select Delete  Click OK to confirm deletion 
4 ☐	PMAC Server: Navigate to guest-dropin directory	<pre>\$ cd /var/TKLC/smac/guest-dropin/</pre>
5 ☐	PMAC Server: Edit the IDIH fdc file	Edit the existing idih_fdc_file_name.xml (or create a new) file configured in procedure 57 step 7 Change the Rack Mount Server to which the VM being Moved/Re-shuffled will be placed by changing the <tvoehost> item for the applicable VM (<tvoeguest id>). Note: It may also be necessary to change the XMI, IMI, and default route IP addresses depending on the location of the rack mount server. IMPORTANT: If moving/Re-shuffling the Oracle VM/Server, it is important to note that doing so will remove all historical trace data. However, moving/Re-Shuffling of the Application and mediation VMs can be done without affecting historical trace data.

Appendix P.3.12 Moving/Re-Shuffle: PMAC

STEP #	This procedure will reference steps to configure the PMAC on a new virtual machine for VM re-shuffling scenarios. Prerequisites: Database backup of the PMAC server is available Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	PMAC: Backup PMAC Database	Backup the PMAC database by following Section 4.17.7 Backup PMAC Application
2 ☐	PMAC TVOE HOST: Login	Establish an SSH session to the PMAC's TVOE host, login as admusr .
3 ☐	PMAC TVOE HOST: Verify PMAC location	Verify the location of the PMAC VM using virsh : <pre>\$ sudo /usr/bin/virsh list</pre> <pre>Id Name State ----- 2 PM&C running</pre>
4 ☐	PMAC TVOE HOST: Remove Existing PMAC Guest	Delete the PMAC Guest: <pre>\$ sudo guestMgr -remove <PMAC_Name></pre>
5 ☐	New PMAC TVOE HOST: Deploy PMAC on new TVOE Host	Once the TVOE host for the new PMAC location has been identified, execute Section 4.3 to deploy the new PMAC
6 ☐	PMAC: Login	Establish an SSH session to the PMAC server, login as admusr .

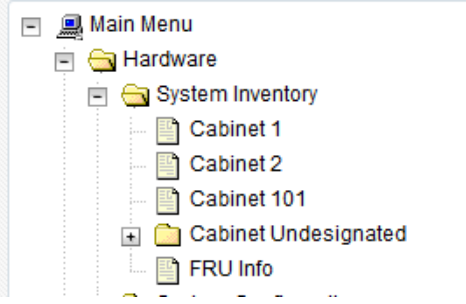
Appendix P.3.12 Moving/Re-Shuffle: PMAC

7 ☐	Restore PMAC Backup image to the TVOE 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. The example below is a simple scp from a redundant PM&C backup location. If using IPv6 addresses, command requires shell escapes, e.g. admsur@[<ipV6addr>]:/<file> <pre>\$ sudo /usr/bin/scp -p \ admsur@<remoteserver>:/var/TKLC/smac/backup/*.pef \ /var/TKLC/smac/backup/</pre> 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 prior to the restoration of the data.
8 ☐	PMAC: Verify no Alarms are present	Verify no alarms are present by executing the following command: <pre>\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre>
9 ☐	Restore the PMAC Data from Backup	Restore the PMAC data from backup by executing the following command: <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm restore</pre> <pre>PM&C Restore been successfully initiated as task ID 1</pre> Note: By default, PMAC restore used the most recent file in /var/TKLC/smac/backup that starts with 'backupPmac'. If the name of the file copied to the system uses a different name or is not the most recent, then provide the name using the --fileName parameter To check the status of the background task, issue the following command: <pre>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</pre> Note: The result will eventually display <i>PMAC Restore successful</i>.

Appendix P.3.12 Moving/Re-Shuffle: PMAC

10 ☐	PMAC GUI: Login	Open web browser and navigate to the PMAC GUI, Login as Guiadmin user: <code>https://<pmac_network_ip></code> 
11 ☐	PMAC GUI: Verify Restore Task completed	Navigate to Task Monitoring 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 will be added in the next step.

Appendix P.3.12 Moving/Re-Shuffle: PMAC

12 ☐	PMAC GUI: Verify System Inventory	Navigate to Main Menu -> System Inventory  Verify previously provisioned enclosures are present
13 ☐	PMAC: Verify PMAC	Perform a system health check on the PMAC <pre>\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre> This command should return no output on a healthy system. <pre>\$ sudo /usr/TKLC/smac/bin/sentry status</pre> All Processes should be running, displaying output similar to the following: <pre>PM&C Sentry Status ----- sentryd started: Mon Jul 23 17:50:49 2012 Current activity mode: ACTIVE Process PID Status StartTS NumR ----- ----- smacTalk 9039 running Tue Jul 24 12:50:29 2012 2 smacMon 9094 running Tue Jul 24 12:50:29 2012 2 hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2 snmpEventHandler 9176 running Tue Jul 24 12:50:29 2012 2 Fri Aug 3 13:16:35 2012 Command Complete.</pre>
14 ☐	PMAC: Add ISO images to the PMAC	Re-add any needed ISO images to the PMAC by executing procedure <i>“Install TVOE on Additional Rack Mount Servers”</i> Steps 2-3

Appendix P.3.13 Moving/Re-Shuffle: Redundant PMAC

S T E P #	This procedure will reference steps to configure the redundant PMAC on a new virtual machine for VM re-shuffling scenarios. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
2 ☐	Redundant PMAC TVOE HOST: Login	Establish an SSH session to the redundant PMAC's TVOE host, login as admusr .
3 ☐	Redundant PMAC TVOE HOST: Verify PMAC location	Verify the location of the redundant PMAC VM using virsh : <pre>\$ sudo /usr/bin/virsh list Id Name State ----- 2 Redundant-PM&C running</pre>
4 ☐	Redundant PMAC TVOE HOST: Remove Existing PMAC Guest	If an error was made use the following command to delete the PMAC Guest and then re-deploy the guest again: <pre>\$ sudo guestMgr -remove <PMAC_Name></pre>
5 ☐	New Redundant PMAC TVOE HOST: Deploy Redundant PMAC on new TVOE Host	Once the TVOE host for the redundant PMAC location has been identified, execute Section 4.11 to deploy the redundant PMAC

Appendix P.3.14 Post Moving/Re-Shuffle Health Check

S T E P #	This procedure will provide steps verify system status and log all alarms after Growth/De-growth. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: 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> Login as the <i>guiadmin</i> user:  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.

Appendix P.3.14 Post Moving/Re-Shuffle Health Check

2	NOAM VIP GUI: Verify Server Status	Navigate to Main Menu -> Status & Manage -> Server Status & Manage Network Elements Server HA Database KPIs Processes Verify all Server Status is Normal (Norm) for: Alarm (Alm), Database (DB), Replication Status, and Processes (Proc). <table><tr><th>Appl State</th><th>Alm</th><th>DB</th><th>Reporting Status</th><th>Proc</th></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr><tr><td>Enabled</td><td>Norm</td><td>Norm</td><td>Norm</td><td>Norm</td></tr></table>	Appl State	Alm	DB	Reporting Status	Proc	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm	Enabled	Norm	Norm	Norm	Norm
Appl State	Alm	DB	Reporting Status	Proc																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
Enabled	Norm	Norm	Norm	Norm																							
3	NOAM VIP GUI: Verify Server Configuration	Navigate to Main Menu -> Configuration -> Server Groups Configuration Networking Servers Server Groups Resource Domains Places Place Associations Verify the configuration data is correct for your network.																									
4	NOAM VIP GUI: Log Current Alarms	Navigate to Main Menu -> Alarms & Events -> View Active Alarms & Events View Active View History View Trap Log Click on the Report button Export Report Clear Selections Save or Print this report, keep copies for future reference. Print Save Back Compare this alarm report with those gathered in procedure Appendix P.3.2																									

Appendix P.3.14 Post Moving/Re-Shuffle Health Check

5 ☐	SOAM VIP GUI: Repeat	Repeat Steps 1-4 for the SOAM

Appendix P.3.15 Post Move/Re-Shuffle Backups

S T E P #	This procedure will reference steps to backup all necessary items after a Re-Shuffle scenario. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Backup TVOE	Backup all TVOE host configurations by executing Section 4.17.6 Backup TVOE Configuration
2 ☐	Backup PMAC	Backup the PMAC application by executing Section 4.17.7 Backup PMAC Application
3 ☐	Backup NOAM/SOAM databases	Backup the NOAM and SOAM Databases by executing Sections 4.17.8 Backup NOAM Database and 4.17.9 Backup SOAM Database Note: Database backup on SDS SOAMs not required

Appendix Q: Non-HA Lab Node Instructions (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) Non-HA Lab Node Only)

This appendix contains deviations required during Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) RMS Non-HA Lab node installation to be followed, and are mainly applicable during VM creation procedures. The rest of the installation steps are similar to “DSR Rack Mount Server” installation mentioned in this document.

- FUNCTIONALITY ARISING OUT OF OR RELATED TO THE IMPLEMENTATION OR USE OF A MATED PAIR. EXCEPT AS EXPRESSLY STATED HEREIN, ORACLE EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE NON-HA LAB NODE WILL OPERATE OR UNINTERRUPTED OR ERROR-FREE; and
- ORACLE SHALL HAVE NO LIABILITY WHATSOEVER FOR ANY LOSSES ARISING OUT OF, RESULTING FROM, OR RELATED TO A NON-HA LAB NODE OR THE USE THEREOF, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES, INCLUDING BUT NOT LIMITED TO LOST OR DAMAGED DATA; LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS; REPLACEMENT COSTS OR COSTS OF SUBSTITUTE PRODUCTS.

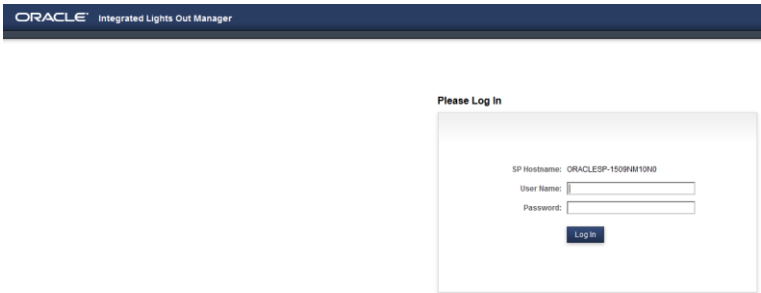
Note:

1. Non-HA Lab Node install include NOAM-Active/Standby, SOAM-Active/Standby, 1 IPFE, 1 DAMP, 1 SBR (B), 1 SBR(S), 1-SS7MP, 1-IDIH_Mediation, 1-IDIH_Application and 1-IDIH_Database and for SDS NOAM-Active/Standby, SOAM-Active/Standby, 1 Query Server, 1 DP.

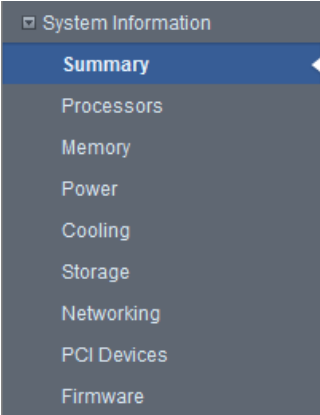
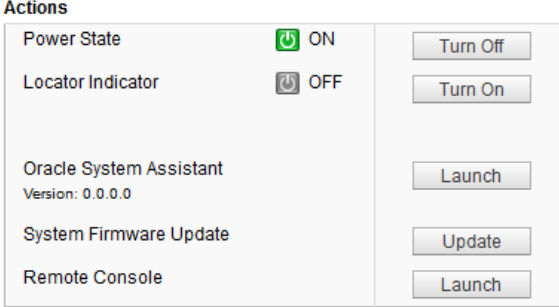
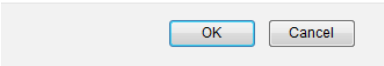
Appendix Q.1: Non-HA Lab Node Pre-IPM Procedures

This procedure details the steps needed to create vgguests logical volume with RAID10 spanning across multiple HDDs for Non-HA lab node deployments.

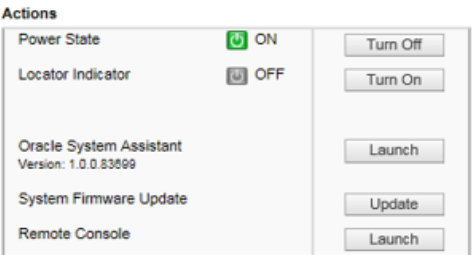
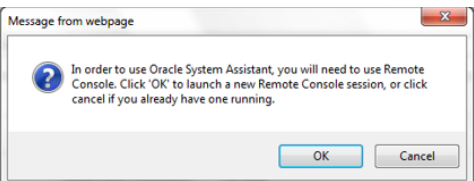
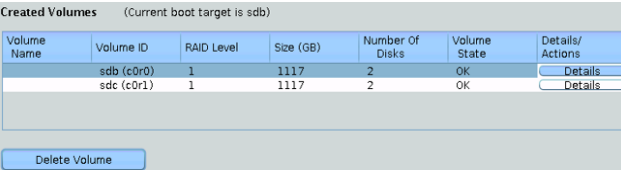
Appendix Q.1.1 RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X5-2/Netra X5-2)

S T E P #	This procedure will provide the steps needed to create a HD RAID10 volume by combining multiple HDD on Oracle X5-2/Netra X5-2. Prerequisite: Multiple HDD must be installed and configured on the target RMS. TVOE ISO USB must be inserted into USB socket. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.
1 ☐	Oracle X5-2/Netra X5-2: Login Login to the Oracle rack mount server ILOM: 

Appendix Q.1.1 RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X5-2/Netra X5-2)

2 ☐	ILOM GUI : Login to ILOM GUI and Turn Off the Power State	Navigate to System Information->Summary  From the Actions window, click Turn Off for Power State:  Press OK to confirm The host power will be set to off. Click OK to continue. 

Appendix Q.1.1 RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X5-2/Netra X5-2)

3 ☐	ILOM GUI: Launch Oracle System Assistant and Accept License Agreement.	Press the Launch button next to “Oracle System Assistant” which will launch a remote console  Press Ok. Wait for “Oracle System Assistant”.  Once “Oracle System Assistant” Launches, It will ask for Accepting License Agreement. Press Accept for Accepting License Agreement.
4 ☐	ILOM GUI: Configure Hardware and select HBA	Click on Configure Hardware on Left side of GUI and select the HBA, there should only be one. 
5 ☐	ILOM GUI: Delete the existing Volume if exists	Look under “Created Volumes”. If there is a volume created that does not match the configuration you want.  Click on Delete Volume. Answer Yes to confirm.  Delete all the volumes.

Appendix Q.1.1 RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X5-2/Netra X5-2)

6

ILOM GUI:
Select RAID
Level and
Select Disks
which needs
to be added.

Click on **Select RAID Level** and choose **RAID 10**.

Under “Available Disks” select each disk to add to the Logical Volume you want to create.

To create a volume, first select RAID level. Then allocate disks to the volume.

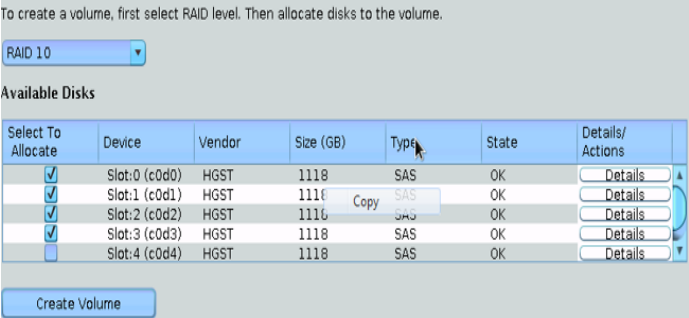
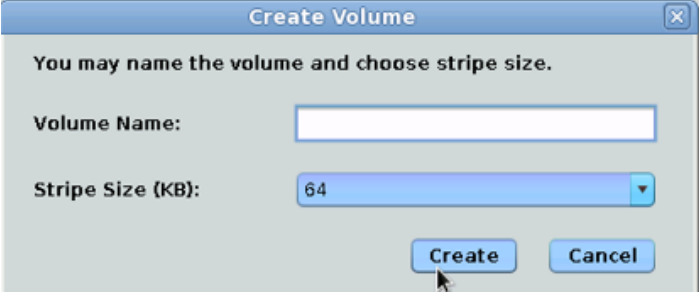
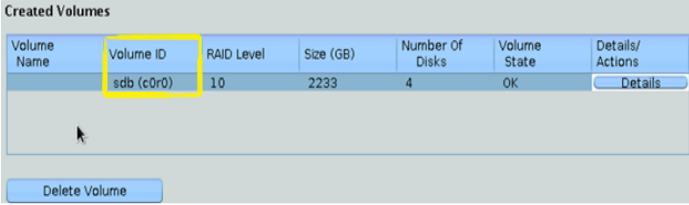
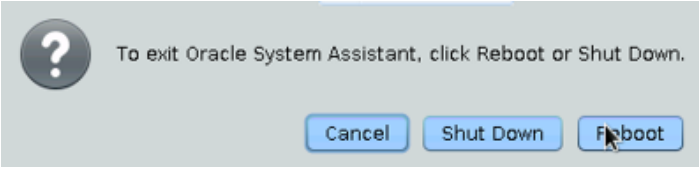
RAID 10

Available Disks

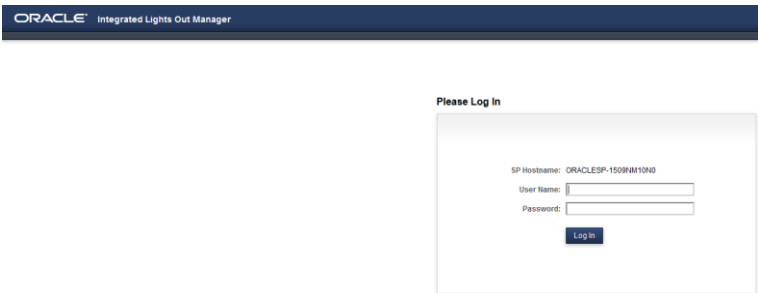
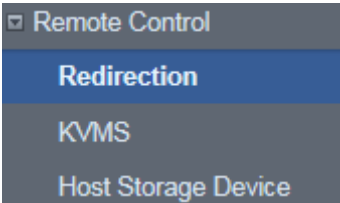
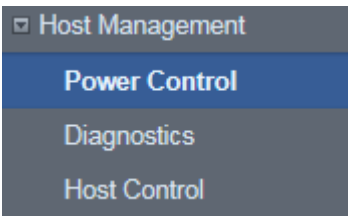
Select To Allocate	Device	Vendor	Size (GB)	Type	State	Details/ Actions
☒	Slot:0 (c0d0)	HGST	1118	SAS	OK	Details
☒	Slot:1 (c0d1)	HGST	1118	SAS	OK	Details
☒	Slot:2 (c0d2)	HGST	1118	SAS	OK	Details
☒	Slot:3 (c0d3)	HGST	1118	SAS	OK	Details
☐	Slot:4 (c0d4)	HGST	1118	SAS	OK	Details

Create Volume

Appendix Q.1.1 RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X5-2/Netra X5-2)

7 ☐	ILOM GUI: Create Volume and note created Volume ID for later use.	Click on Create Volume  Click on Create in the popup box to confirm creation. No name is needed.  Under “Created Volumes” note Volume ID, and save for later. In this case Volume ID : sdb 
8 ☐	ILOM GUI: Exit OSA screen UI and Reboot.	Click on Exit in the OSA GUI.  Click Reboot on the warning screen.  Note: Please ignore warning messages related to “Primary OS” and storage not being available.

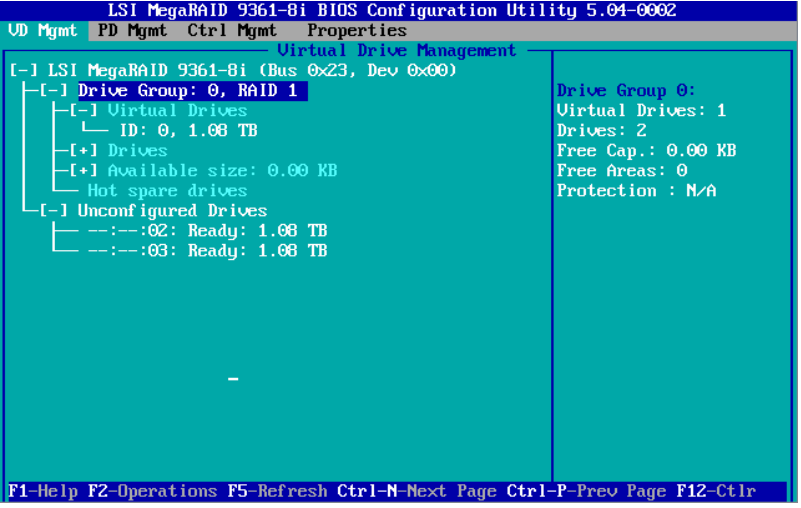
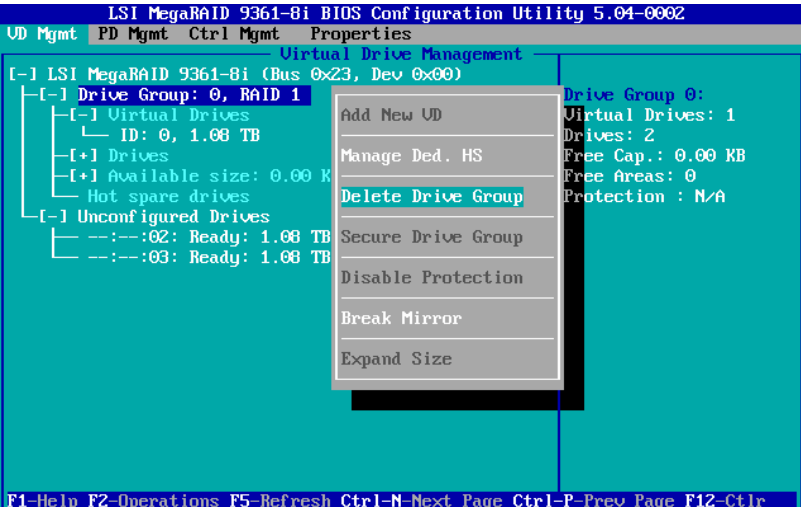
Appendix Q.1.2 RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2)

S T E P #	This procedure will provide the steps needed to create a HD RAID10 volume by combining multiple HDD on Oracle X6-2. Prerequisite: Multiple HDD must be installed on the target RMS. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	Oracle X6-2: Login	Login to the Oracle rack mount server ILOM: 
2 ☐	ILOM GUI: Launch Remote Console	Navigate to Remote Control -> Redirection  Click on Launch Remote Console.
3 ☐	ILOM GUI: Power Cycle server	Navigate to Host Management -> Power Control  From the Settings window, select Power Cycle, then Save:

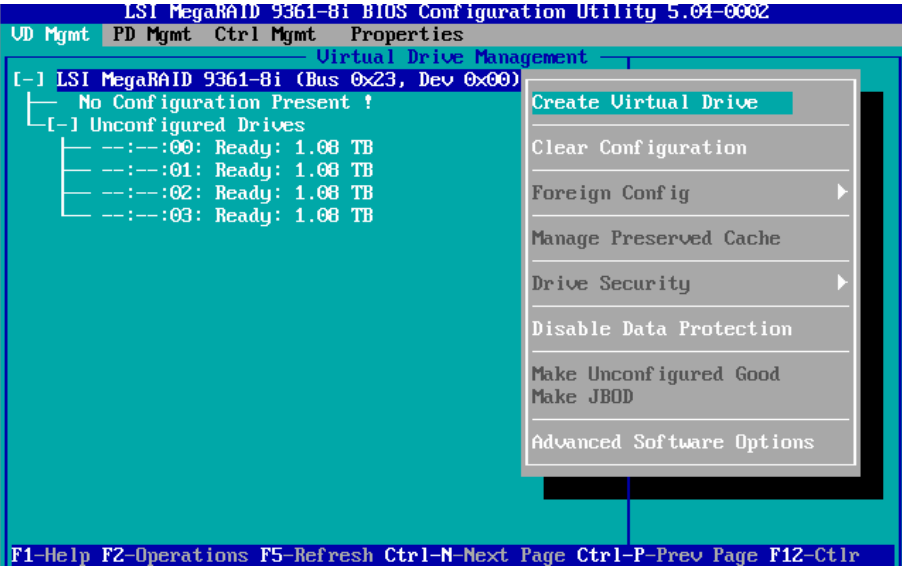
Appendix Q.1.2 RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2)

4	ILOM GUI: Launch RAID BIOS configuration utility	Type CTRL+R during the boot process to launch the BIOS Configuration Utility. The LSI MegaRAID BIOS Configuration Utility appears. 

Appendix Q.1.2 RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2)

5 ☐	ILOM GUI: Delete the existing Drive Group if exists	Look under “Drive Group”. If there is a volume created that does not match the configuration you want.  Click F2. Select Delete Drive Group.  Select Yes.

Appendix Q.1.2 RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2)

6 ☐	ILOM GUI: Create Virtual Drive	Select the MegaRAID item and click F2  Select Create Virtual Drive.

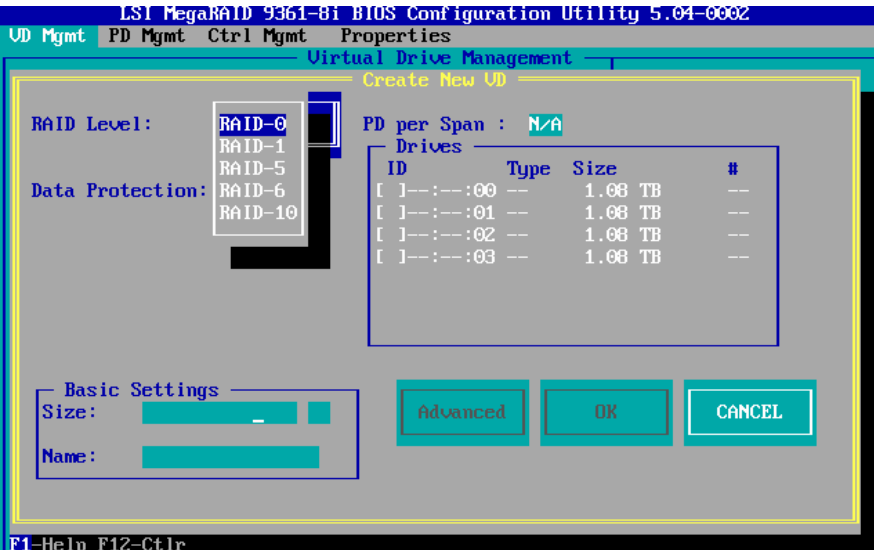
Appendix Q.1.2 RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2)

7

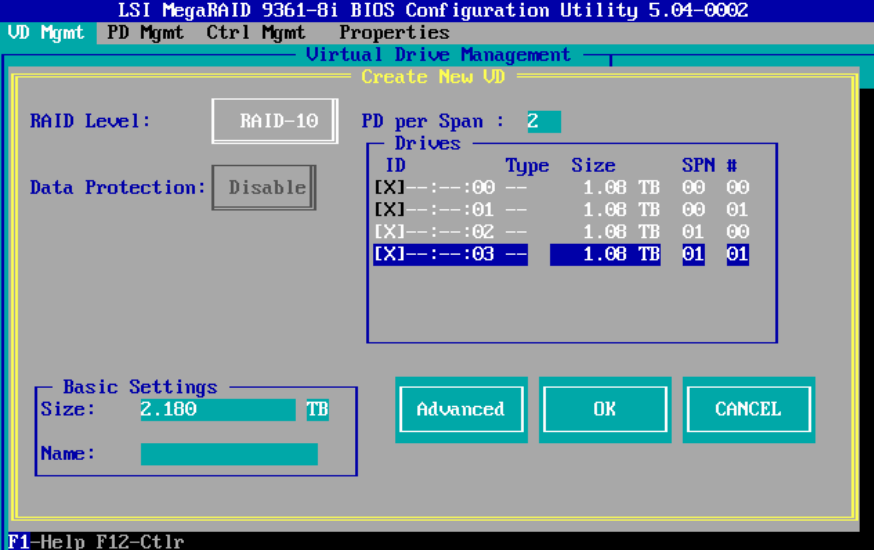
ILOM GUI:

Select RAID level and assign drives

Select RAID level, **RAID-10**

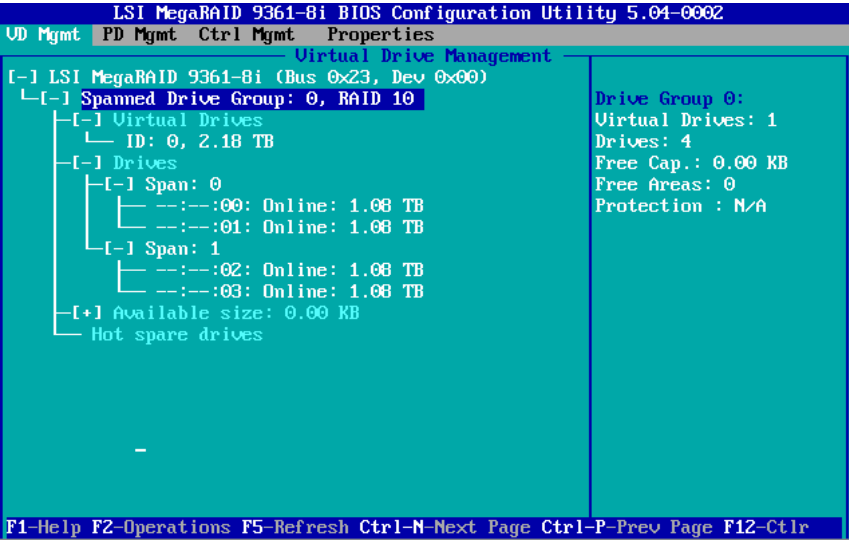
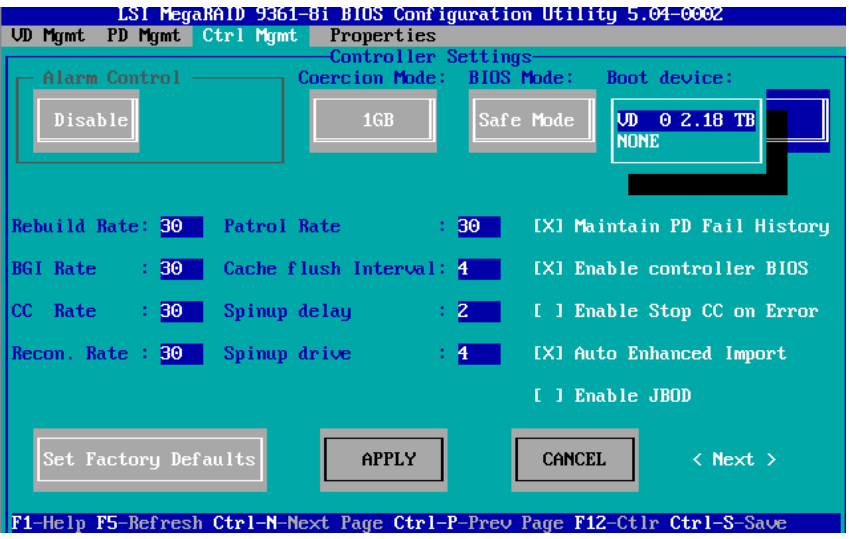


For each drive that you want in the logical drive, navigate to the drive and press **Enter** in its ID field to produce an X in the field.

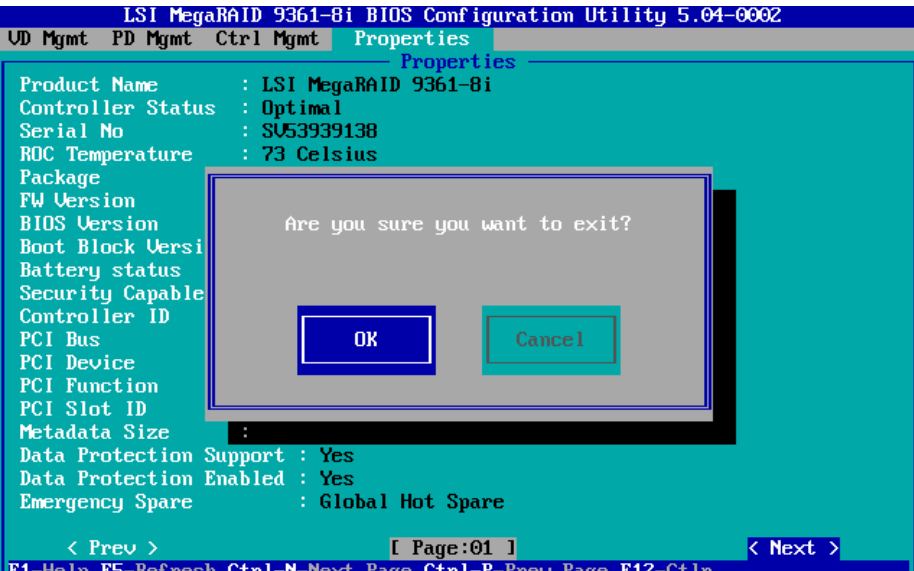


After selecting all the drives that you want included in the logical drive, use the arrow keys to navigate to the **OK** button, then press **Enter**, and **OK**.

Appendix Q.1.2 RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2)

8 ☐	ILOM GUI: Verify drive creation	Verify the logical drive creation by reviewing the drive groups on the main page of the BIOS Configuration Utility. Note the new drive group that is now displayed on the page. 
9 ☐	ILOM GUI: Make drive bootable	Click Ctrl + N twice to select Ctrl Mgmt. From the Ctrl Mgmt page, use the arrow keys to navigate to the Boot device field, and press Enter. Select the drive to make it bootable.  Use the arrow keys to navigate to the Apply button, and then press Enter. Type CTRL+S to save the configuration.

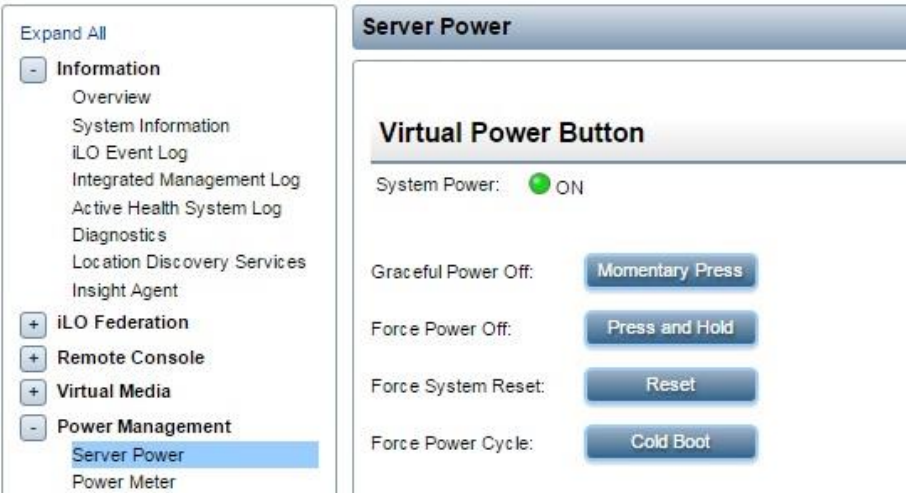
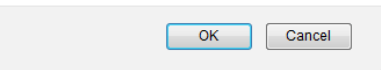
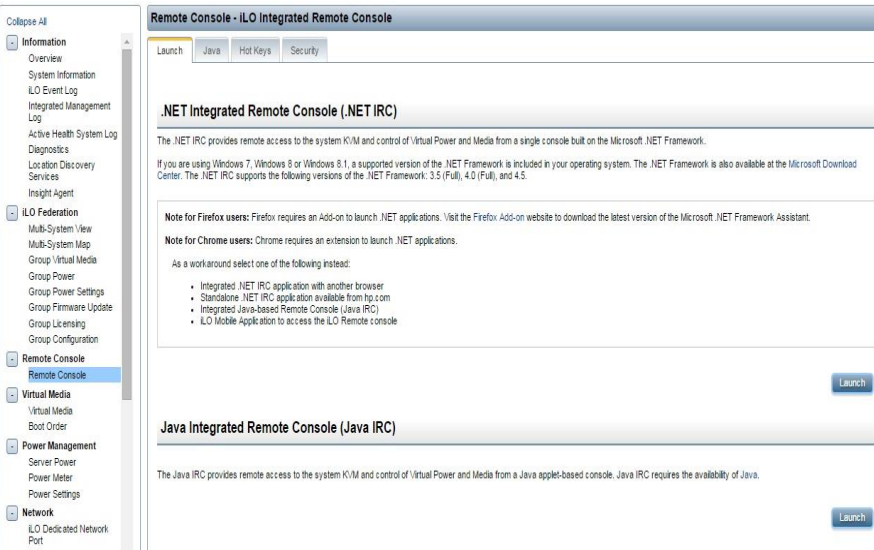
Appendix Q.1.2 RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2)

10 ☐	ILOM GUI: Exit configuration	Press Esc and click on OK.  The screenshot shows the LSI MegaRAID BIOS Configuration Utility. The 'Properties' tab is active, displaying various RAID controller details. A confirmation dialog box is overlaid, asking 'Are you sure you want to exit?' with 'OK' and 'Cancel' buttons. The background text includes: Product Name: LSI MegaRAID 9361-8i, Controller Status: Optimal, Serial No: SU53939138, ROC Temperature: 73 Celsius, Package, FW Version, BIOS Version, Boot Block Version, Battery status, Security Capable, Controller ID, PCI Bus, PCI Device, PCI Function, PCI Slot ID, Metadata Size, Data Protection Support: Yes, Data Protection Enabled: Yes, Emergency Spare: Global Hot Spare. Navigation keys at the bottom include < Prev >, [Page:01], < Next >, F1-Help, F5-Refresh, Ctrl-N-Next Page, Ctrl-P-Prev Page, and F12-Ctrl.
11 ☐	ILOM GUI: Reboot	Press Ctrl + Alt + Delete to reboot  The screenshot shows a black screen with the text: ** Press Control+Alt+Delete to reboot **. Note Volume ID for X6-2 is: sda. This is used as input parameter when installing TVOE.

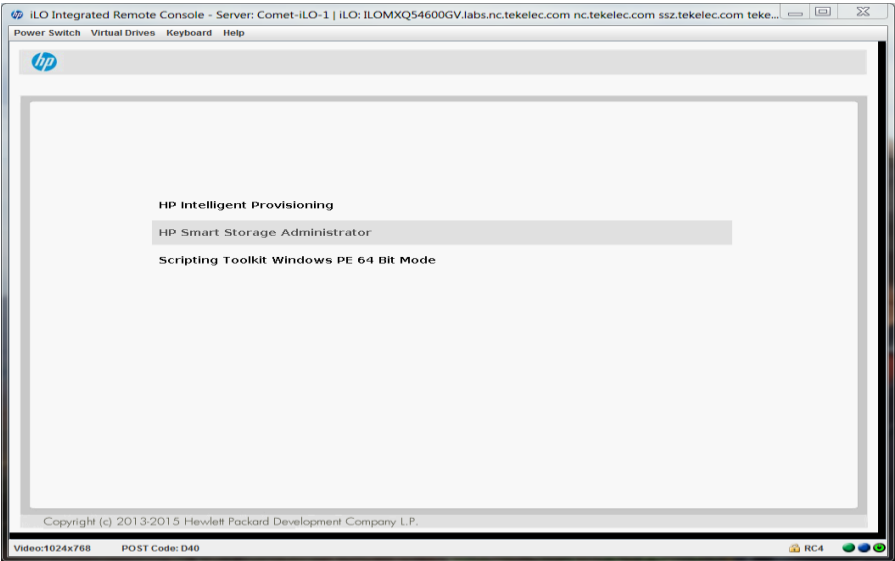
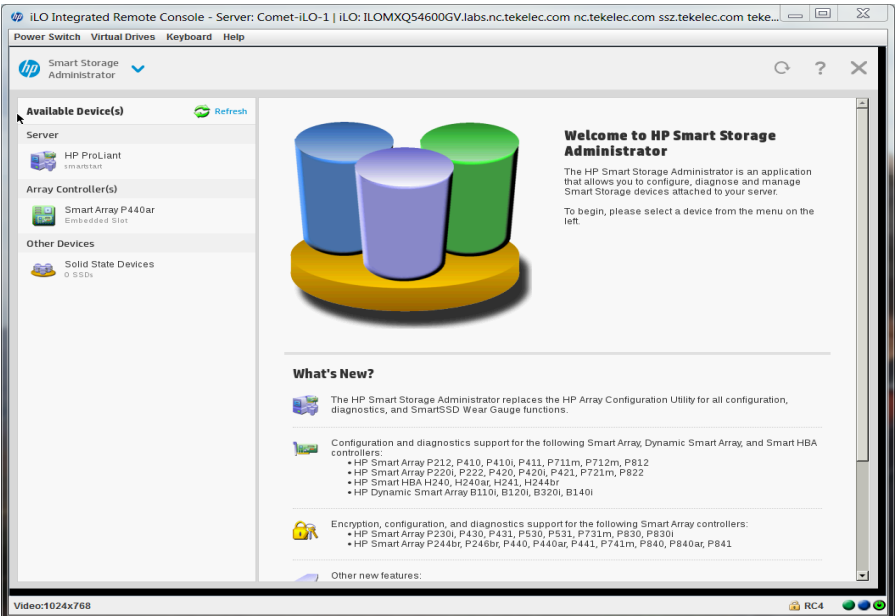
Appendix Q.1.3 RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380 Gen9)

S T E P #	This procedure will provide the steps needed to create a HD RAID10 volume by combining multiple HDD on HP DL380 Gen 9. Prerequisite: Multiple HDD must be installed and configured on the target RMS. TVOE ISO USB must be inserted into USB socket. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	HP Gen9: Login to ILOM GUI	Login to the HP rack mount server ILOM:  © Copyright 2002-2015 Hewlett-Packard Development Company, L.P.

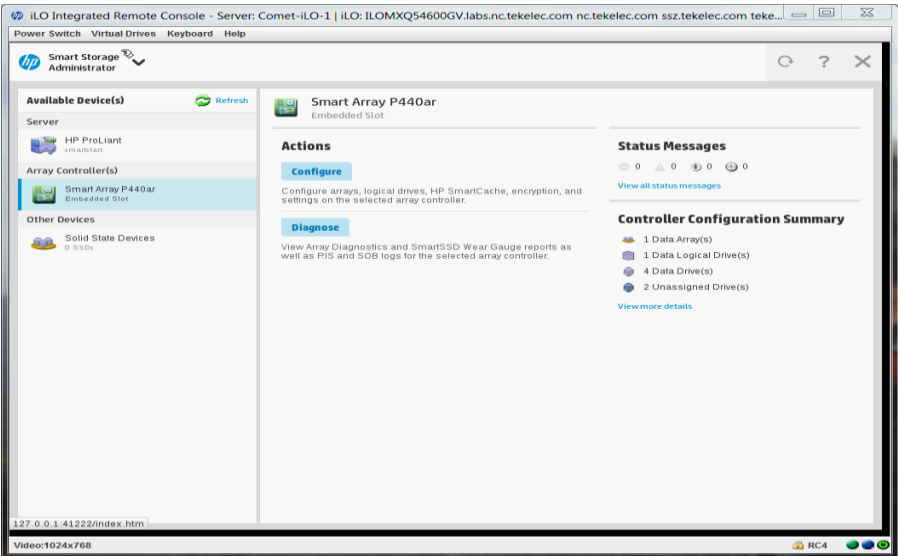
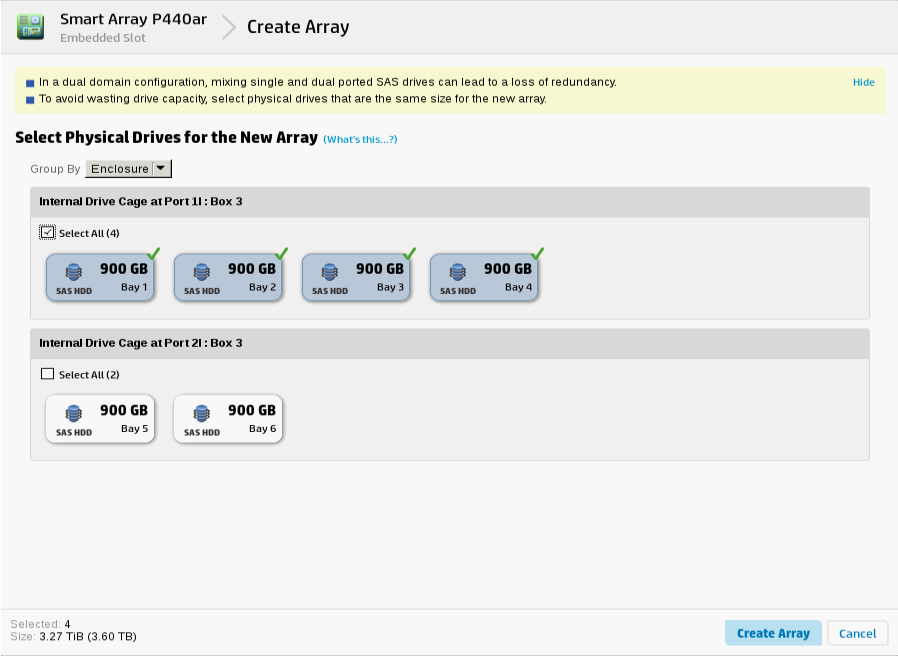
Appendix Q.1.3 RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380 Gen9)

2 ☐	ILOM GUI : Turn Off the Power State	Navigate to Power Management->Server Power  From the Virtual Power Button, click Momentary Press for Graceful Power Off Press OK to confirm The host power will be set to off. Click OK to continue. 
3 ☐	ILOM GUI: Launch HP iLO Integrated Remote Console.	Press the Launch button from Remote Console -> Remote Console 

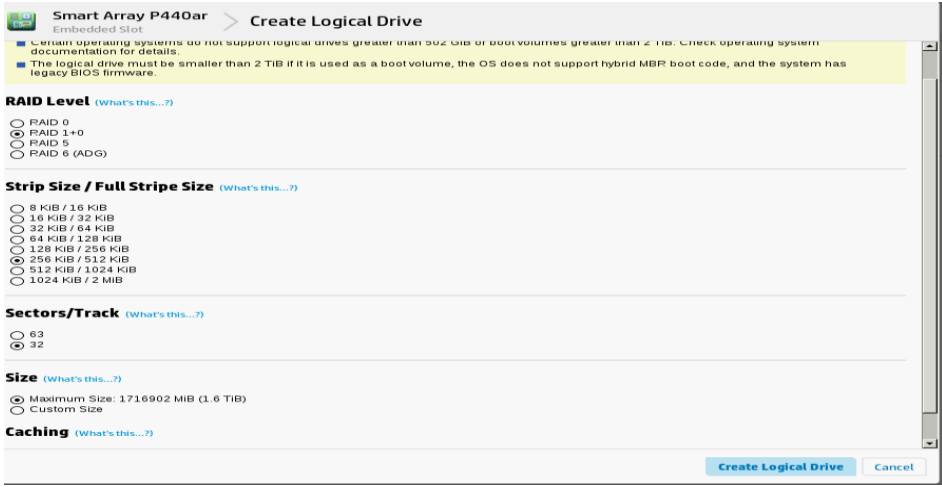
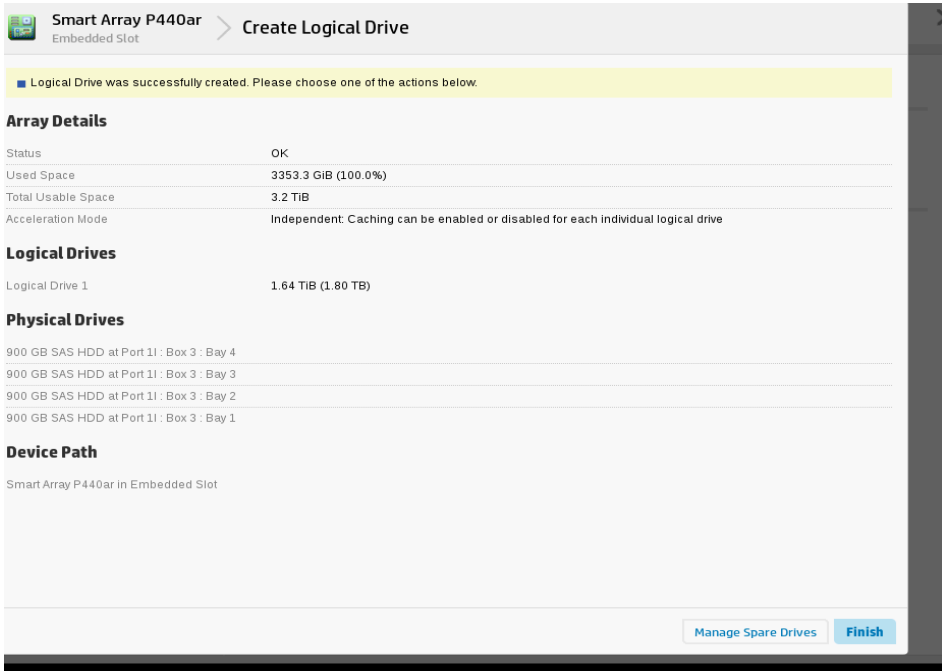
Appendix Q.1.3 RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380 Gen9)

4 ☐	ILOM GUI: Enter HP Intelligent Provisioning and HP smart storage administrator	Enter into the HP Intelligent Provisioning by pressing F10 during boot up. Enter HP Smart Storage Administrator 
5 ☐	ILOM GUI: Configure the Array Controllers	Click Smart Array P440ar 

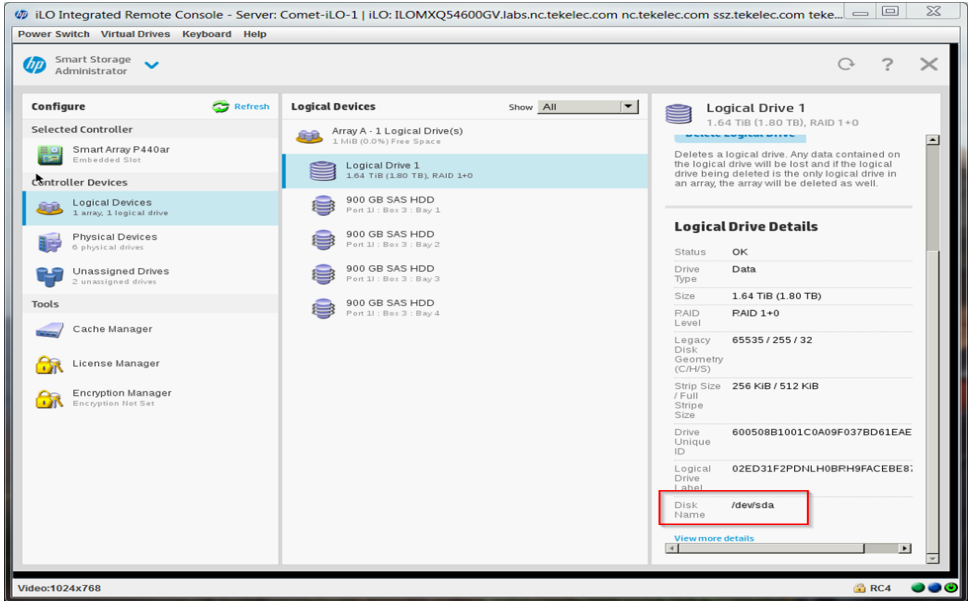
Appendix Q.1.3 RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380 Gen9)

6 ☐	ILOM GUI: Configure the Array Controllers	Click Configure 
7 ☐	ILOM GUI: Select the physical drives for the new array and click on Create Array:	Select 4 physical drives and Click Create Array. 

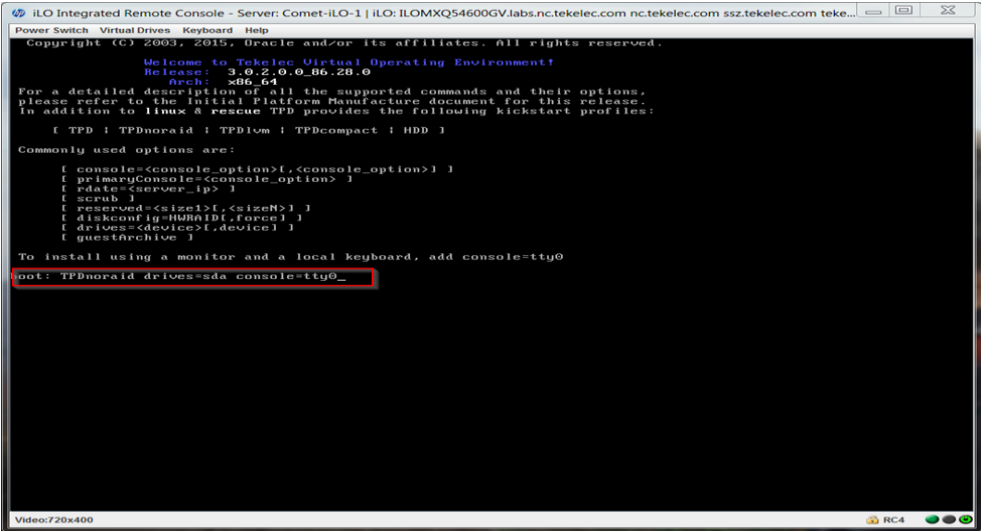
Appendix Q.1.3 RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380 Gen9)

8 ☐	ILOM GUI: RAID 10 Logical Volume creation	Select RAID Level as RAID1+0, leave the rest defaults and click Create Logical Drive. 
9 ☐	ILOM GUI: RAID 10 Logical Volume creation	Click Finish 
10 ☐	ILOM GUI: Restart Server	Restart the server by clicking the power button at the bottom right corner of the window. 

Appendix Q.1.3 RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380 Gen9)

11 ☐	ILOM GUI:	Repeat step 4 to get into the “Smart Storage Administrator” screen.
12 ☐	ILOM GUI: Select the created logical drive	Click on the Logical Devices under the Controller Devices and select “Logical Drive 1” and note down the Disk Name. For example, /dev/sda. This will be used in the steps below. 
13 ☐	ILOM GUI: Reboot Server	Reboot the server by clicking the power button at the bottom right hand corner. 

Appendix Q.1.3 RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380 Gen9)

14	ILOM GUI: TVOE installation	When prompted with the boot: provide the following command and press Enter. Note: You need to use the correct “Disk Name” (noted in Step 12) in this command.  TVOE installation would begin and continue normally.

Appendix Q.2: Non-HA Lab Node PMAC Deployment

The following steps covers the deviations during PMAC deployment and VM creations and provide the CPU, RAM and Hard Disk information that will override the default values when importing profile during VM creations. These changes are required to place all VMs onto a single Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) server.

Appendix Q.2.1 PMAC Deployment: Procedure 6 Deviation

S T E P #	This procedure will deploy PMAC on the TVOE Host Prerequisite: First RMS Network Configuration (PMAC Host) has been completed. Needed material: - PMAC Media on USB Drive or ISO Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	1st RMS iLO/iLOM: Login and Launch the Integrated Remote Console	Log in to iLO/iLOM; follow Appendix D: TVOE iLO/iLOM GUI Access for instructions on how to access the iLO/iLOM GUI. https://<management_server_iLO_ip>

Appendix Q.2.1 PMAC Deployment: Procedure 6 Deviation

2 ☐	TVOE iLO/iLOM: Mount the PMAC Media to the TVOE Server	Use one of the following 2 options to mount the PMAC Media: <u>Option 1:</u> If using a USB media, insert the PMAC USB into a USB port and execute the following to mount the ISO: <pre>\$ ls /media/*/*.iso /media/sdd1/872-2586-101-5.7.0_57.3.0-PM&C-x86_64.iso</pre> Use the output of the previous command to populate the next command <pre>\$ sudo mount -o loop /media/sdb1/872-2586-101-5.7.0_57.3.0-PM&C-x86_64.iso /mnt/upgrade</pre> <u>Option 2:</u> If using an ISO image, run the following to mount it: <pre>\$ sudo mount -o loop ISO_FILENAME.iso /mnt/upgrade</pre> Next Validate the PMAC media by executing the following commands: <pre>\$ cd /mnt/upgrade/upgrade \$.validate/validate_cd</pre> <pre>Validating cdrom... UMVT Validate Utility v2.2.2, (c)Tekelec, June 2012 Validating <device or ISO> Date&Time: 2012-10-25 10:07:01 Volume ID: tklc_872-2441-106_Rev_A_50.11.0 Part Number: 872-2441-106_Rev_A Version: 50.11.0 Disc Label: PM&C Disc description: PM&C The media validation is complete, the result is: PASS CDROM is Valid</pre> Note: If the media validation fails, the media is not valid and should not be used.

Appendix Q.2.1 PMAC Deployment: Procedure 6 Deviation

3 ☐	TVOE iLO/iLOM: Deploy PMAC	Using the PMAC-deploy script, deploy the PMAC instance using the configuration captured during the site survey. <pre>\$ cd /mnt/upgrade/upgrade</pre> If deploying PMAC without NetBackup feature, run the following command: <pre>\$ sudo ./pmac-deploy --guest=<PMAC_Name> --hostname=<PMAC_Name> --controlBridge=control --controlIP=<PMAC_Control_ip_address> --controlNM=<PMAC_Control_netmask> --managementBridge=management --managementIP=<PMAC_Management_ip_address> --managementNM=<PMAC_Management_netmask/prefix> --routeGW=<PMAC_Management_gateway_address> --ntpserver=<TVOE_Management_server_ip_address> --imageSizeGB=20 --isoimagesVolSize=20</pre> The PMAC will deploy and boot. The management and control network will come up based on the settings that were provided to the PMAC-deploy script. Note: This step takes between 5 and 10 minutes.
4 ☐	TVOE iLO/iLOM: Unmount the Media	The media should auto-unmount, if it does not, unmount the media using the following command: <pre>\$ cd / \$ sudo /bin/umount /mnt/upgrade</pre> Remove the media from the drive.

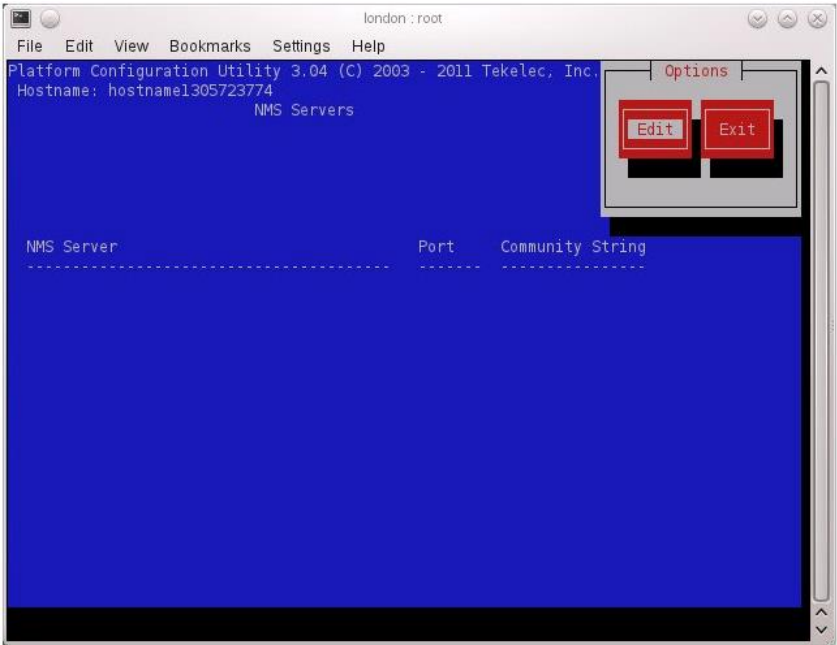
Appendix Q.2.1 PMAC Deployment: Procedure 6 Deviation

5 ☐	TVOE iLO/iLOM: SSH into the Management Server	Using an SSH client such as putty, ssh to the TVOE host as admusr. Login using virsh, and wait until you see the login prompt : <pre>\$ sudo /usr/bin/virsh list</pre> <pre>Id Name State ----- 2 PM&C running</pre> <pre>\$ sudo /usr/bin/virsh console <PM&C></pre> [Output Removed] <pre>Starting ntdMgr: [OK] Starting atd: [OK] 'TPD Up' notification(s) already sent: [OK] upstart: Starting tpdProvd... upstart: tpdProvd started. CentOS release 6.2 (Final) Kernel 2.6.32-220.17.1.el6prere16.0.0_80.14.0.x86_64 on an x86_64 PM&Cdev7 login:</pre>
6 ☐	Virtual PMAC: Verify the PMAC is configured correctly on first boot	Establish an SSH session to the PMAC, login as admusr. Run the following command (there should be no output): <pre>\$ sudo /bin/ls /usr/TKLC/plat/etc/deployment.d/</pre>
7 ☐	TVOE iLO/iLOM: Error doing verification, if error is outputted	If an error was made use the following command to delete the PMAC Guest and then re-deploy the guest again: <pre>\$ sudo guestMgr --remove <PMAC_Name></pre>

Appendix Q.2.1 PMAC Deployment: Procedure 6 Deviation

8 ☐	Virtual PMAC: Set the PMAC time zone	Determine the Time Zone to be used for the PMAC Note: Valid time zones can be found in Appendix J: List of Frequently used Time Zones Run <pre>\$ sudo set_pmac_tz.pl <time zone></pre> Example: <pre>\$ sudo set_pmac_tz.pl America/New_York</pre> Verify that the time zone has been updated: <pre>\$ sudo date</pre>

Appendix Q.2.1 PMAC Deployment: Procedure 6 Deviation

9 ☐	Virtual PMAC: Set SNMP	Set SNMP by running the following: <pre>\$ sudo su - platcfg</pre> Navigate to Network Configuration -> SNMP Configuration -> NMS Configuration.  Select Edit and then choose Add a New NMS Server. The 'Add an NMS Server' page will be displayed. Complete the form by entering in all information about the SNMP trap destination. Select OK to finalize the configuration. The 'NMS Server Action Menu' will now be displayed. Select Exit. The following dialogue will then be presented. Select Yes and then wait a few seconds while the Alarm Routing Service is restarted. At that time the SNMP Configuration Menu will be presented. Exit platcfg.
10 ☐	Virtual PMAC: Reboot the server	Reboot the server by running: <pre>\$ sudo init 6</pre>

Appendix Q.3: Non-HA Lab Node VM Automation Profile Values

This table reflects the values needed for Non-HA lab node VM profile values.

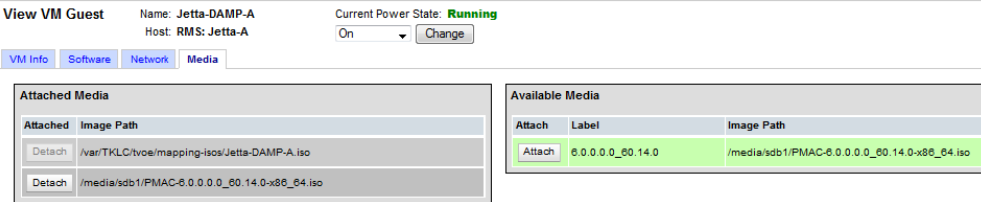
CPU	MEMORY	VDISK
DSR NOAM		
DSR_VIRT_NOAM_CPU="2"	DSR_VIRT_NOAM_MEM="6144"	DSR_VIRT_NOAM_VDISK="71680"
DSR SOAM		
DSR_VIRT_SOAM_CPU="2"	DSR_VIRT_SOAM_MEM="6144"	DSR_VIRT_SOAM_VDISK="71680"
DSR DAMP		
DSR_VIRT_DAMP_CPU="6"	DSR_VIRT_DAMP_MEM="24576"	DSR_VIRT_DAMP_VDISK="71680"
DSR SS7MP		
DSR_VIRT_SS7MP_CPU="6"	DSR_VIRT_SS7MP_MEM="24576"	DSR_VIRT_SS7MP_VDISK="71680"
DSR IPFE		
DSR_VIRT_IPFE_CPU="2"	DSR_VIRT_IPFE_MEM="16384"	DSR_VIRT_IPFE_VDISK="71680"
DSR SESSION SBR		
DSR_VIRT_SBR_SESSION_CPU="6"	DSR_VIRT_SBR_SESSION_MEM="16384"	DSR_VIRT_SBR_SESSION_VDISK="71680"
DSR BINDING SBR		
DSR_VIRT_SBR_BINDING_CPU="6"	DSR_VIRT_SBR_BINDING_MEM="16384"	DSR_VIRT_SBR_BINDING_VDISK="71680"
SDS NOAM		
SDS_VIRT_NOAM_CPU="4"	SDS_VIRT_NOAM_MEM="12288"	SDS_VIRT_NOAM_VDISK="102400"
SDS SOAM		
SDS_VIRT_SOAM_CPU="2"	SDS_VIRT_SOAM_MEM="10240"	SDS_VIRT_SOAM_VDISK="71680"
SDS DP		
SDS_VIRT_DP_CPU="2"	SDS_VIRT_DP_MEM="10240"	SDS_VIRT_DP_VDISK="71680"
SDS QUERY SERVER		
SDS_VIRT_QS_CPU="2"	SDS_VIRT_QS_MEM="16384"	SDS_VIRT_QS_VDISK="71680"

Appendix Q.4: Non-HA Lab Node IDIH Procedure Deviation

Appendix Q.4.1 IDIH Installation: Procedure 58 Deviation

S T E P #	This procedure will provide the steps to install and configure IDIH. Prerequisite: TVOE has been installed and configured on the target RMS Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.	
1 ☐	TVOE Host: Load Application ISO	Note: If the IDIH ISO images have NOT yet been added to the PMAC, execute steps 1-4 Add the Application ISO images (Mediation, Application, and OracleGuest) to the PMAC, this can be done in one of three ways: 4. Insert the CD containing the IDIH media into the removable media drive. 5. Attach the USB device containing the ISO to a USB port. 6. Copy the Application ISO file to the PMAC server into the /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as pmacftpusr user: cd into the directory where your ISO image is located on the TVOE Host (<i>not on the PMAC server</i>) Using sftp, connect to the PMAC server <pre>\$ sftp pmacftpusr@<pmac_management_network_ip> \$ put <image>.iso</pre> After the image transfer is 100% complete, close the connection: <pre>\$ quit</pre>

Appendix Q.4.1 IDIH Installation: Procedure 58 Deviation

2 ☐	PMAC GUI: Login	Open web browser and enter: https://<PMAC_Mgmt_Network_IP> Login as guiadmin user: 
3 ☐	PMAC GUI: Attach the software Image to the PMAC Guest	If in Step 1 the ISO image was transferred directly to the PMAC guest via sftp, skip the rest of this step and continue with step 4. If the image is on a CD or USB device, continue with this step. In the PMAC GUI, navigate to Main Menu -> VM Management. In the "VM Entities" list, select the PMAC guest. On the resulting "View VM Guest" page, select the Media tab. Under the Media tab, find the ISO image in the "Available Media" list, and click its Attach button. After a pause, the image will appear in the "Attached Media" list. 

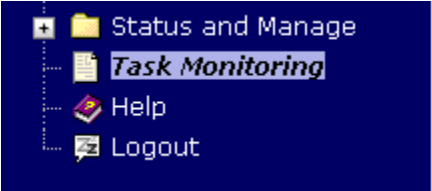
Appendix Q.4.1 IDIH Installation: Procedure 58 Deviation

4 ☐	PMAC GUI: Add Application Image	Navigate to Main Menu -> Software -> Manage Software Images Press Add Image button. Use the drop down to select the image.  If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://..."). These devices are assigned in numerical order as CD and USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the iso image of interest is normally present on the second device, "device://dev/sr1". If one or more CD or USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number. If in Step 1 the image was transferred to PMAC via sftp it will appear in the list as a local file "/var/TKLC/...". Select the appropriate path and Press Add New Image button. You may check the progress using the Task Monitoring link. Observe the green bar indicating success. Once the green bar is displayed, remove the IDIH Media from the optical drive of the management server.
5 ☐	PMAC: Establish Terminal Session	Establish an SSH session to the PMAC. Login as admusr.
6 ☐	PMAC: Copy the fdccfg template XML file to the guest-dropin Directory	Copy the vedsr_idih.xml.template XML file to the pmac guest-dropin directory. Execute the following command: <pre>\$ sudo cp /usr/TKLC/smac/html/TPD/mediation-7.1.0.0.0_x.x.x.x/vedsr_idih.xml.template /var/TKLC/smac/guest-dropin</pre> <pre>\$ cd /var/TKLC/smac/guest-dropin/</pre> <pre>\$ mv vedsr_idih.xml.template <idih_fdc_file_name>.xml</pre>

Appendix Q.4.1 IDIH Installation: Procedure 58 Deviation

7 ☐	PMAC: Configure the fdc.cfg file	Configure the <idih_fdc_file_name>.xml template file. See Appendix M: IDIH Fast Deployment Configuration for a breakdown of the parameters and a sample XML configuration file. Update the software versions, hostnames, bond interfaces, network addresses, and network VLAN information for the TVOE host and IDIH guests that you are installing. Also modify CPU, RAM and Virtual Disk information as shown below : <table border="1"> <thead> <tr> <th>IDIH</th><th>Profile Parameters (No. Of CPU, RAM, Virtual Disk)</th><th>XML Stanzas to Modify</th></tr> </thead> <tbody> <tr> <td>IDIH-Mediation</td><td>No. of CPUs: 2 Memory (MBs): 8192 MB Virtual Disks: 65536 MB</td><td> <pre> <cpus>2</cpus> <memory>8192</memory> <vdisk> <hostvolname>MED.img</hostvolname> <hostpool>vgguests</hostpool> <size>65536</size> <primary>yes</primary> <guestdevname>PRIMARY</guestdevname> </vdisk> </pre> </td></tr> <tr> <td>IDIH-Application</td><td>No. of CPUs: 2 Memory (MBs): 8192 MB Virtual Disks : 65536 MB</td><td> <pre> <cpus>2</cpus> <memory>8192</memory> <vdisk> <hostvolname>APP.img</hostvolname> <hostpool>vgguests</hostpool> <size>65536</size> <primary>yes</primary> <guestdevname>PRIMARY</guestdevname> </vdisk> </pre> </td></tr> <tr> <td>IDIH-Database</td><td>No. of CPUs: 4 Memory (MBs): 8192 MB Virtual Disks: 166926 MB (102400 MB for ORA_SDB and 65536 MB for ORA)</td><td> <pre> <cpus>2</cpus> <memory>8192</memory> <vdisk> <hostvolname>ORA.img</hostvolname> <hostpool>vgguests</hostpool> <size>65536</size> <primary>yes</primary> <guestdevname>PRIMARY</guestdevname> </vdisk> <vdisk> <hostvolname>ORA_sdb.img</hostvolname> <hostpool>vgguests</hostpool> <size>102400</size> <primary>yes</primary> <guestdevname>PRIMARY</guestdevname> </vdisk> </pre> </td></tr> </tbody> </table>	IDIH	Profile Parameters (No. Of CPU, RAM, Virtual Disk)	XML Stanzas to Modify	IDIH-Mediation	No. of CPUs: 2 Memory (MBs): 8192 MB Virtual Disks: 65536 MB	<pre> <cpus>2</cpus> <memory>8192</memory> <vdisk> <hostvolname>MED.img</hostvolname> <hostpool>vgguests</hostpool> <size>65536</size> <primary>yes</primary> <guestdevname>PRIMARY</guestdevname> </vdisk> </pre>	IDIH-Application	No. of CPUs: 2 Memory (MBs): 8192 MB Virtual Disks : 65536 MB	<pre> <cpus>2</cpus> <memory>8192</memory> <vdisk> <hostvolname>APP.img</hostvolname> <hostpool>vgguests</hostpool> <size>65536</size> <primary>yes</primary> <guestdevname>PRIMARY</guestdevname> </vdisk> </pre>	IDIH-Database	No. of CPUs: 4 Memory (MBs): 8192 MB Virtual Disks: 166926 MB (102400 MB for ORA_SDB and 65536 MB for ORA)	<pre> <cpus>2</cpus> <memory>8192</memory> <vdisk> <hostvolname>ORA.img</hostvolname> <hostpool>vgguests</hostpool> <size>65536</size> <primary>yes</primary> <guestdevname>PRIMARY</guestdevname> </vdisk> <vdisk> <hostvolname>ORA_sdb.img</hostvolname> <hostpool>vgguests</hostpool> <size>102400</size> <primary>yes</primary> <guestdevname>PRIMARY</guestdevname> </vdisk> </pre>
IDIH	Profile Parameters (No. Of CPU, RAM, Virtual Disk)	XML Stanzas to Modify												
IDIH-Mediation	No. of CPUs: 2 Memory (MBs): 8192 MB Virtual Disks: 65536 MB	<pre> <cpus>2</cpus> <memory>8192</memory> <vdisk> <hostvolname>MED.img</hostvolname> <hostpool>vgguests</hostpool> <size>65536</size> <primary>yes</primary> <guestdevname>PRIMARY</guestdevname> </vdisk> </pre>												
IDIH-Application	No. of CPUs: 2 Memory (MBs): 8192 MB Virtual Disks : 65536 MB	<pre> <cpus>2</cpus> <memory>8192</memory> <vdisk> <hostvolname>APP.img</hostvolname> <hostpool>vgguests</hostpool> <size>65536</size> <primary>yes</primary> <guestdevname>PRIMARY</guestdevname> </vdisk> </pre>												
IDIH-Database	No. of CPUs: 4 Memory (MBs): 8192 MB Virtual Disks: 166926 MB (102400 MB for ORA_SDB and 65536 MB for ORA)	<pre> <cpus>2</cpus> <memory>8192</memory> <vdisk> <hostvolname>ORA.img</hostvolname> <hostpool>vgguests</hostpool> <size>65536</size> <primary>yes</primary> <guestdevname>PRIMARY</guestdevname> </vdisk> <vdisk> <hostvolname>ORA_sdb.img</hostvolname> <hostpool>vgguests</hostpool> <size>102400</size> <primary>yes</primary> <guestdevname>PRIMARY</guestdevname> </vdisk> </pre>												

Appendix Q.4.1 IDIH Installation: Procedure 58 Deviation

8 ☐	PMAC: Run the fdconfig.	Run the fdconfig configuration by executing the following commands: <pre>\$ screen \$ sudo fdconfig config --file=<idih_fdc_file_name>.xml Example: \$ sudo fdconfig config --file=tvoe-ferbrms4 01-22-15.xml</pre> Note: This is a long duration command. If the screen command was run prior to executing the fdconfig, perform a “<i>screen -dr</i>” to resume the screen session in the event of a terminal timeout etc.
9 ☐	PMAC GUI: Monitor the Configuration	If not already done so, establish a GUI session on the PMAC server. Navigate to Main Menu -> Task Monitoring  The screenshot shows a dark blue GUI window titled 'Main Menu'. It contains four items: 'Status and Manage' (with a folder icon), 'Task Monitoring' (with a document icon and highlighted in blue), 'Help' (with a question mark icon), and 'Logout' (with a door icon). Monitor the IDIH configuration to completion.

Appendix R: VM Automation Profile Values

Server profile values defined in VM automation .cfg file.

Note: It is recommended that there should be no deviation in the values defined in the VM automation .cfg file from the values defined above.

CPU	MEMORY	VDISK
DSR NOAM		
DSR_VIRT_NOAM_CPU="4"	DSR_VIRT_NOAM_MEM="6144"	DSR_VIRT_NOAM_VDISK="71680"
DSR SOAM		
DSR_VIRT_SOAM_CPU="4"	DSR_VIRT_SOAM_MEM="6144"	DSR_VIRT_SOAM_VDISK="71680"
DSR DAMP		
DSR_VIRT_DAMP_CPU="12"	DSR_VIRT_DAMP_MEM="24576"	DSR_VIRT_DAMP_VDISK="71680"
DSR SS7MP		
DSR_VIRT_SS7MP_CPU="12"	DSR_VIRT_SS7MP_MEM="24576"	DSR_VIRT_SS7MP_VDISK="71680"
DSR IPFE		
DSR_VIRT_IPFE_CPU="4"	DSR_VIRT_IPFE_MEM="16384"	DSR_VIRT_IPFE_VDISK="71680"
DSR SESSION SBR		
DSR_VIRT_SBR_SESSION_CPU="1 4"	DSR_VIRT_SBR_SEESION_MEM="3276 8"	DSR_VIRT_SBR_SESSION_VDISK="7168 0"
DSR BINDING SBR		
DSR_VIRT_SBR_BINDING_CPU="1 2"	DSR_VIRT_SBR_BINDING_MEM="2560 0"	DSR_VIRT_SBR_BINDING_VDISK="7168 0"
SDS NOAM		
SDS_VIRT_NOAM_CPU="4"	SDS_VIRT_NOAM_MEM="16384"	SDS_VIRT_NOAM_VDISK="204800"
SDS SOAM		
SDS_VIRT_SOAM_CPU="4"	SDS_VIRT_SOAM_MEM="10240"	SDS_VIRT_SOAM_VDISK="71680"
SDS DP		
SDS_VIRT_DP_CPU="6"	SDS_VIRT_DP_MEM="102400"	SDS_VIRT_DP_VDISK="71680"
SDS QUERY SERVER		
SDS_VIRT_QS_CPU="4"	SDS_VIRT_QS_MEM="16384"	SDS_VIRT_QS_VDISK="102400"

Table 4: VM Automation Profile Values

Appendix S: VM placement in HP DL380 Gen8/Gen9 (Onboard 1Gbps NICs) and CPU Pinning in HP DL380 Gen9 (Onboard 1Gbps NICs)

HP DL380 Gen8 and HP DL380 DL380 Gen9 rack mount server solutions should place VMs in one of the following deployment scenarios:

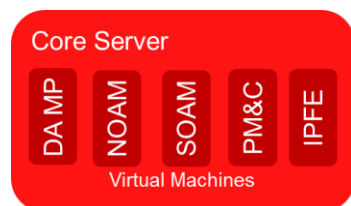


Figure 5. HP DL380 Gen8/Gen9(1Gbps) VM placement non-HA LAB deployment

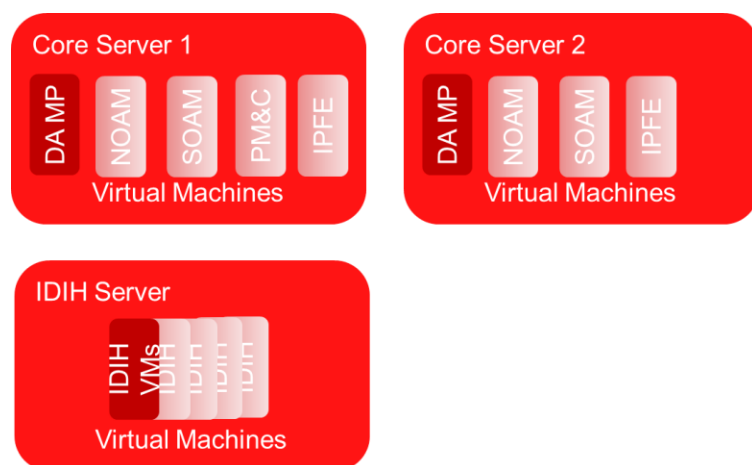


Figure 6. HP DL380 Gen8/Gen9(1Gbps) VM placement small production DSR with IDIH

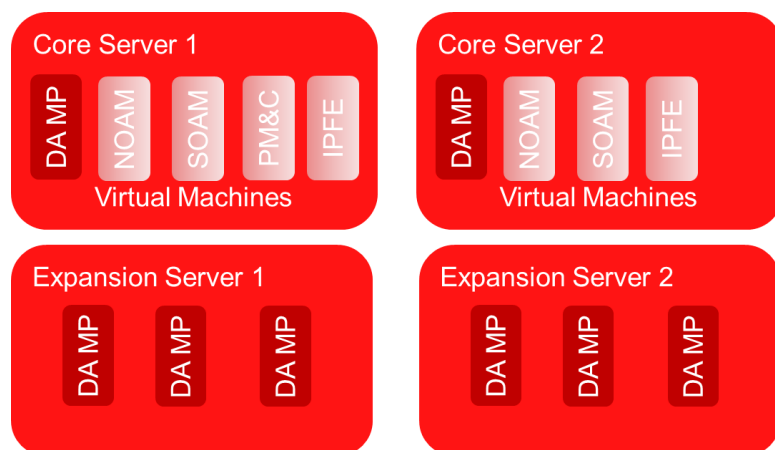


Figure 7. HP DL380 Gen8/Gen9(1Gbps) VM placement scaled DSR

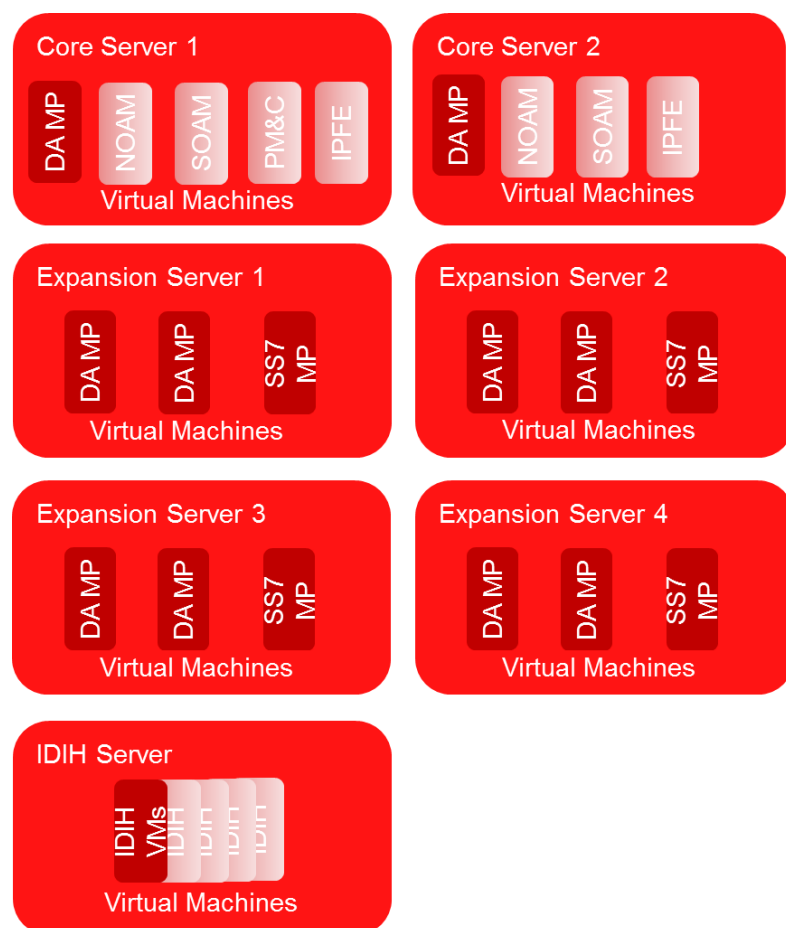


Figure 8. HP DL380 Gen9(1Gbps) VM placement scaled DSR with SS7 MPs and IDIH

Core Server 1		Core Server 2		Expansion Server 1		Expansion Server 2		IDIH Server	
Numa 0	Numa 1	Numa 0	Numa 1	Numa 0	Numa 1	Numa 0	Numa 1	Numa 0	Numa 1
NOAM	DAMP	NOAM	DAMP	DAMP	DAMP	DAMP	DAMP	IDIH-A	
SOAM		SOAM			DAMP		DAMP	IDIH-M	
IPFE		IPFE						IDIH-DB	
PMAC									

Table 5.HP DL380 Gen9 (1Gbps) CPU Pinning without SS7MPs

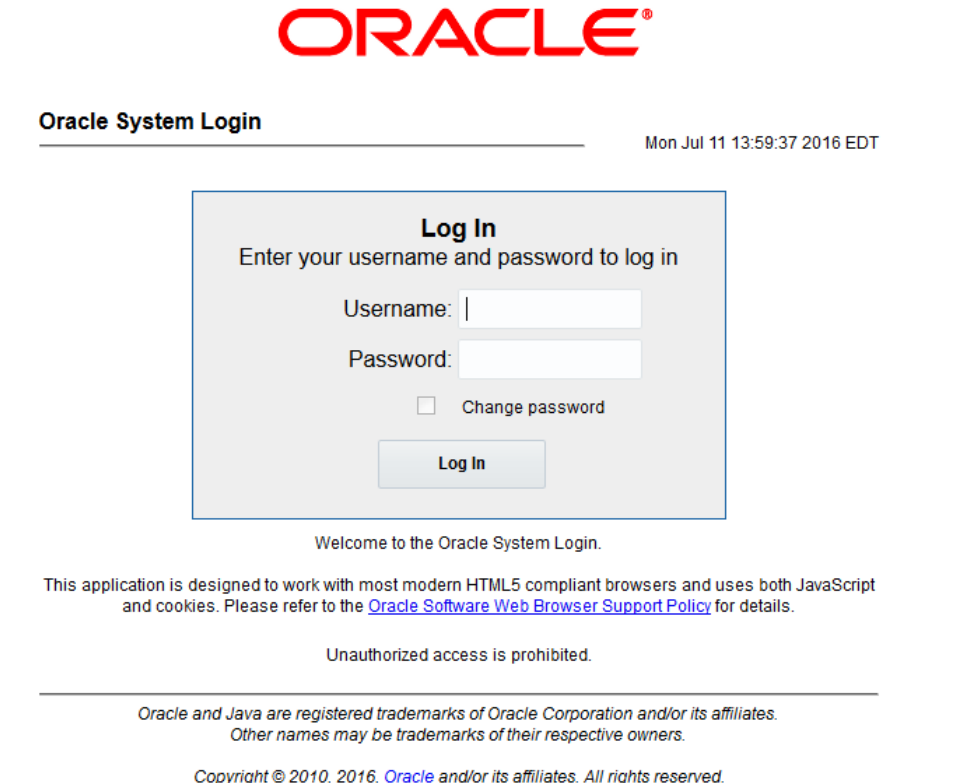
Core Server 1		Core Server 2		Expansion Server 1		Expansion Server 2		Expansion Server 3		Expansion Server 4		IDIH Server	
Numa 0	Numa 1	Numa 0	Numa 1	Numa 0	Numa 1	Numa 0	Numa 1	Numa 0	Numa 1	Numa 0	Numa 1	Numa 0	Numa 1
NOAM	DAMP	NOAM	DAMP	DAMP	DAMP	DAMP	DAMP	DAMP	DAMP	DAMP	DAMP	IDIH-A	
SOAM		SOAM			SS7MP		SS7MP		SS7MP		SS7MP	IDIH-M	
IPFE		IPFE										IDIH-DB	
PMAC													

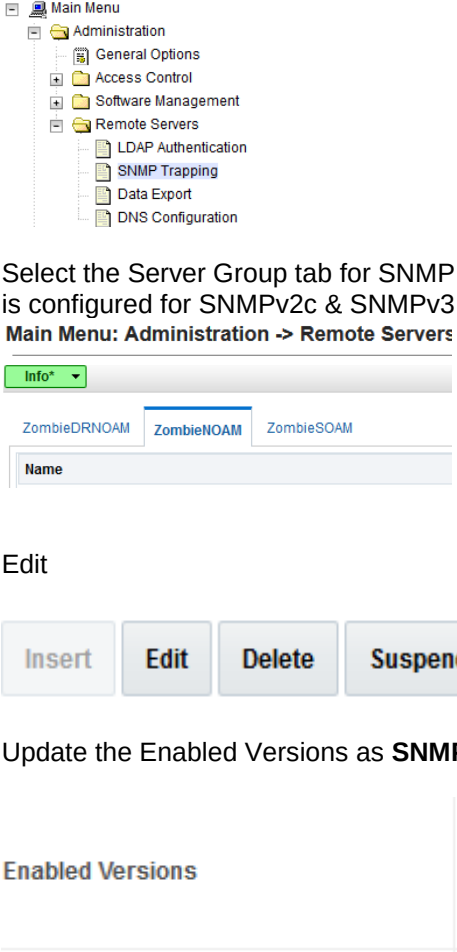
Table 6.HP DL380 Gen9 (1Gbps) CPU Pinning with SS7MPs

Refer CPU Pinning to perform the pinning.

Appendix T: Restoring SNMP configuration to SNMPv3 (Optional)

S T E P #	This procedure will provide the steps to restore SNMP configuration to SNMPv3 for forwarding of SNMP Traps from each individual server. NOTE: If SNMP is configured with SNMPv2c and SNMPv3 as enabled versions as a work around step (section 4.14.10, steps 5-8) and the SNMPv3 is required to be configured Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Appendix U: My Oracle Support (MOS) and ask for assistance.

1 ☐	(Workaround) PRIMARY NOAM VIP GUI: Login	NOTE: This workaround step should be performed only in the following case: 1) If SNMP is configured with SNMPv2c and SNMPv3 as enabled versions as a work around step (section 4.14.10, steps 5-8) and the SNMPv3 is required to be configured Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of < NOAM_XMI_VIP_IP_Address >: Login as the guiadmin user: 
2	NOAM VIP GUI:	

☐	Configure System-Wide SNMP Trap Receiver(s)	Navigate to Main Menu -> Administration -> Remote Servers -> SNMP Trapping  Select the Server Group tab for SNMP trap configuration (The Server Group that is configured for SNMPv2c & SNMPv3 as a workaround): Main Menu: Administration -> Remote Servers Info* ZombieDRNOAM ZombieNOAM ZombieSOAM Name Edit Insert Edit Delete Suspend Resume Update the Enabled Versions as SNMPv3: Enabled Versions SNMPv3 Press OK

Appendix U: 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 <https://www.oracle.com/us/support/contact/index.html>.

When calling, there are multiple layers of menus selections. Make the selections in the sequence shown below on the Support telephone menu:

- 1) For the first set of menu options, select 2, "New Service Request". You will hear another set of menu options.
- 2) In this set of menu options, select 3, "Hardware, Networking and Solaris Operating System Support". A third set of menu options begins.
- 3) In the third set of options, select 2, "Non-technical issue". Then you will be connected to a live agent who can assist you with MOS registration and provide Support. Identifiers. Simply mention you are a Tekelec Customer new to MOS.

