Oracle® Communications

Diameter Signaling Router

Rack Mount Installation Guide

Release 8.4

F12328-02

July 2020

Oracle Communications DSR Rack Mount Server Installation Guide, Release 8.4

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

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

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

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

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

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

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

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

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

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

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

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

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

See more information My Oracle Support (MOS).

Table of Contents

1. Introduction 11
1.1 References 11
1.2 Acronyms 12
1.3 Terminology 13
1.4 How to Use this Document 14
1.5 Optional Features 15
2. General Description 16
2.1 Acquiring Firmware 16
2.1.1 HP DL380 16
2.1.2 Oracle X5-2/Netra X5-2/X6-2/X7-2 17
2.2 Hardware Requirements 17
2.2.1 Required Materials 17
2.2.2 Rack Mount Server Network Interface Reference 18
3. Software Installation Procedure 18
3.1 Prepare Servers for IPM 18
3.1.1 Configure BIOS Settings 19
3.1.2 Upgrade Rack Mount Server Firmware 21
3.2 Install and Configure TVOE on First RMS (PMAC Host) 22
3.3 Install PMAC 39
3.4 Initialize the PMAC Application 44
3.5 Configure Cisco 4948E-F Aggregation Switches (HP DL380 Gen 8 Servers Only) 46
3.5.1 Configure netConfig Repository (HP DL380 Gen 8 Servers Only) 46
3.5.2 Configure Cisco 4948E-F Aggregation Switches (HP DL380 Gen 8 Servers Only) 55
3.6 Configure PMAC Server (NetBackup Only) 61
3.7 Add a Rack Mount Server to PMAC 66
3.8 Install TVOE on Additional Rack Mount Servers 70
3.9 Configure TVOE on Additional Rack Mount Servers 75
3.10 Determine VM Placement 87
3.11 Deploy Redundant PMAC (Optional) 88
3.12 Virtual Machine/Network Fast Deployment 95
3.13 CPU Pinning 103
3.14 DSR Application Configuration 107
3.14.1 NOAM Configuration 107
3.14.2 NetBackup Client Installation (Optional) 122
3.14.3 Disaster Recovery NOAM (Optional) 123
3.14.4 SOAM Configuration 131

3.14.5 Activate PCA ... 144
3.14.6 Activate DCA ... 144
3.14.7 MP Configuration ... 144
3.14.8 Signaling Network Configuration ... 169
3.14.9 DSCP Configuration (Optional) ... 170
3.14.10 SNMP Configuration ... 174
3.14.11 IPFE Configuration (Optional) ... 180
3.15 SDS Application Configuration ... 185
3.15.1 NOAM Configuration ... 185
3.15.2 NetBackup Client Installation (Optional) ... 199
3.15.3 Disaster Recovery NOAM (Optional) ... 200
3.15.4 Query Server Configuration ... 207
3.15.5 SOAM Configuration ... 215
3.15.6 DP Configuration ... 224
3.15.7 DSCP Configuration (Optional) ... 227
3.15.8 SNMP Configuration (Optional) ... 230
3.16 IDIH Installation and Configuration (Optional) ... 232
3.16.1 IDIH Installation ... 232
3.16.2 IDIH Configuration ... 237
3.17 Post Installation Procedures ... 255
3.17.1 Optimization (DSR and Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 (10Gbps) Only) ... 255
3.17.2 Configure ComAgent Connections (DSR and SDS Only) ... 256
3.17.3 Activate Optional Features ... 261
3.17.4 Shared Secret Encryption Key Revocation (RADIUS Only) ... 261
3.17.5 Enable/Disable DTLS (SCTP Diameter Connections Only) ... 262
3.17.6 Back Up TVOE Configuration ... 262
3.17.7 Back Up PMAC Application ... 264
3.17.8 Back Up NOAM Database ... 266
3.17.9 Back Up SOAM Database ... 269
Appendix A. Pre-IPM Procedures ... 272
Appendix A.1 Set the Server’s CMOS Clock ... 272
Appendix A.2 Configure the RMS Server BIOS Settings ... 272
Appendix A.2.1 Configure HP Gen 8 Servers ... 272
Appendix A.2.2 Configure HP Gen 9 Servers ... 274
Appendix A.2.3 Configure Oracle X5-2/Netra X5-2/X6-2/X7-2 Server ... 277
Appendix B. Upgrade Server Firmware ... 281

- Appendix B.1 HP DL380 Server 281
- Appendix B.2 Oracle X5-2/Netra X5-2/X6-2/X7-2 287

Appendix C. Change the SNMP Configuration Settings 287

Appendix D. TVOE iLO/iLOM GUI Access 289

- Appendix D.1 Access the iLO GUI (HP DL380) 289
- Appendix D.2 Access the iLOM GUI (Oracle X5-2/Netra X5-2/X6-2/X7-2) 290

Appendix E. Change the TVOE iLO/iLOM Address 293

- Appendix E.1 HP DL380 Servers (iLO4) 293
- Appendix E.2 Oracle X5-2/Netra X5-2/X6-2 Servers (Change iLOM IP Address using Keyboard/Monitor) 296
- Appendix E.3 Oracle X5-2/Netra X5-2/X6-2/X7-2 Servers (Change iLOM IP Address using Serial Console) 300

Appendix F. Attach an ISO Image to a Server using the iLO or iLOM 302

- Appendix F.1 HP DL380 Servers (iLO4) 302
- Appendix F.2 Oracle X5-2/Netra X5-2/X6-2/X7-2 Servers (iLOM) 304

Appendix G. Configure TVOE iLO Access 308

Appendix H. SNMP Configuration 310

Appendix I. Install NetBackup Client 313

- Appendix I.1 Install NetBackup Client Using platcfg 313
- Appendix I.2 Install NetBackup Client Using NBAutoInstall 320
- Appendix I.3 Create NetBackup Client Configuration File 321
- Appendix I.4 Configure PMAC Application NetBackup Virtual Disk 322

Appendix J. List of Frequently Used Time Zones 326

Appendix K. Upgrade Cisco 4948 PROM 328

Appendix L. Sample Network Element 331

Appendix M. Configure IDIH Fast Deployment 332

Appendix N. Create a Bootable USB Drive on Linux 342

Appendix O. Remove IDIH External Drive 343

Appendix P. Growth/De-Growth/Re-Shuffle (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 (10Gbps) Only) 346

- Appendix P.1 Growth (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 (10Gbps) Only) 346
- Appendix P.2 De-Growth (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 (10Gbps) Only) 364
- Appendix P.3 Re-Shuffle (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 (10Gbps) Only) 384

Appendix Q. Non-HA Lab Node Instructions (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 (10Gbps) Non-HA Lab Node Only) 412

- Appendix Q.1 Non-HA Lab Node Pre-IPM Procedures 412
- Appendix Q.2 Non-HA Lab Node PMAC Deployment 429
- Appendix Q.3 Non-HA Lab Node VM Automation Profile Values 433

Appendix Q.4 Non-HA Lab Node IDIH Procedure Deviation 434
Appendix R. VM Automation Profile Values 438
Appendix S. VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1Gbps NICs) 439
Appendix T. Restore SNMP Configuration to SNMPv3 (Optional) 441
Appendix U. CPU Pinning in HP DL380 Gen 9 (Onboard 1Gbps NICs) 442
Appendix V. netConfig backupConfiguration/restoreConfiguration/upgradeFirmware with TPD Cipher Change 443
Appendix W. My Oracle Support (MOS) 444

List of Tables

Table 1. Acronyms 12
Table 2. Terminology 13
Table 3. Optional Features 15
Table 4. RMS Network Interfaces 18
Table 5. List of Selected Time Zone Values 326
Table 6. VM Automation Profile Values 438
Table 7. HP DL380 Gen 9 (1Gbps) CPU Pinning without SS7MPs 442
Table 8. HP DL380 Gen 9 (1Gbps) CPU Pinning with SS7MPs 443

List of Figures

Figure 1. Example Procedure Steps Used in This Document 15
Figure 2. Initial Application Installation Path-Example Shown 16
Figure 3. Example Network Element XML File 331
Figure 4. HP DL380 Gen 8/Gen 9 (1Gbps) VM Placement Non-HA LAB Deployment 439
Figure 5. HP DL380 Gen 8/Gen 9 (1Gbps) VM Placement Small Production DSR with IDIH 439
Figure 6. HP DL380 Gen 8/Gen 9 (1Gbps) VM Placement Scaled DSR 440
Figure 7. HP DL380 Gen 9 (1Gbps) VM Placement Scaled DSR with SS7 MPs and IDIH 440

List of Procedures

Procedure 1. Configure BIOS Settings 19
Procedure 2. Upgrade Rack Mount Server Firmware 21
Procedure 3. Install and Configure TVOE on First RMS (PMAC Host) 22
Procedure 4. Configure First Rack Mount Server 26
Procedure 5. PMAC Deployment 39
Procedure 6. Initialize PMAC 44

Procedure 7. Configure netConfig Repository (HP DL380 Gen 8 Servers Only) 48
Procedure 8. Configure Cisco 4948E-F Aggregation Switches-netConfig (HP DL380 Servers Only) 56
Procedure 9. Configure the PMAC Server (NetBackup Only) 61
Procedure 10. Add RMS to the PMAC System Inventory... 66
Procedure 11. Restore an Archive That Does Not Contain a Current User 70
Procedure 12. Configure TVOE on Additional Rack Mount Servers 75
Procedure 13. Install a Redundant PMAC 88
Procedure 14. Load DSR, SDS, and TPD ISOs onto the PMAC Server 95
Procedure 15. Execute VM/Network Fast Deployment 98
Procedure 16. Load DSR, SDS, and TPD ISOs onto the PMAC Server 103
Procedure 17. Configure First DSR NOAM NE and Server.. 107
Procedure 18. Configure the DSR NOAM Server Group.. 113
Procedure 19. Configure Second DSR NOAM Server 117
Procedure 20. Complete DSR NOAM Server Group Configuration 120
Procedure 21. Install NetBackup Client (Optional) 122
Procedure 22. Configure DSR NOAM for DR Site (Optional) 123
Procedure 23. Pairing for DSR DR NOAM Site (Optional) 127
Procedure 24. Configure DSR SOAM NE... 131
Procedure 25. Configure DSR SOAM Server 133
Procedure 26. Configure the DSR SOAM Server Group.. 138
Procedure 27. Configure RMS-Specific B-Level Resources (HP DL380 Gen 8 Servers Only) 143
Procedure 28. Activate PCA 144
Procedure 29. Activate DCA 144
Procedure 30. Configure Places and Assign MP Servers to Places (PCA and DCA Only) 145
Procedure 31. Configure DAMP Server Groups and Profiles 148
Procedure 32. Configure IPFE Server Groups 152
Procedure 33. Configure SS7-MP Server Groups and Profiles 156
Procedure 34. Configure Session SBR Server Groups 162
Procedure 35. Configure Binding SBR Server Groups 166
Procedure 36. Configure DSCP Values for Outgoing Traffic (Optional) 170
Procedure 37. Configure SNMP Trap Receivers 174
Procedure 38. Configure IPFE (Optional) 180
Procedure 39. Configure First SDS NOAM NE and Server.. 185
Procedure 40. Configure the SDS NOAM Server Group.. 190
Procedure 41. Configure Second SDS NOAM Server.. 193
Procedure 42. Complete SDS NOAM Server Group Configuration 196
Procedure 43. Install NetBackup Client (Optional) 199

Procedure 44. Configure SDS NOAM for DR Site (Optional) ... 200
Procedure 45. Pairing for SDS DR NOAM Site (Optional) ... 204
Procedure 46. Configure SDS Query Server ... 207
Procedure 47. Pair SDS Query Server with SDS NOAMs ... 212
Procedure 48. Configure SDS DP SOAM NE ... 215
Procedure 49. Configure SDS DP SOAM Server ... 217
Procedure 50. Configure the SDS DP SOAM Server Group ... 222
Procedure 51. Configure the SDS DP Server Group ... 225
Procedure 52. Configure DSCP Values for Outgoing Traffic (Optional) ... 227
Procedure 53. Configure SNMP Trap Receivers (Optional) ... 230
Procedure 54. IDIH Installation ... 233
Procedure 55. Configure DSR Reference Data Synchronization for IDIH ... 237
Procedure 56. Configure the SSO Domain ... 241
Procedure 57. Configure in DSR ... 247
Procedure 58. Configure Mail Server (Optional) ... 250
Procedure 59. Change SNMP Management Server (Optional) ... 251
Procedure 60. Change Network Interface (Optional) ... 252
Procedure 61. Back Up the Upgrade and Disaster Recovery FDC File (Optional) ... 253
Procedure 62. Optimization Procedure ... 255
Procedure 63. Configure ComAgent Connections ... 256
Procedure 64. Activate Optional Features ... 261
Procedure 65. Shared Secret Encryption Key Revocation (RADIUS Only) ... 261
Procedure 66. Enable/Disable DTLS (SCTP Diameter Connections Only) ... 262
Procedure 67. Back Up TVOE Configuration ... 262
Procedure 68. Back Up PMAC Application ... 264
Procedure 69. Back Up NOAM Database ... 266
Procedure 70. Back Up SOAM Database ... 269
Procedure 71. Configure HP Gen 8 Server BIOS Settings ... 272
Procedure 72. Configure HP Gen 8 Server BIOS Settings ... 274
Procedure 73. Configure Oracle X5-2/Netra X5-2/X6-2/X7-2 Server BIOS Settings ... 277
Procedure 74. Enable Oracle Netra X5-2 CPU Power Limit for NEBS (Optional) ... 280
Procedure 75. Disable Oracle Netra X5-2/X6-2/X7-2 CPU Power Limit for NEBS (Optional) ... 280
Procedure 76. Upgrade HP DL380 Server Firmware ... 282
Procedure 77. Change SNMP Configuration Settings for HP DL380 ... 287
Procedure 78. Access the TVOE iLO4 GUI ... 289
Procedure 79. Access the iLOM GUI ... 290
Procedure 80. Change the TVOE iLO Address ... 293

Procedure 81. Change the TVOE Oracle X5-2/Netra X5-2/X6-2iLOM Address....................................296
Procedure 82. Change the TVOE Oracle X5-2/Netra X5-2/X6-2iLOM Address....................................300
Procedure 83. Mount HP DL380 Servers with ISO Image using iLO4 302
Procedure 84. Mount Oracle X5-2/Netra X5-2/X6-2/X7-2 Servers with ISO Image using iLOM..............304
Procedure 85. Connect to the TVOE iLO....................................308
Procedure 86. Configure SNMP 310
Procedure 87. Install NetBackup Client Using platcfg 313
Procedure 88. Install NetBackup Client Using NBAutoInstall....................................320
Procedure 89. Create NetBackup Client Configuration File 321
Procedure 90. Configure PMAC Application NetBackup Virtual Disk....................................322
Procedure 91. Configure PMAC Application NetBackup Virtual Disk....................................328
Procedure 92. Configure PMAC Application NetBackup Virtual Disk....................................342
Procedure 93. Remove the IDIH External Drive 343
Procedure 94. Perform Backups....................................347
Procedure 95. Perform Health Check 347
Procedure 96. Add a New TVOE Server/VMs 349
Procedure 97. Growth: DR NOAM....................................350
Procedure 98. Growth: SOAM Spare (DSR/PCA Only)....................................351
Procedure 99. Growth: MP/DP 352
Procedure 100. Growth: MP (For 7.x to 8.x Upgraded System)....................................353
Procedure 101. Growth: Query Server (SDS Only) 362
Procedure 102. Post Growth Health Check....................................362
Procedure 103. Post Growth Backups....................................364
Procedure 104. Perform Backups....................................364
Procedure 105. Perform Health Check 365
Procedure 106. Remove Server from Server Group 368
Procedure 107. Delete Server/Server Group....................................377
Procedure 108. Delete Server VM 380
Procedure 109. Post De-Growth Health Check 382
Procedure 110. Post De-Growth Backups....................................384
Procedure 111. Perform Backups....................................385
Procedure 112. Perform Health Check 385
Procedure 113. Add a New TVOE Server 387
Procedure 114. Place Server in OOS....................................388
Procedure 115. Delete Server VM 390
Procedure 116. Move/Re-Shuffle: Create/Configure VMs....................................392
Procedure 117. Move/Re-Shuffle: NOAM/DR NOAM....................................393

Procedure 118. Move/Re-Shuffle: SOAM 395
Procedure 119. Move/Re-Shuffle: MP/DP 397
Procedure 120. Move/Re-Shuffle: Query Server (SDS Only) 402
Procedure 121. Move/Re-Shuffle: iDIH 404
Procedure 122. Move/Re-Shuffle: PMAC 406
Procedure 123. Move/Re-Shuffle: Redundant PMAC 409
Procedure 124. Post Moving/Re-Shuffling Health Check 410
Procedure 125. Post Move/Re-Shuffle Backups 412
Procedure 126. RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X5-2/Netra X5-2) .. 412
Procedure 127. RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2) 417
Procedure 128. RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380) 422
Procedure 129. PMAC Deployment: Deviation 429
Procedure 130. iDIH Installation: Deviation 434
Procedure 131. Restore SNMP Configuration to SNMP v3 441
Procedure 132. Turn Off Cipher List Before backupConfiguation/restoreConfiguration/upgradeFirmware Command 443
Procedure 133. Resume Cipher List After backupConfiguation/restoreConfiguration/upgradeFirmware Command 444

1. Introduction

This document is a guide to describe procedures used to configure HP DL380 Gen 8/9 or Oracle Rack Mount Servers (RMS) to use with Oracle Communication Diameter Signaling Router. It is assumed that the hardware installation and network cabling were already executed. The audience for this document includes Oracle customers and 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 DL380 Gen 8/9 or Oracle rack mount servers.

Oracle X5-2/Netra X5-2/X6-2/X7-2/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/X7-2/HP DL380 Gen 9 (10Gbps) Only).

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

Disclaimer: To understand the capacity/performance impact of this software release, refer to DSR 8.4 bechmarking document.

1.1 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 2.2.12)

[2] HP Solutions Firmware Upgrade Pack, version 2.x.x (Min 2.2.12)

[3] Oracle Firmware Upgrade Pack Release Notes (Min 3.1.8)

[4] Oracle Firmware Upgrade Pack Upgrade Guide

[5] Communication Agent User's Guide

[6] DSR Communication Agent Configuration Guide

[7] DSR RBAR Feature Activation Procedure

[8] DSR MAP-Diameter Feature Activation Procedure

[9] DSR Mediation Feature Activation Procedure

[10] DSR FABR Feature Activation Procedure

[11] Gateway Location Application (GLA) Feature Activation

[12] DSR PCA Activation Guide

[13] 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

[18] TPD Initial Product Manufacture Software Installation Procedure

[19] DSR Security Guide

[20] DCA Framework and Application Activation and Deactivation Guide

[21] Oracle TPD Initial Product Manufacture Software Installation Procedure

[22] DSR Rack Mount Server Network Interconnect Guide

[23] DSR Benchmarking Guide

[24] C-Class Software Installation and Configuration Procedure 2/2

[25] DSR Initial Installation and Configuration Guide

1.2 Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

Acronym	Definition
BIOS	Basic Input Output System
DCA	Diameter Custom Applications
DSR	Diameter Signaling Router
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
FABR	Full Address Based Resolution
FRU	Field Replaceable Unit
GLA	Gateway Location Application
HIDS	Host Intrusion Detection System
IDIH	Integrated Diameter Intelligence Hub
iLO	Integrated Lights Out manager
IPFE	IP Front End
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
MAP-IWF	Map-Diameter Interworking
MSA	Modular Smart Array
NB	NetBackup
OA	HP Onboard Administrator
OS	Operating System (for example, TPD)
PCA	Policy and Charging Application
PMAC	Platform Management & Configuration
RBAR	Range Based Address Resolution
RMS	Rack Mounted Server
SAN	Storage Area Network
SBR	Session Binding Repository
SDS	Subscriber Database Server
SFTP	Secure File Transfer Protocol

Acronym	Definition
SNMP	Simple Network Management Protocol
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtual Operating Environment
VM	Virtual Machine
VSP	Virtual Serial Port

1.3 Terminology

An alphabetized list of terms used in the document.

Table 2. Terminology

Term	Definition
Enablement	The business practice of providing support services (hardware, software, documentation, etc.) that enable a 3rd party entity to install, configuration, and maintain Oracle products for Oracle customers.
Management Server	HP ProLiant DL380 or Oracle X5-2/ Netra X5-2/X6-2/X7-2 deployed to run TVOE and host a virtualized PMAC application.
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 and Charging DRA application defines two place association types: policy binding region and Policy and Charging mated sites.
PMAC Application	PMAC is an application that provides platform-level management functionality, such as the capability to manage and provision platform components of the system so it can host applications, for HP DL380 and the Oracle X5-2/Netra X5-2/X6-2/X7-2 system.
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 and 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 have a primary site.

Term	Definition
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 and 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 sites (places) 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 site redundancy is wanted, a secondary site is required for all SOAM and SBR server groups.
Session Binding Repository (SBR) Server Group Redundancy	The DCA and Policy and Charging applications may use SBR server groups to store application session data. The SBR server groups support both two and three site redundancy. The server group function name is **Session and Binding Repository**.
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 and 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.
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.
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 and 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 ensures there is always a functioning active server in a server group even if all the servers in a single site fail.

1.4 How to Use this Document

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

1. Before beginning a procedure, completely read the instructional text (it displays immediately after the **Section heading for each procedure) and all associated procedural WARNINGS or NOTES.**
2. **Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.**

3. **If a** procedural STEP fails to execute successfully or fails to receive the desired output, STOP the procedure. It is recommended to contact My Oracle Support (MOS) for assistance, as described in Appendix W before attempting to continue.

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

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

	Title/Instructions	**Directive/Result Steps**
1. ☐	Change directory	Change to the backout directory. `$ cd /var/TKLC/backout`
2. ☐	Verify network element data	1. View the Network Elements configuration data; verify the data; save and print report. 2. Select **Configuration > Network Elements** to view Network Elements Configuration screen.

Figure 1. Example Procedure Steps Used in This Document

1.5 Optional Features

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

Table 3. Optional Features

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

2. General Description

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.

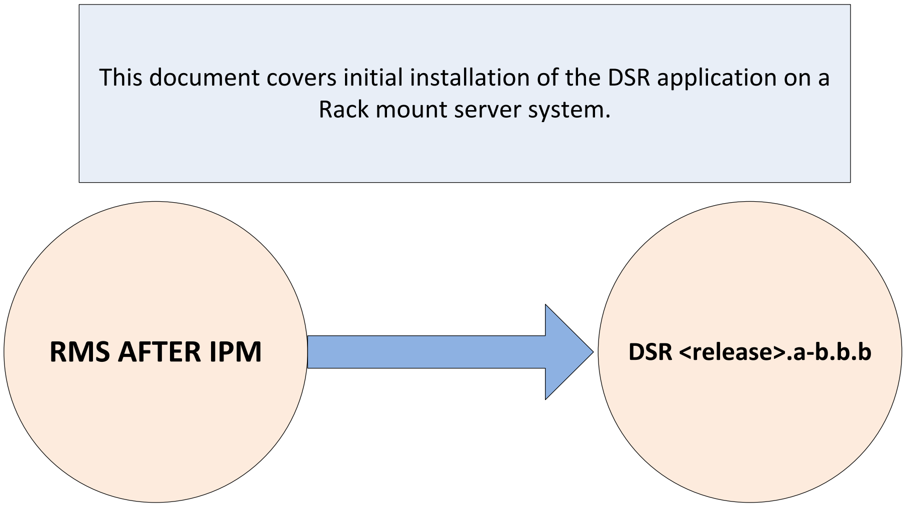

This document covers initial installation of the DSR application on a Rack mount server system.
RMS AFTER IPM
DSR <release>.a-b.b.b

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 2.2.12; however, if a firmware upgrade is needed, use the current GA release of the HP Solutions Firmware Upgrade Pack 2.x.x.

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

Contact 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/X7-2

The Oracle Firmware Upgrade Pack (FUP) consists of documentation to upgrade the Oracle rack mount servers. The pack consists of an upgrade guide and release notes. The current minimum supported release is 3.1.8; however, if a firmware update is required, use the latest available release. Firmware components can be downloaded from My Oracle Support (MOS) at https://support.oracle.com. Refer to the appropriate FUP release notes for directions on how to acquire the firmware.

2.2 Hardware Requirements

This section provides the required materials needed to install DSR on a rack mount system and provides the Ethernet interfaces depending on hardware type.

2.2.1 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]
10. Oracle Firmware Upgrade Pack Release Notes[3]
11. At least (1) Console cable and required software to connect to X7-2 blade

Other installation requirements to consider when installing DSR include:

- The total number of sites
- The number of servers at each site and their role(s)
- Does DSR's networking interface terminate on a Layer 2 or Layer 3 boundary?
- Number of enclosures at each site -- if any at all.
- Will NOAMs use rack-mount servers or server blades?
- (Per Site) Will MP's be in N+ 0 configurations?
- What time zone should be used across the entire collection of DSR sites?
- Will SNMP traps be viewed at the NOAM, or an external NMS be used? (Or both?)

2.2.2 Rack Mount Server Network Interface Reference

Throughout the installation procedure, configuration steps reference Ethernet interfaces. Depending on the hardware type, these Ethernet interfaces can vary. Refer to [22] for more details on network interconnect.

Table 4 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.

Table 4. RMS Network Interfaces

Network Interface	HP DL380 (with 4pt Gigabit in PCI Slot 1) (Gen 8/Gen 9 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)	Oracle X7-2
<ethernet_interface_1>	eth01	eth05	eth01	eth02
<ethernet_interface_2>	eth02	eth06	eth03	eth03
<ethernet_interface_3>	eth11	eth31	eth02	
<ethernet_interface_4>	eth12	eth32	eth04	

Note: When VE-DSR is deployed, in order for the PM&C to manage all Rack Mount Servers (RMS), the Customer's switch ports connected to bond0 NICs must be configured with the control VLAN as the native VLAN.

3. 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

Standard IPv6 formats for IPv6 and prefix can be used in all IP configuration screens, which enable DSR to be run in an IPv6 only environment. When using IPv6 for XMI and management, place the IPv6 address in brackets (highlighted in red below) as shown.

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

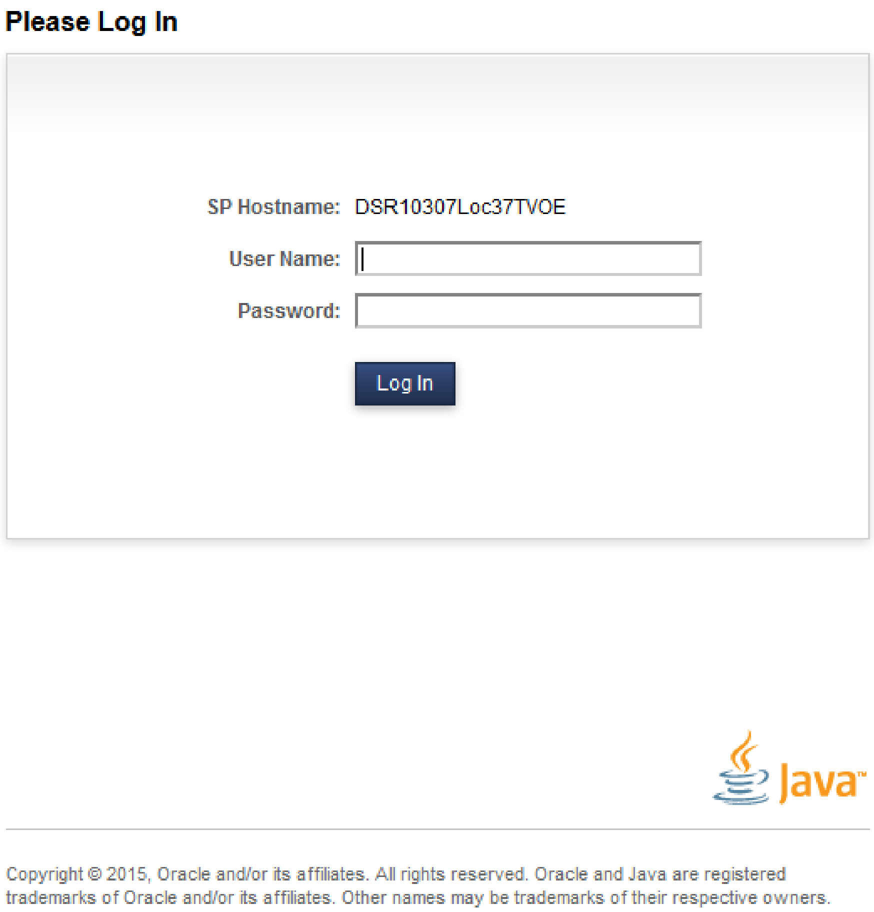
If a dual-stack (IPv4 and IPv6) network is required, configure the topology with IPv4 and then migrate to IPv6. Refer to [13] for instructions on how to accomplish this IPv6 migration.

3.1 Prepare Servers for IPM

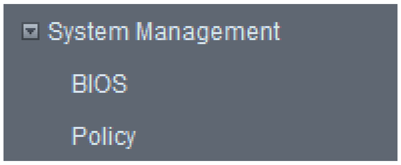
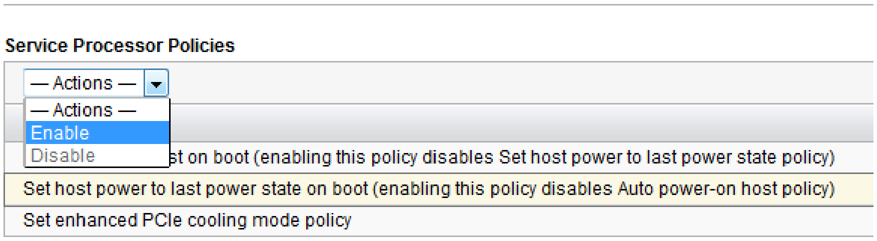
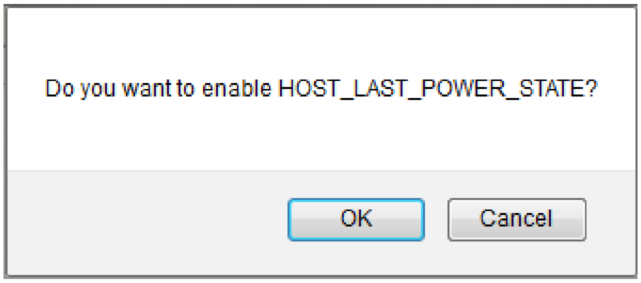
This section explains the steps needed to configure the BIOS settings and update the firmware (if needed) for the HP and Oracle rack mount servers.

3.1.1 Configure BIOS Settings

Procedure 1. Configure BIOS Settings

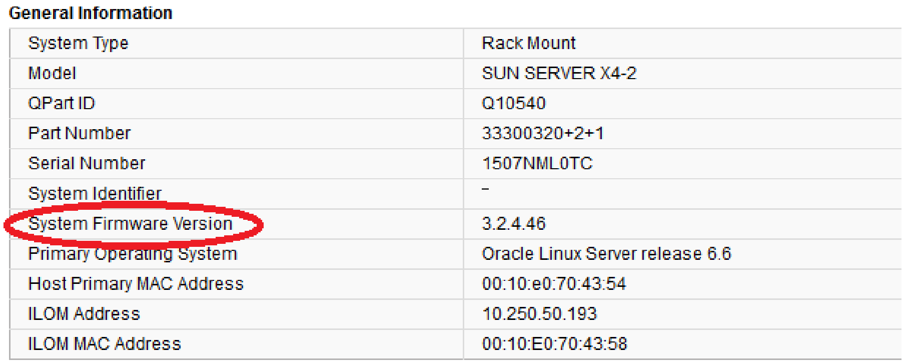
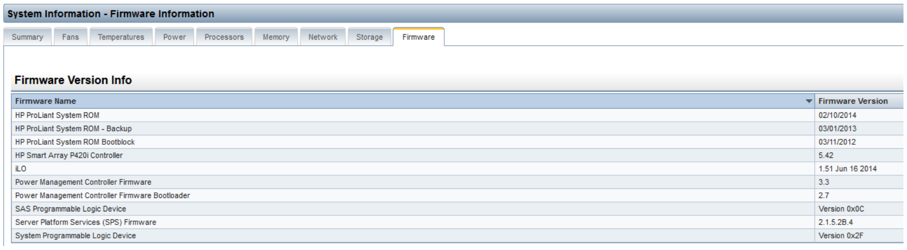
This procedure Configures HP DL380, Oracle/Netra servers, and Oracle server BIOS settings. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**RMS Server**: Configure the BIOS settings	Follow the appropriate appendix procedure for the corresponding hardware type: • **HP DL380 Gen 8 RMS**: Appendix A.2.1 Configure HP Gen 8 Servers • **HP DL380 Gen 9 RMS**: Appendix A.2.2 Configure HP Gen 9 Servers • **Oracle X5-2/Netra X5-2/X6-2/X7-2**: Appendix A.2.3 Configure Oracle X5-2/Netra X5-2/X6-2/X7-2 Server
2. ☐	**Oracle X5-2/Netra X5-2/X6-2 Server**: Login HP DL380 skip this step	Log into the Oracle X5-2/Netra X5-2/X6-2/X7-2 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 BIOS Settings

3. ☐	**Oracle X5-2/Netra X5-2/X6-2 Server**: Update power settings HP DL380 skip this step	1. Navigate to **System Management > Policy**.  System Management BIOS Policy 2. Select **Set host power to last power state on boot**.  Service Processor Policies — Actions — — Actions — Enable Disable st on boot (enabling this policy disables Set host power to last power state policy) Set host power to last power state on boot (enabling this policy disables Auto power-on host policy) Set enhanced PCIe cooling mode policy 3. Select the **Enable from the Actions** option. 4. Click **OK** to confirm.  Do you want to enable HOST_LAST_POWER_STATE?

3.1.2 Upgrade Rack Mount Server Firmware

Procedure 2. Upgrade Rack Mount Server Firmware

<table>
<tr><td colspan="3">This procedure updates 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr>
<td>1.
☐</td>
<td>RMS Server: Verify firmware of the rack mount server</td>
<td>For Oracle X5-2/Netra X5-2/X6-2/X7-2
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].


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>2.1.5.2B.4</td></tr>
<tr><td>System Programmable Logic Device</td><td>Version 0x2F</td></tr>
</table>
</td>
</tr>
<tr>
<td>2.
☐</td>
<td>RMS Server: Upgrade firmware</td>
<td>Follow the appropriate appendix procedure for the corresponding hardware type:
• HP DL380 Gen 8/9 RMS: Appendix B.1 HP DL380 Server
• Oracle Rack Mount Servers: Appendix B.2 Oracle X5-2/Netra X5-2/X6-2/X7-2</td>
</tr>
</table>

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

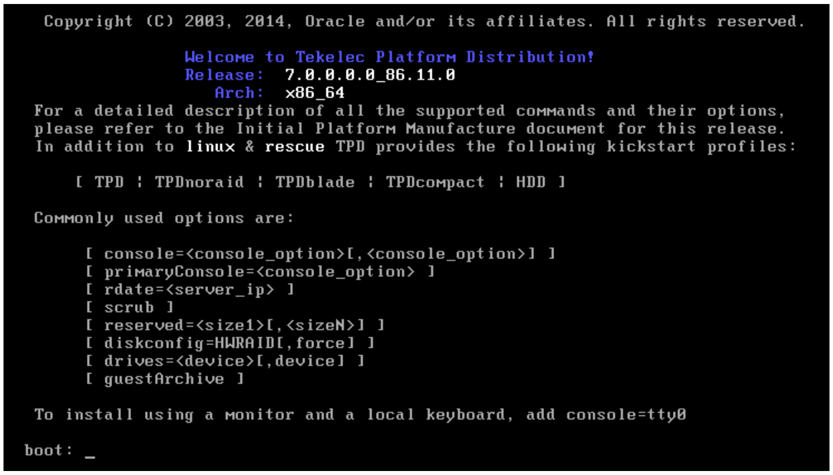
Throughout this section, the first RMS server refers to the server hosting the PMAC VM.

Note: **Non-HA Lab Node Installations Only-Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 GEN 9**: Before starting Procedure 3, execute Appendix Q.1 Non-HA Lab Node Pre-IPM Procedures to create vgguests logical volume with RAID10 spanning across multiple HDDs:

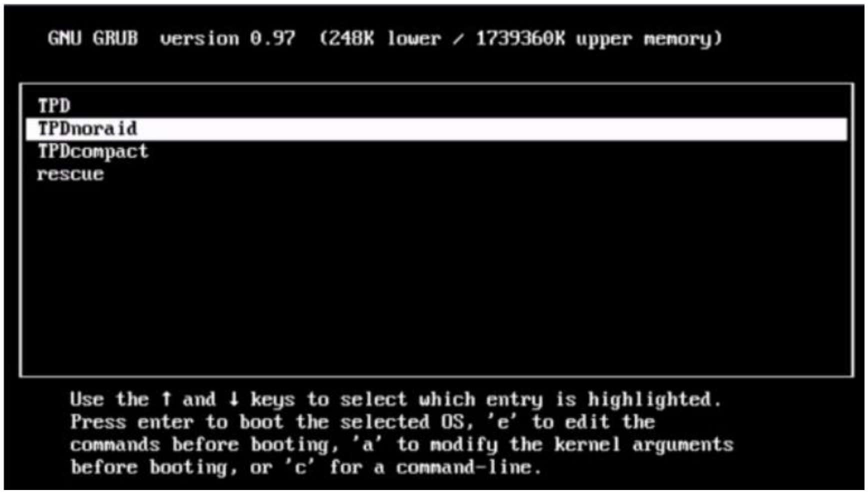
Procedure 3. Install and Configure TVOE on First RMS (PMAC Host)

This procedure installs TVOE on the first 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Connect to the 1st RMS server	Connect to the server using a VGA display and USB keyboard, or using the iLO interface on a browser. ***Note:*** Appendix D TVOE iLO/iLOM GUI Access and Appendix E Change the TVOE iLO/iLOM Address explain 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 Create a Bootable USB Drive on Linux for creating a bootable USB Alternatively, ISO can be mounted using virtual media. Refer to Appendix F Attach an ISO Image to a Server using the iLO or iLOM. ***Note:*** If using Appendix F, skip to step 5. in this procedure.
3. ☐	Power cycle 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, press the power button, and release it again to power on the system. In a second or 2 the **OK** LED starts to blink faster as the system powers up.
4. ☐	Select boot method	For some servers, you must select a boot method so the server does not boot directly from the hard drive. For **HP rack mount servers**, press **F11** when asked to bring up the boot menu and select the appropriate boot method. For **Oracle rack mount servers**, press **F8** when asked to bring up the boot menu and select the appropriate boot method.

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

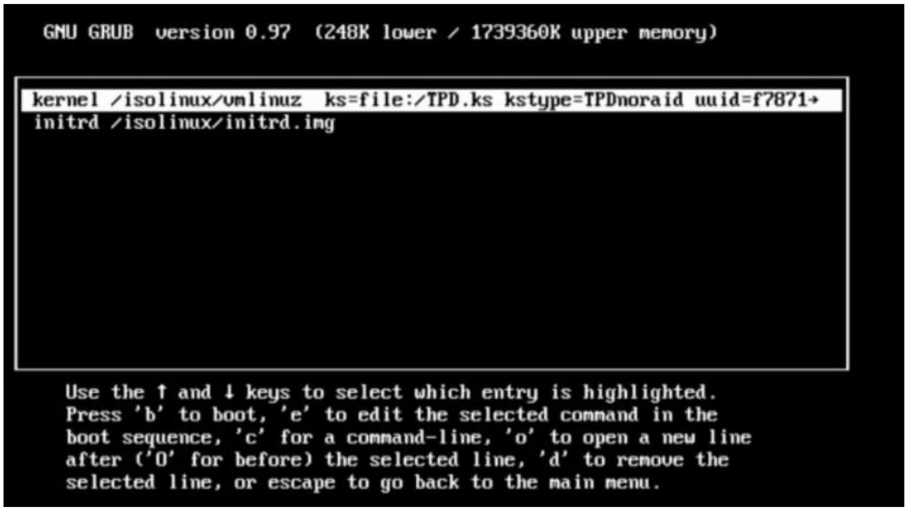
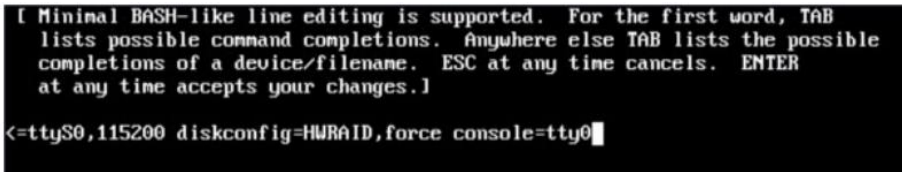
5.
☐
	RMS Server: Begin IPM process
	For X7-2 hardware, skip to step 6.
		
		IPM the server.
		`TPDnoraid diskconfig=HWRAID,force console=tty0`
		HP DL380 Gen 9 only (equiped with 10GB FlexLOM).
		`TPDnoraid diskconfig=HWRAID,force console=tty0 control_if=eth05,eth06`
		For non-HA lab node (Oracle X5-2/Netra X5-2/X6-2).
		`TPDnoraid drives=<Volume ID recorded in procedure Q.1.1-Q.1.3> console=tty0`
		For non-HA lab node (HP DL380 Gen 9 equiped with 10GB FlexLOM).
		`TPDnoraid drives=<Volume ID recorded in procedure S.1/S.2> console=tty0 control_if=eth05,eth06`

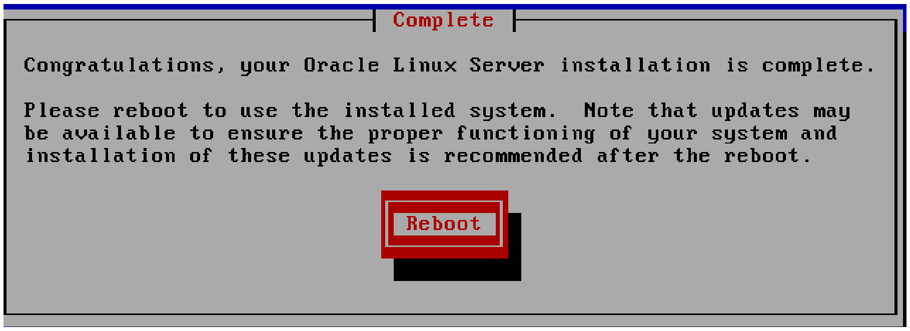
```
 Copyright (C) 2003, 2014, Oracle and/or its affiliates. All rights reserved.

                Welcome to Tekelec Platform Distribution!
                Release:  7.0.0.0.0_86.11.0
                   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 | TPDnoraid | 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: _
```

6. ☐	**RMS Server(X7-2)**: Begin IPM process	For **UEFI BIOS servers** (Unified Extensible Firmware Interface-compatible BIOS) such as X7-2: Below is a sample of the output screen indicating initial boot from the installation media was successful. The information in this screen is representative of the X7-2 support start in TPD 7.5.0.0.0. 1. Use the up and down arrow keys to select **TPDnoraid**. 

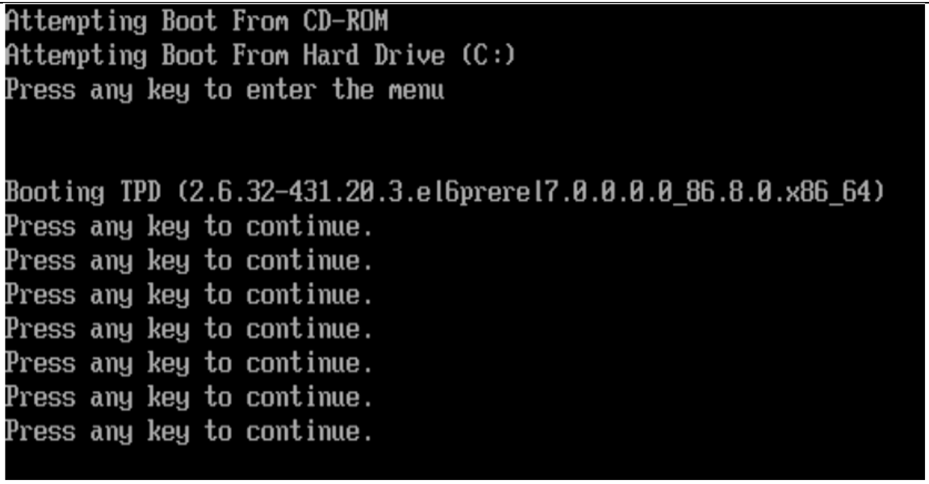
```
  GNU GRUB  version 0.97  (248K lower / 1739360K upper memory)

 TPD
 TPDnoraid
 TPDcompact
 rescue

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    commands before booting, 'a' to modify the kernel arguments
    before booting, or 'c' for a command-line.
```

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

		2. Type **e** to edit.
		
		`GNU GRUB  version 0.97  (248K lower / 1739360K upper memory)`
		`kernel /isolinux/vmlinuz  ks=file:/TPD.ks kstype=TPDnoraid uuid=f7871→`
		`initrd /isolinux/initrd.img`
		`Use the ↑ and ↓ keys to select which entry is highlighted.`
		`Press 'b' to boot, 'e' to edit the selected command in the`
		`boot sequence, 'c' for a command-line, 'o' to open a new line`
		`after ('O' for before) the selected line, 'd' to remove the`
		`selected line, or escape to go back to the main menu.`
		3. Append additional inputs to the TPDnoraid command as shown (example additional arguments).
		
		`[ Minimal BASH-like line editing is supported.  For the first word, TAB`
		`lists possible command completions.  Anywhere else TAB lists the possible`
		`completions of a device/filename.  ESC at any time cancels.  ENTER`
		`at any time accepts your changes.]`
		`<=ttyS0,115200 diskconfig=HWRAID,force console=tty0`
		4. Press **Enter** to continue IPM and monitor progress.
		5. Wait 30-60 seconds for the the terminal to respond and echo to the terminal. For any additional commands or custom IPM options, refer to [21] . Some topics of interest may be **OS IPM Install**, **IPM Command Options**, **Time Estimates for IPM in Minutes**, and **Possible Errors During IPM Installation Processing**, and other useful information.
		6. Monitor the IPM installation.
		The IPM process takes about 30 minutes. Several messages and screens display in the process.

7.
☐
	RMS Server: Reboot	1. Once the IPM is complete, remove the disk from the drive or unmount the TPD image from the iLO and press **Enter** to reboot the server.
		
		`Complete`
		`Congratulations, your Oracle Linux Server installation is complete.`
		`Please reboot to use the installed system.  Note that updates may`
		`be available to ensure the proper functioning of your system and`
		`installation of these updates is recommended after the reboot.`
		`Reboot`
		After a few minutes and multiple reboots, the server boot sequence starts and eventually displays that it is booting the new IPM load.

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

<table>
<tr>
<td></td>
<td></td>
<td>


```
Attempting Boot From CD-ROM
Attempting Boot From Hard Drive (C:)
Press any key to enter the menu


Booting TPD (2.6.32-431.20.3.el6prerel7.0.0.0.0_86.8.0.x86_64)
Press any key to continue.
Press any key to continue.
Press any key to continue.
Press any key to continue.
Press any key to continue.
Press any key to continue.
Press any key to continue.
```

Note: A successful IPM platform installation process results in a user login prompt.
</td>
</tr>
<tr>
<td>8.
☐</td>
<td>For NEBS and non NEBS deployment (Oracle Netra X5-2/X6-2 server only)</td>
<td>
For NEBS and non NEBS deployment, execute these steps (Oracle Netra X5-2/X6-2 server only):

- NEBS deployment configuration, execute Procedure 74.
- Non-NEBS deployment configuration, execute Procedure 75.
</td>
</tr>
</table>

Procedure 4. Configure First Rack Mount Server

<table>
<tr><td colspan="3">This procedure configures 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>Determine bridge names and interfaces</td><td>Determine the bridge interfaces to use on the TVOE server and fill in the appropriate values this table. If NetBackup is used, determine the bridge interface to use for the NetBackup network and fill in the <TVOE_NetBackup_Bridge_Interface> value.
<table>
<tr><th>Guest Interface Alias</th><th>TVOE Bridge Name</th><th>TVOE Bridge Interface</th></tr>
<tr><td>control</td><td>control</td><td>Fill in the appropriate value (bond0): ______________
<TVOE_Control_Bridge_Interface>
<i>Note:</i> bond0 should be used, and the Customer must configure the control VLAN as the native VLAN on ports connecting to the OAM NICs of each server.</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 values:
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>
</table></td></tr>
<tr><td>2.
☐</td><td>1st RMS iLO/iLOM: Login and start the integrated remote console</td><td>1. Log into iLO/iLOM and follow Appendix D TVOE iLO/iLOM GUI Access to access the iLO/iLOM GUI.
<code>https://<management_server_iLO_ip></code>
2. Login as admusr.</td></tr>
</table>

Procedure 4. Configure First Rack Mount Server

3. ☐	**1st RMS iLO/iLOM**: Create the management network	***Note:*** This output is for illustrative purposes only. The site information for this system determines the network interfaces (network devices, bonds, and bond enslaved devices) to configure.

```
$ sudo /usr/TKLC/plat/bin/netAdm add
--device=<TVOE_Management_Bridge_Interface> --
onboot=yes

Interface bond0.2 added
```

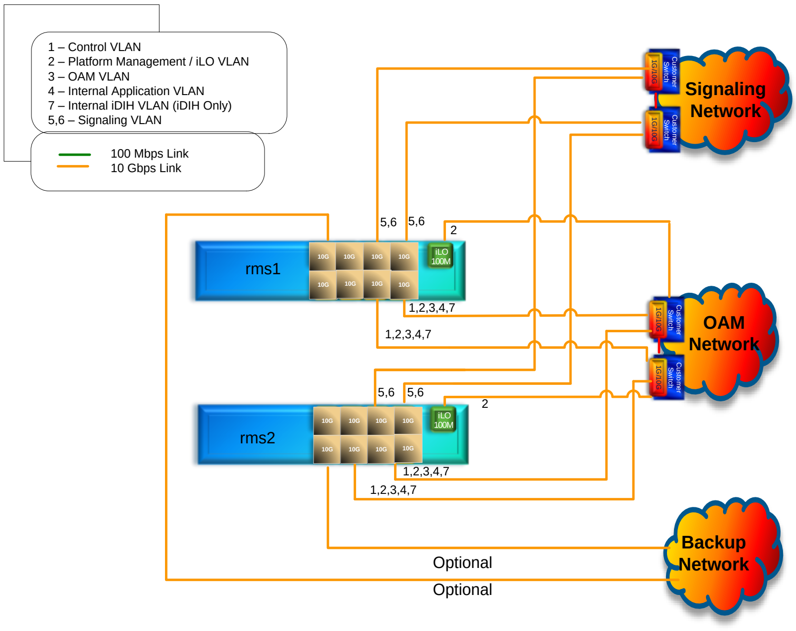
```
$sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge
--name=management --bootProto=none --onboot=yes
--address=<Management_Server_TVOE_IP>
--netmask=<Management_Server_TVOE_Netmask/prefix>
--bridgeInterfaces=<TVOE_Management_Bridge_Interface>
Bridge management added!
```

4. ☐	**1st RMS iLO/iLOM**: Configure default route	

```
$ sudo /usr/TKLC/plat/bin/netAdm add --route=default
--device=management
--gateway=<Management_Gateway_IP_Address>

Route to management added
```

Procedure 4. Configure First Rack Mount Server

5. ☐	**1st RMS iLO/iLOM**: TVOE bond1 configuration (segregated signaling)	If the 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 the OAM related networks share the same physical NICs (non-segregated), skip this step.


1 – Control VLAN
2 – Platform Management / iLO VLAN
3 – OAM VLAN
4 – Internal Application VLAN
7 – Internal iDIH VLAN (iDIH Only)
5,6 – Signaling VLAN
100 Mbps Link
10 Gbps Link
Signaling Network
Customer Switch
1G/10G
Customer Switch
1G/10G
5,6
5,6
2
rms1
10G
iLO 100M
1,2,3,4,7
1,2,3,4,7
OAM Network
Customer Switch
1G/10G
Customer Switch
1G/10G
5,6
5,6
2
rms2
iLO 100M
1,2,3,4,7
1,2,3,4,7
Backup Network
Optional
Optional

Create Bond1 interface:

Note: Refer to section 2.2.2 for network interface server reference table.

```
$ 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. Configure First Rack Mount Server

6. ☐	**1st RMS iLO/iLOM**: Set Ethernet interface ring buffer sizes	***Note:*** Refer to section 2.2.2 for network interface server reference table.

```
$ 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 these commands:

```
$ sudo netAdm set --device=<ethernet_interface_3>  --
ringBufferRx=4096 --ringBufferTx=4096
$ sudo netAdm set --device=<ethernet_interface_4>  --
ringBufferRx=4096 --ringBufferTx=4096
```

Ring Buffer Sizes For X7-2

```
$ sudo netAdm set --device=<ethernet_interface_1> --
ringBufferRx=2047 --ringBufferTx=2047
$ sudo netAdm set --device=<ethernet_interface_2>  --
ringBufferRx=2047 --ringBufferTx=2047
```

If step 5. was executed, execute these commands:

```
$ sudo netAdm set --device=<ethernet_interface_3>  --
ringBufferRx=2047 --ringBufferTx=2047
$ sudo netAdm set --device=<ethernet_interface_4>  --
ringBufferRx=2047 --ringBufferTx=2047
```

Procedure 4. Configure First Rack Mount Server

7. ☐ **1st RMS iLO/iLOM**: Add the NetBackup network — **Option 1** (optional)

If NetBackup is used, execute this step; otherwise, skip to step 12.

Before selecting the configuration option, first read the description in each step to determine which configuration is applicable to your installation and network.

Select only this option or one of the options listed in steps 8. or 9.

NetBackup is a tool that allows the customer to take remote backups of the system.

Notes:

- This output is for illustrative purposes only and shows the control bridge configured.
- This example shows a TVOE management server configuration with the NetBackup feature enabled and the NetBackup network configured with a non-default MTU size.
- 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.

```
$ 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>
```

8. ☐ **1st RMS iLO/iLOM**: Add the NetBackup network — **Option 2** (optional)

If NetBackup is used, select only this option or one of the options listed in steps 7. or 9.

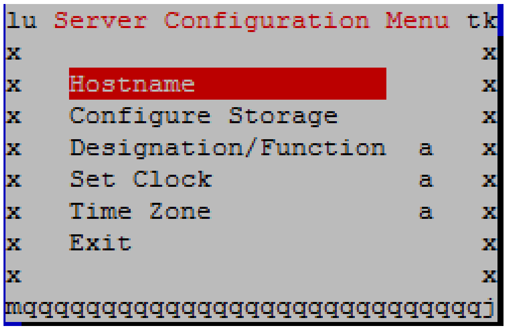
Create NetBackup bridge using an untagged native interface.

```
$ 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>
```

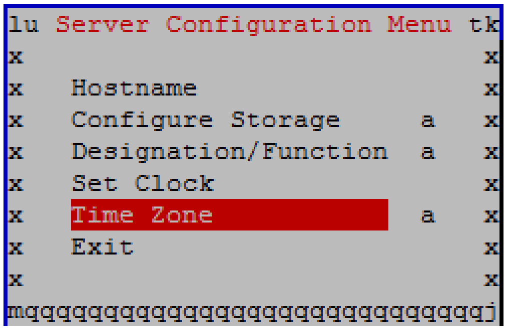
Procedure 4. Configure First Rack Mount Server

9.
☐
	1st RMS iLO/iLOM: Add the NetBackup network — **Option 3** (optional)	If NetBackup is used, select only this option or one of the options listed in steps 7. or 8.
		Create NetBackup bridge using a tagged device.
		`$ 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>`

10.
☐
	1st RMS iLO/iLOM: Configure networking for NetBackup interface (optional)	`$ 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>`

11. ☐	**1st RMS iLO/iLOM**: Restart network interfaces	`$ sudo service network restart`
12. ☐	**1st RMS iLO/iLOM**: Set the server hostname	1. Enter the platcfg menu. `$ sudo  su - platcfg` 2. Navigate to **Server Configuration > Hostname >Edit**.  Server Configuration Menu Hostname Configure Storage Designation/Function Set Clock Time Zone Exit 3. Set the TVOE management server **hostname**. 4. Click **OK**. 5. Navigate out of hostname.

Procedure 4. Configure First Rack Mount Server

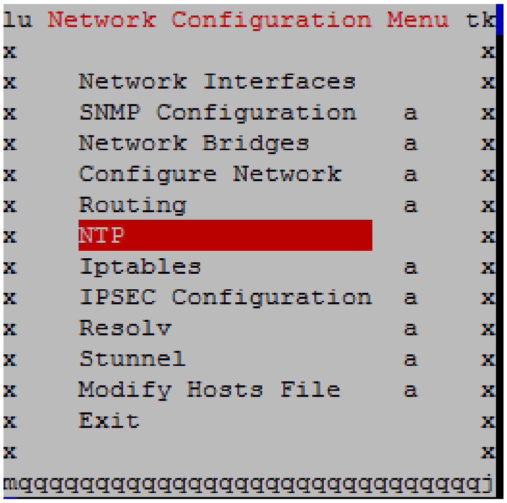
13. ☐	**1st RMS iLO/iLOM**: Set the time zone and/or hardware clock	1. Navigate to **Server Configuration > Time Zone**.  2. Click **Edit**. 3. Set the time zone and/or hardware clock to **GMT** (or appropriate time zone value). 4. Click **OK**. 5. Navigate out of server configuration.

```
lu Server Configuration Menu tk
x                             x
x   Hostname                  x
x   Configure Storage     a   x
x   Designation/Function  a   x
x   Set Clock                 x
x   Time Zone             a   x
x   Exit                      x
x                             x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

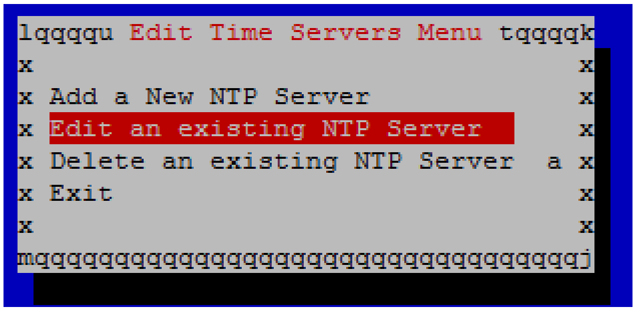
Procedure 4. Configure First Rack Mount Server

<table>
<tr>
<td>14.
☐</td>
<td>1st RMS iLO/iLOM: Configure/Edit NTP server</td>
<td>

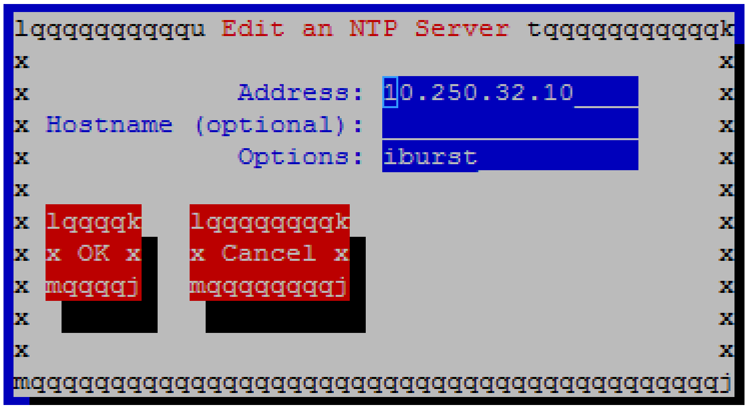
1. Navigate to **Network Configuration > NTP**.


Network Configuration Menu
Network Interfaces
SNMP Configuration
Network Bridges
Configure Network
Routing
NTP
Iptables
IPSEC Configuration
Resolv
Stunnel
Modify Hosts File
Exit

2. Select **Edit an existing NTP Server**.


Edit Time Servers Menu
Add a New NTP Server
Edit an existing NTP Server
Delete an existing NTP Server
Exit

3. Select the NTP server, edit the data, and click **OK**.



Edit an NTP Server

Address: 10.250.32.10

Hostname (optional):

Options: iburst

4. Exit platcfg.

</td>
</tr>
</table>

Procedure 4. Configure First Rack Mount Server

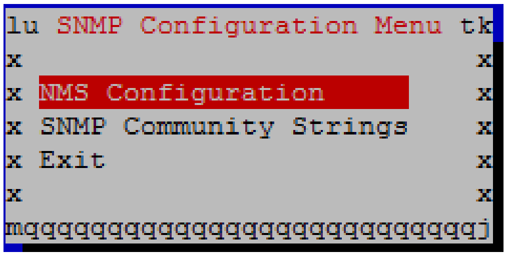
15. ☐ **1st RMS iLO/iLOM**: Set SNMP

1. Enter the platcfg menu.

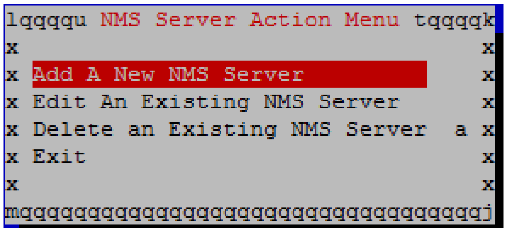
```
$ sudo su - platcfg
```

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

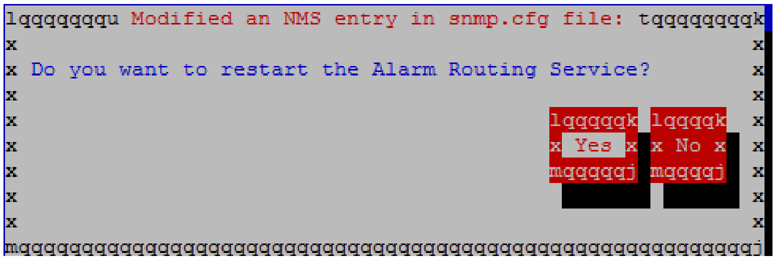
2. Navigate to **Network Configuration > SNMP Configuration > NMS Configuration**.


SNMP Configuration Menu
NMS Configuration
SNMP Community Strings
Exit

3. Click **Edit** and select **Add a New NMS Server**.


NMS Server Action Menu
Add A New NMS Server
Edit An Existing NMS Server
Delete an Existing NMS Server
Exit

4. Complete the form by entering the NMS server IP, Port (default port is 162), and community string provided by the customer about the SNMP trap destination.
5. Click **OK** to finalize the configuration.
6. Click **Exit**.
7. Click **Yes**.



Modified an NMS entry in snmp.cfg file:

Do you want to restart the Alarm Routing Service?

8. Wait a few seconds while the Alarm Routing Service restarts.
9. Exit platcfg.

16. ☐ **1st RMS iLO/iLOM**: Restart the server

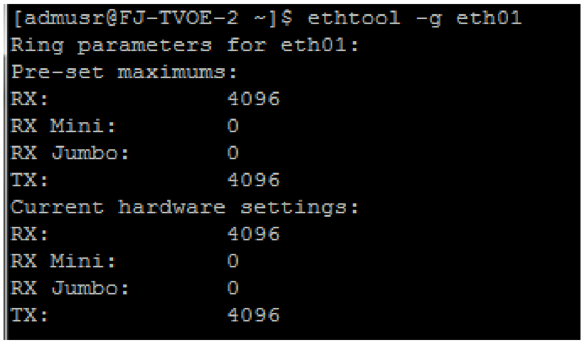
```
$ sudo init 6
```

Procedure 4. Configure First Rack Mount Server

17. ☐	**1st RMS iLO/iLOM**: Verify ring buffer settings	Verify the ring buffer sizes have been configured correctly (from step 6.) by executing this command for each Ethernet interface configured.

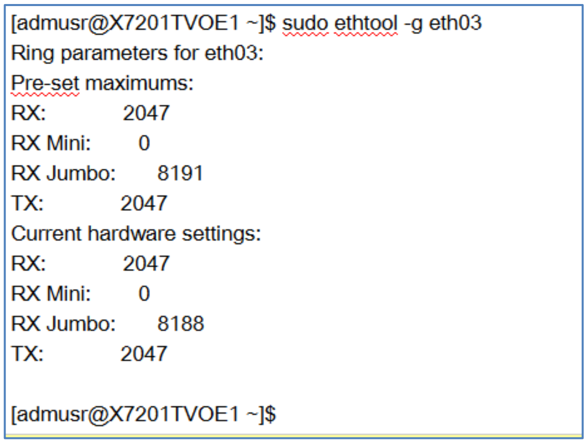
```
$ ethtool -g <eth interfaces configured above>
```

Example output:



```
[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
```

For X7-2 Hardware: Example output:



```
[admusr@X7201TVOE1 ~]$ sudo ethtool -g eth03
Ring parameters for eth03:
Pre-set maximums:
RX:             2047
RX Mini:        0
RX Jumbo:       8191
TX:             2047
Current hardware settings:
RX:             2047
RX Mini:        0
RX Jumbo:       8188
TX:             2047

[admusr@X7201TVOE1 ~]$
```

Procedure 4. Configure First Rack Mount Server

<table>
<tr>
<td>18.
☐</td>
<td>1st RMS iLO/iLOM: Configure NetBackup client on PMAC TVOE host — Part 1 (optional)</td>
<td>
Execute this step if the NetBackup feature is enabled for this system; otherwise, skip this step.

1. Open firewall ports for NetBackup.

```
$ sudo ln -s
/usr/TKLC/plat/share/NetBackup/60NetBackup.ipt
/usr/TKLC/plat/etc/iptables/
$ sudo /usr/TKLC/plat/bin/iptablesAdm reconfig
```

2. Enable platcfg to show the NetBackup menu.

```
$ sudo platcfgadm --show NBConfig;
$ sudo platcfgadm --show NBInit;
$ sudo platcfgadm --show NBDeInit;
$ sudo platcfgadm --show NBInstall;
$ sudo platcfgadm --show NBVerifyEnv;
$ sudo platcfgadm --show NBVerify;
```

3. Create LV and file system for NetBackup client software on the vgguests volume group:

```
$ sudo /usr/TKLC/plat/sbin/storageMgr /tmp/nb.lvm
```

This creates the LV, formats it with a filesystem, and mounts it under **/usr/openv/**.

Example output:

```
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!
```
</td>
</tr>
</table>

Procedure 4. Configure First Rack Mount Server

19. ☐ **1st RMS iLO/iLOM**: Install/Configure NetBackup client software — Part 2 (optional)

Refer to Appendix I Install NetBackup Client for instructions how to install the NetBackup client.

Note: Skip any steps relating to copying NetBackup **notify** scripts to the **/usr/openv/NetBackup/bin**. The TVOE NetBackup notify scripts are created in the next step.

Create soft links for TVOE specific NetBackup notify scripts.

```
$sudo ln -s /usr/TKLC/plat/sbin/bpstart_notify
/usr/openv/NetBackup/bin/bpstart_notify
$sudo ln -s /usr/TKLC/plat/sbin/bpend_notify
/usr/openv/NetBackup/bin/bpend_notify
```

Note: Once the NetBackup client is installed on TVOE, the NetBackup master should be configured to back up the **/var/TKLC/bkp/*.iso** file from the TVOE host.

20. ☐ **1st RMS iLO/iLOM**: Set up syscheck

syscheck must be configured to monitor bonded interfaces.

Replace **bondedInterfaces** with **bond0**, or **bond0,bond1**, if segregated networks are used:

```
$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set
--var=DEVICES --val=<bondedInterfaces>
$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --
enable
```

21. ☐ **1st RMS iLO/iLOM**: Verify syscheck

Verify syscheck:

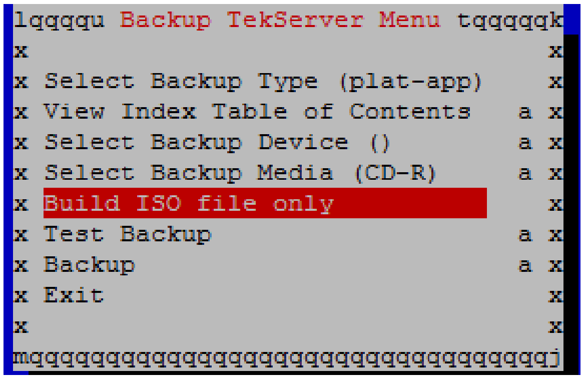
```
$ sudo /usr/TKLC/plat/bin/syscheck net ipbond -v
Expected output should look similar to below:
Running modules in class net...
      ipbond: Bonded interface bond0 is OK
                                OK
LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

22. ☐ **1st RMS iLO/iLOM**: Verify server health

```
$ alarmMgr –alarmStatus
```

This command should return no output on a healthy system. If any alarms are reported, contact My Oracle Support (MOS).

Procedure 4. Configure First Rack Mount Server

23. ☐	**1st RMS iLO/iLOM**: Back up TVOE using TPD platcfg utility	1. Enter the platcfg menu from the TVOE server. `$ sudo su – platcfg` 2. Navigate to **Maintenance > Backup and Restore >Backup Platform (CD/DVD)**. ***Note:*** If no cdrom device is found by TPD, a **No disk device available. This is normal on systems without a cdrom device** error displays. Press **Enter**. 3. Navigate to **Build ISO file only** and press **Enter**.  Backup TekServer Menu Select Backup Type (plat-app) View Index Table of Contents Select Backup Device () Select Backup Media (CD-R) Build ISO file only Test Backup Backup Exit ***Note:*** Creating the ISO image may happen so quickly that this screen may only display for an instant. 4. Exit platcfg by selecting **Exit**. After the ISO is created, platcfg returns to the Backup TekServer menu. The ISO has been created and is located in the **/var/TKLC/bkp/** directory. An example filename of a backup file that was created is **RMS503u14-plat-app-201210301505.iso**. 5. Move the TVOE backup to a customer provided backup server for safe keeping.

3.3 Install PMAC

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

Procedure 5. PMAC Deployment

This procedure deploys PMAC on the TVO host.

Prerequisite: Complete RMS network configuration (PMAC) host) first.

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

1. ☐	**PMAC TVOE iLO/iLOM**: Login and start the integrated remote console	Log into iLO/iLOM and follow Appendix D TVOE iLO/iLOM GUI Access to access the iLO/iLOM GUI. `https://<management_server_iLO_ip>`

Procedure 5. PMAC Deployment

2. ☐ **TVOE iLO/iLOM**: Mount the PMAC media to the TVOE server

Use one of the following two options to mount the PMAC media:

Option 1:

1. If using a USB media, insert the PMAC USB into a USB port and execute this command to mount the ISO.

```
$ ls /media/*/*.iso
/media/sdd1/872-2586-101-5.7.0_57.3.0-PM&C-x86_64.iso
```

2. Use the output of the previous command to populate the next command.

```
$ sudo mount -o loop /media/sdd1/872-2586-101-
5.7.0_57.3.0-PM&C-x86_64.iso /mnt/upgrade
```

Option 2:

1. If using an ISO image, run this to mount it.

```
$ sudo mount -o loop ISO_FILENAME.iso /mnt/upgrade
```

2. Validate the PMAC media.

```
$ cd /mnt/upgrade/upgrade
$ .validate/validate_cd
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
```

Note: If the media validation fails, the media is not valid and should not be used.

Procedure 5. PMAC Deployment

3. ☐ **TVOE iLO/iLOM**: Deploy PMAC

1. Using the PMAC-deploy script, deploy the PMAC instance using the configuration captured during the site survey.

```
$ cd /mnt/upgrade/upgrade
```

2. If deploying PMAC without the NetBackup feature, run this command:

```
$ 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
```

If deploying PMAC with NetBackup feature, run the following command:

```
$ 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
```

The PMAC deploys and boots. The management and control network displays based on the settings provided to the PMAC-deploy script.

Note: This step takes between 5 and 10 minutes.

4. ☐ **TVOE iLO/iLOM**: Unmount the media

1. The media should auto-unmount, if it does not, unmount the media.

```
$ cd /
$ sudo /bin/umount /mnt/upgrade
```

2. Remove the media from the drive.

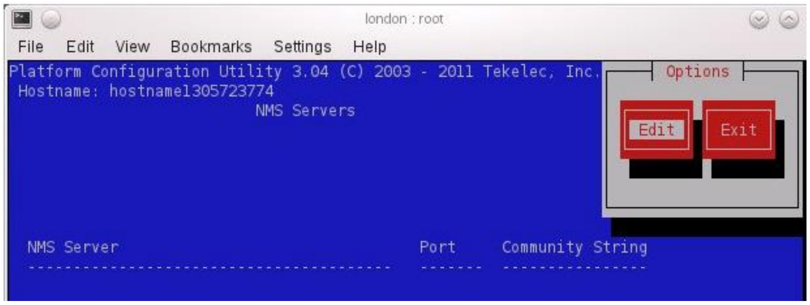
Procedure 5. PMAC Deployment

5.
☐
	TVOE iLO/iLOM: SSH into the management server	1. Using an SSH client such as putty, ssh to the TVOE host as **admusr**.
		2. Login using **virsh** and wait until you see the login prompt.
		`$ sudo /usr/bin/virsh list`
		`Id  Name  State`
		`----------------------------------`
		`2   PM&C  running`
		`$ 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.`
		`PM&Cdev7 login:`

6. ☐	**Virtual PMAC**: Verify the PMAC is configured correctly on first boot	1. Establish an SSH session to the PMAC and login as **admusr**. 2. Run this command (there should be no output). `$ sudo /bin/ls /usr/TKLC/plat/etc/deployment.d/`
7. ☐	**TVOE iLO/iLOM**: Error doing verification, if error is outputted	If an error displays, delete the PMAC guest and re-deploy the guest again: `$ sudo guestMgr --remove <PMAC_Name>`

8.
☐
	Virtual PMAC: Set the PMAC time zone	***Note:*** Valid time zones can be found in Appendix J List of Frequently Used Time Zones.
		1. Run:
		`$ sudo set_pmac_tz.pl <time zone>`
		Example:
		`$ sudo set_pmac_tz.pl America/New_York`
		2. Verify the time zone has been updated.
		`$ sudo date`

Procedure 5. PMAC Deployment

9.
☐
	Virtual PMAC:
	Set SNMP
		1. Enter the platcfg menu.
		`$ sudo su – platcfg`
		2. Navigate to **Network Configuration > SNMP Configuration > NMS Configuration**.
		 london : root
		File
		Edit
		View
		Bookmarks
		Settings
		Help
		Options
		Edit
		Exit`Platform Configuration Utility 3.04 (C) 2003 - 2011 Tekelec, Inc.`
		`Hostname: hostname1305723774`
		`NMS Servers`
		`NMS Server                              Port     Community String`
		`--------------------------------------- -------  ---------------`
		3. Select **Edit** > **Add a New NMS Server**.
		4. Enter all the information to complete the form about the SNMP trap destination.
		Refer to Appendix H SNMP Configuration for more information.
		5. Click **OK** to finalize the configuration.
		6. Click **Exit**.
		7. Click **Yes** and wait until the Alarm Routing Service restarts.
		8. Exit platcfg.

10. ☐	**Virtual PMAC**: Reboot the server	`$ sudo init 6`

3.4 Initialize the PMAC Application

Procedure 6. Initialize PMAC

This procedure gathers and prepares configuration files 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐ **PMAC's TVOE iLO/iLOM**: SSH into the management server

   1. Using an SSH client such as putty, ssh to the TVOE host as **admusr**.
   2. Login using **virsh** and wait until you see the login prompt:

```
$ sudo /usr/bin/virsh list

Id  Name  State
----------------------------------
1  PM&C   running
```

```
$ 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.
PM&Cdev7 login:
```

2. ☐ **Virtual PMAC**: Initialize the PMAC application

   Initialize the PMAC application and run these commands.

```
$ sudo /usr/TKLC/smac/bin/pmacadm applyProfile --
fileName=TVOE
Profile successfully applied.
```

```
$ sudo /usr/TKLC/smac/bin/pmacadm getPmacFeatureState
PMAC Feature State = InProgress
```

```
$ sudo /usr/TKLC/smac/bin/pmacadm finishProfileConfig
Initialization has been started as a background task
```

Procedure 6. Initialize PMAC

3. ☐	**Virtual PMAC**: Initialize the PMAC application ***Note***: Initialization typically takes about 1 minute.	1. Wait for the background task to successfully complete. The command displays **IN_PROGRESS** for a short time. 2. Run this command until a **COMPLETE** or **FAILED** response displays.

```
$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks
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:
```

4. ☐	**Virtual PMAC**: Initialize the PMAC application	Perform a system health check on the PMAC.

```
$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus
```

Note: Some expected networking alarms may be present.

This command should return no output on a healthy system.

Note: An NTP alarm is detected if the system switches are not configured.

```
$ sudo /usr/TKLC/smac/bin/sentry status
```

All processes should be running, displaying output similar to this:

```
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.
```

Procedure 6. Initialize PMAC

5. ☐	**Virtual PMAC**: Verify the PMAC application product release	***Note:*** If the PMAC application product release is not as expected, STOP and contact 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**: Log out of the PMAC	Log out of the virsh console. Press **Ctrl]** to log out of the PMAC.
7. ☐	Note	If configuring a system with aggregation switches (HP DL380 Gen 8 only), continue to Procedure 7. If configuring a system without aggregation switches (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9), skip to Procedure 9.

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

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

This procedure configures the netConfig repository for all required services and for each switch that needs 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 this command:

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

For services, use this command:

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

Users returning to this procedure after initial installation should run these 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, delete the original entry first and then add the service again.

IPv4 and IPv6

Configuration supports using IPv4 or IPv6 addresses through netConfig. Wherever IP addresses are required for networking procedures in section Note:, 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 it 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 allows 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 in these worksheets based on NAPD and 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>	

Variable	Value
<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)

This procedure configures 4948E-4948E-F switches with an appropriate IOS and configuration specified by platform engineering and application requirements.

Prerequisite: This procedure assumes a recently IPMed TVOE server with a VM hosting PMAC.

Needed Materials:

- HP Misc. Firmware USB
- [1] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes (Min 2.2.12)
- DSR USB or ISO

Notes:

- Disconnect uplinks from the customer network before executing this procedure. One of the steps in this procedure instructs when to reconnect these uplink cables.
- 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**1st RMS iLO/iLOM**: Login and start the integrated remote console	1. Log into iLO/iLOM and follow Appendix D TVOE iLO/iLOM GUI Access to access the iLO/iLOM GUI. `https://<management_server_iLO_ip>` 2. Login as **admusr**.

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

2.
☐
	1st RMS iLO/iLOM: Mount firmware image	1. Insert the Misc. Firmware USB media into the USB drive.
		2. Copy each ISO image as determined by the release notes.
		Determine the correct IOS version in the HP Solutions Firmware Upgrade Pack, Software Centric Release Notes (Min 2.2.12) [1].
		3. 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.
		4. Mount the media on the TVOE Host using one of these commands:
		• If using a USB drive, mount it.
		`$ sudo /bin/ls /media/*/*.iso`
		Use the output of the previous command to populate the next command.
		`$ sudo /bin/mount -o loop /media/sdb1/<MISC file name>  /mnt/upgrade`
		• If the DSR in on an ISO, mount it.
		`$ sudo /bin/mount -o loop <path to DSR ISO> /mnt/upgrade`

3. ☐	**TVOE iLO/iLO**: SSH into the management server	1. Using an SSH client such as putty, ssh to the TVOE host as admusr. 2. Login using virsh, and wait until you see the login prompt :

```
$ sudo /usr/bin/virsh list

Id  Name  State
----------------------------------
1   PM&C  running
```

```
$ 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.
PM&Cdev7 login:
```

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

4. ☐	**Virtual PMAC**: Copy ISO images into place (this copies both the 4948E IOS images into place)

```
$ sudo /usr/bin/scp -r
admusr@<TVOE_management_ip_address:/mnt/upgrade/<4948E_
ISO_image_filename> /var/TKLC/smac/image/
```

1. Log out of PMAC.
2. Login again to TVOE Host and unmount the ISO.
3. Press **Ctrl]** to logout of the PMAC.

```
$ sudo umount /mnt/upgrade
```

4. Remove the Misc. Firmware media from the drive.

5. ☐	**Virtual PMAC**: Setup netConfig repository

1. Use netConfig to create a repository entry that uses the ssh service.

   This command displays several prompts for the user. The prompts with **<variables>** as the answers are site specific so the user MUST modify them. Other prompts that do not have a **<variable>** as an answer must be entered EXACTLY as they are shown here.

```
$ 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
```

2. Make sure you entered the information correctly using this command and inspect the output.

```
$ 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
```

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

6. ☐	**Virtual PMAC**: Configure TFTP service	Use netConfig to create a repository entry that uses the TFTP service. This command displays several prompts for the user. The prompts with **<variables>** as the answers are site specific so the user MUST modify them. Other prompts that do not have a **<variable>** as an answer must be entered EXACTLY as they are shown here.

```
$ 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
```

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

7. ☐	**Virtual PMAC**: Run the conserverSetup command	

```
$ sudo /usr/TKLC/plat/bin/conserverSetup –<serial
console type> -s <management_server_mgmt_ip_address>
```

You are asked for the **platcfg** credentials.

An example:

```
[admusr@vm-pmac1A]$ sudo
/usr/TKLC/plat/bin/conserverSetup -u –s
<management_server_mgmt_ip_address>


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.

```
$ sudo /bin/cp /mnt/upgrade/files/<FW_image>
/var/TKLC/smac/image
$ sudo /bin/chmod 644 /var/TKLC/smac/image/<FW_image>
```

9. ☐	**Virtual PMAC**: Set up the netConfig repository with aggregation switch Information	Use netConfig to create a repository entry for each switch. The initial command displays several prompts for the user. The prompts with **<variables>** as the answers are site specific so the user MUST modify them. Other prompts that do not have a **<variable>** as an answer must be entered EXACTLY as they are shown here.

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

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 My Oracle Support (MOS).

```
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
```

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

```
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.
```

10. ☐	**Virtual PMAC**: Verification	Make sure you entered the information correctly.

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice
name=<switch_hostname>
```

Example output:

```
$ 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
```

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

11. ☐	**Virtual PMAC**: Repeat for second 4948.	Repeat steps 9. through 10. for the second Cisco 4948.

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

This procedure configures 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>	
<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 DL380 Servers Only)

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

Needed Materials:

- HP Misc. Firmware USB
- [1] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes (Min 2.2.12)
- 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**Virtual PMAC**: Verify IOS image is on the system	`$ /bin/ls -i /var/TKLC/smac/image/<IOS_image_file>` If the appropriate image does not exist, copy the image to the PMAC.

2.
☐
	Virtual PMAC: Modify PMAC feature to allow TFTP	Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow TFTP traffic.
		`$ sudo /usr/TKLC/smac/bin/pmacadm editFeature`
		`--featureName=DEVICE.NETWORK.NETBOOT --enable=1`
		`$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures`
		Notes:
		• Ignore the restart instructions.
		• 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 pressing **Ctrl-]**. Ensure the interface of the server connected to switch1A is the only interface up and obtain the IP address of the management server management interface.
		`$ sudo /sbin/ifup <ethernet_interface_1>`
		`$ sudo /sbin/ifdown <ethernet_interface_2>`
		`$ sudo /sbin/ip addr show`
		`<management_server_mgmtInterface>`
		`| grep inet`
		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 DL380 Servers Only)

4. ☐	**Virtual PMAC**: Determine if switch1A PROM upgrade is required	

Note: ROM and PROM are intended to have the same meaning for this procedure.

1. Connect serially to switch1A.

```
$ 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
```

Note: If the console command fails, contact My Oracle Support (MOS).

2. Note the IOS image and ROM version for comparison in a following step.
3. Exit from the console by pressing <**Ctrl-e**><**c**><**.**> to the server prompt.
4. Check the version from the previous command against the version from the release notes. If the versions are different, execute Appendix K to Upgrade Cisco 4948 PROM for switch1A.

5. ☐	**Virtual PMAC**: Modify the xml file with information to initialize the switch	

1. Extract the configuration files from the zip file copied in Procedure 6.

```
$ cd /usr/TKLC/smac/etc
$ sudo unzip DSR_NetConfig_Templates.zip
```

This creates a directory called **DSR_NetConfig_Templates** that contains all the configuration files.

2. Copy the files.

```
$ 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
```

3. Update the **4948E init** and **configure xml** files to match your network parameters.

Values to modify are notated in this step by a preceding dollar sign. So if a value with **<some_variable_name>** needs to be modified, then remove the dollar sign and the less than, greater than signs. For example:

```
$ 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
```

Procedure 8. Configure Cisco 4948E-F Aggregation Switches-netConfig (HP DL380 Servers Only)

6. ☐ **Virtual PMAC**: Initialize switch1A

```
$ sudo /usr/TKLC/plat/bin/netConfig --
file=/usr/TKLC/smac/etc/switch1A_4948_4948E_init.xml


Processing file:
/usr/TKLC/smac/etc/switch1A_4948_4948E_init.xml
```

Note: This step takes 5-10 minutes.

1. Check the output of this command for any errors.

   If this fails for any reason, stop this procedure and contact My Oracle Support (MOS). A successful completion of netConfig returns you to the prompt.
2. Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A
getHostname


Hostname: switch1A
```

Note: If this command fails, stop this procedure and contact My Oracle Support (MOS).

3. Exit PMAC by pressing **Ctrl-]**.

7. ☐ **Virtual PMAC TVOE Host**: Manipulate host server physical interfaces

Ensure the interface of the server connected to switch1B is the only interface up and obtain the IP address of the management server management interface.

```
$ sudo /sbin/ifup <ethernet_interface_2>
$ sudo /sbin/ifdown <ethernet_interface_1>
```

Procedure 8. Configure Cisco 4948E-F Aggregation Switches-netConfig (HP DL380 Servers Only)

8. ☐ **TVOE iLO/iLO**: SSH into the management server

1. Using an SSH client such as putty, ssh to the TVOE host as **admusr**.
2. Login using **virsh** and wait until you see the login prompt:

```
$ sudo /usr/bin/virsh list

Id  Name   State
----------------------------------
1   myTPD  running
2   PM&C   running
```

```
$ 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.
PM&Cdev7 login:
```

9. ☐ **Virtual PMAC**: Initialize switch1B

```
$ sudo /usr/TKLC/plat/bin/netConfig --
file=/usr/TKLC/smac/etc/switch1B_4948_4948E_init.xml


Processing file:
/usr/TKLC/smac/etc/switch1B_4948_4948E_init.xml
```

Note: This step takes 5-10 minutes.

1. Check the output of this command for any errors.

   If this fails for any reason, stop this procedure and contact My Oracle Support (MOS). A successful completion of netConfig returns you to the prompt.
2. Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.

```
$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B
getHostname


Hostname: switch1B
```

Note: If this command fails, stop this procedure and contact My Oracle Support (MOS).

Procedure 8. Configure Cisco 4948E-F Aggregation Switches-netConfig (HP DL380 Servers Only)

10. ☐ **Virtual PMAC**: Modify PMAC feature to disable TFTP

Disable the DEVICE.NETWORK.NETBOOT feature.

```
$ sudo /usr/TKLC/smac/bin/PM&Cadm editFeature
--featureName=DEVICE.NETWORK.NETBOOT --enable=0
$ sudo /usr/TKLC/smac/bin/PM&Cadm resetFeatures
```

Notes:

- Ignore the restart instructions.
- This may take up to 60 seconds to complete.

11. ☐ **Virtual PMAC**: Configure both switches

```
$ 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
```

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 My Oracle Support (MOS).

12. ☐ **TVOE Management Server**: Enable interfaces on TVOE host

1. Exit from the virtual PMAC console, by pressing **Ctrl-]** to return to the server prompt.
2. Ensure the interfaces of the server connected to switch1A and switch1B are up.

```
$ sudo /sbin/ifup <ethernet_interface_1>
$ sudo /sbin/ifup <ethernet_interface_2>
```

13. ☐ **TVOE iLO/iLO**: SSH into the management server

1. Using an SSH client such as putty, ssh to the TVOE host as **admusr**.
2. Login using **virsh** and wait until you see the login prompt:

```
$ sudo /usr/bin/virsh list

Id  Name   State
----------------------------------
1   myTPD  running
2   PM&C   running
```

```
$ 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.
PM&Cdev7 login:
```

Procedure 8. Configure Cisco 4948E-F Aggregation Switches-netConfig (HP DL380 Servers Only)

14.
☐
	Virtual PMAC: Verify switch configuration	Ping each interface to verify switch configuration.
		`$ /bin/ping <switch1A_mgmtVLANIP>`
		`$ /bin/ping <switch1B_mgmtVLANIP>`

15. ☐	**Cabinet**: Connect uplinks of switch1A	Attach switch1A customer uplink cables. Refer to the NAPD for which ports are uplink ports. ***Note:*** If you are 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. `$ /bin/ping <customer_supplied_ntp_server_address>`
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 you are using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.
18. ☐	**Virtual PMAC**: Verify access to customer network	Verify connectivity to the customer network. `$ /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 you are 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 to its original state	1. Exit from the virtual PMAC console, by pressing **Ctrl-]** to return to the server prompt. 2. Restore the server networking to its original state. `$ sudo /sbin/service network restart`

3.6 Configure PMAC Server (NetBackup Only)

Procedure 9. Configure the PMAC Server (NetBackup Only)

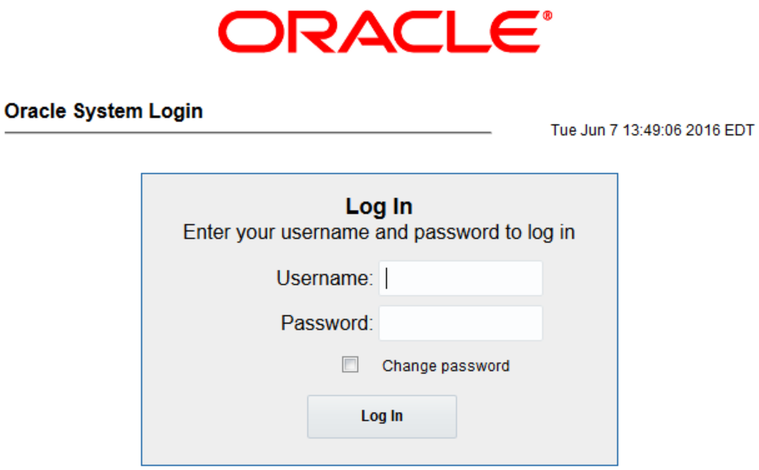
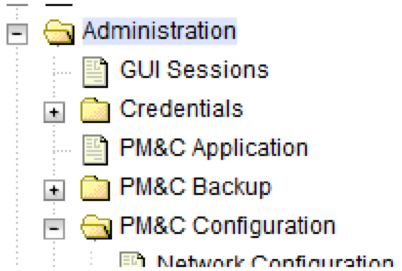
This procedure provides PMAC configuration for NetBackup using the web interface.

Note: The installer must be knowledgeable of the network. If you make a mistake, click **Cancel** and try again. The last step may take a while because it reconfigures the network and attempts to connect may fail.

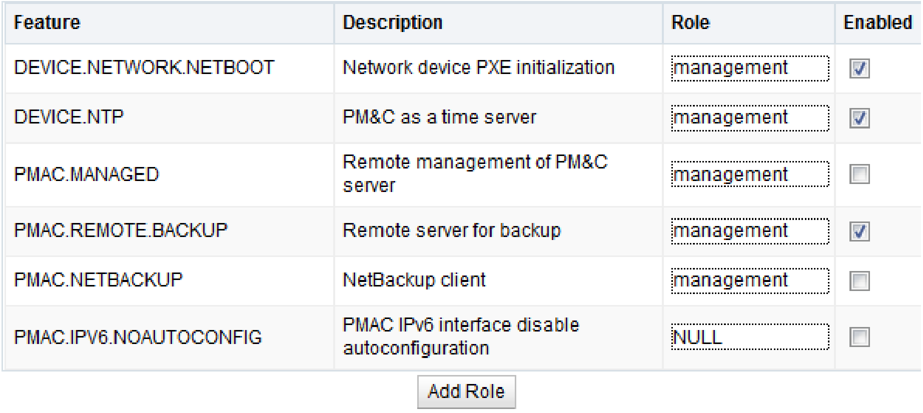
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

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

Procedure 9. Configure the PMAC Server (NetBackup Only)

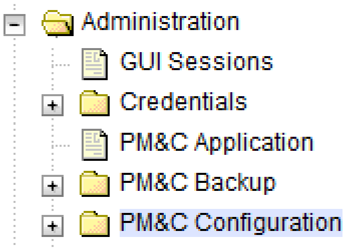
1. ☐	**PMAC GUI**: Login	1. Open the web browser and navigate to the PMAC GUI: `http://<PMAC_network_IP>` 2. Login as the **guiadmin** user:  ORACLE Oracle System Login Tue Jun 7 13:49:06 2016 EDT Log In Enter your username and password to log in Username: Password: ☐ Change password Log In
2. ☐	**PMAC GUI**: Configure optional features	1. Navigate to **Administration > PM&C Configuration > Feature Configuration**.  Administration GUI Sessions Credentials PM&C Application PM&C Backup PM&C Configuration Network Configuration 2. If NetBackup is used, mark the checkbox to enable the NetBackup feature; otherwise, use the selected features as is. 3. Make sure the roles for all the features are set to **management**. 4. Also mark the checkbox to enable the following: • DEVICE.NETWORK.NETBOOT • DEVICE.NTP • PM&C.REMOTE.BACKUP • PM&C.NETBACK (only if NetBackup is used) Example output:

Procedure 9. Configure the PMAC Server (NetBackup Only)



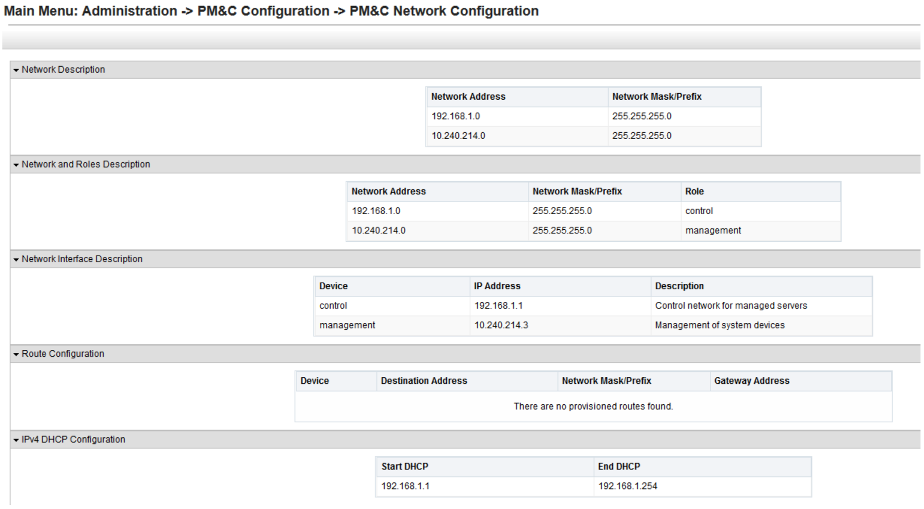
Feature	Description	Role	Enabled
DEVICE.NETWORK.NETBOOT	Network device PXE initialization	management	☑
DEVICE.NTP	PM&C as a time server	management	☑
PMAC.MANAGED	Remote management of PM&C server	management	☐
PMAC.REMOTE.BACKUP	Remote server for backup	management	☑
PMAC.NETBACKUP	NetBackup client	management	☐
PMAC.IPV6.NOAUTOCONFIG	PMAC IPv6 interface disable autoconfiguration	NULL	☐

5. Click **Apply**.
6. This foreground task takes a few moments. Refresh the view with an Info or Error notice to verify the action. To discard changes, just navigate away from the view.
7. Navigate to **Administration > PM&C Configuration**.



8. Make sure the summary is what you want.

Example output with IPv4:



Main Menu: Administration -> PM&C Configuration -> PM&C Network Configuration

Network Description

Network Address	Network Mask/Prefix
192.168.1.0	255.255.255.0
10.240.214.0	255.255.255.0

Network and Roles Description

Network Address	Network Mask/Prefix	Role
192.168.1.0	255.255.255.0	control
10.240.214.0	255.255.255.0	management

Network Interface Description

Device	IP Address	Description
control	192.168.1.1	Control network for managed servers
management	10.240.214.3	Management of system devices

Route Configuration

Device	Destination Address	Network Mask/Prefix	Gateway Address

There are no provisioned routes found.

IPv4 DHCP Configuration

Start DHCP	End DHCP
192.168.1.1	192.168.1.254

Procedure 9. Configure the PMAC Server (NetBackup Only)

3. ☐ **PMAC Command Line**: Perform a system healthcheck

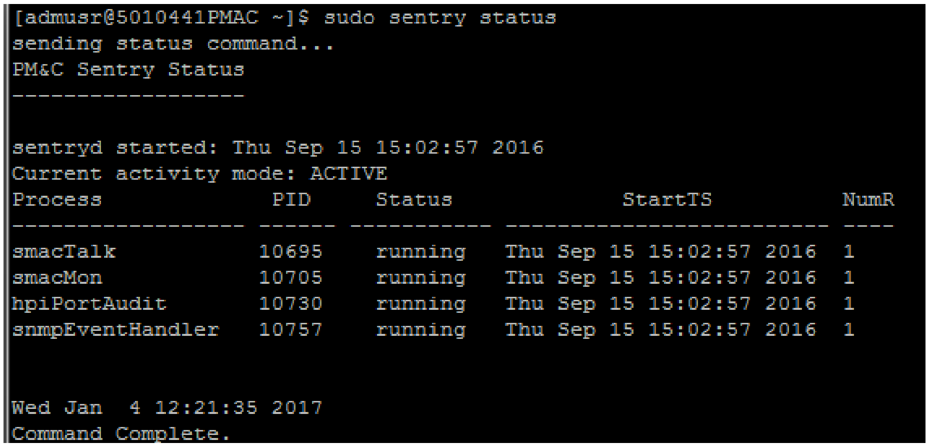
```
$ alarmMgr --alarmStatus
```

This command should return no output on a healthy system.

```
$ sudo sentry status
```

All processes should be running.

Example output:



```
[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.
```

4. ☐ **PMAC Command Line**: Install NetBackup (optional)

1. If the NetBackup client installation relies on the TPD **nbAutoInstall** process to configure the PMAC NetBackup client, execute these commands; otherwise, refer to [14], PMAC NetBackup Client Installation and Configuration procedure, for how to install the NetBackup client on the TVOE management server.

```
$ sudo mkdir -p /usr/openv/NetBackup/bin/
$ sudo ln -s /usr/TKLC/smac/sbin/bpstart_notify
/usr/openv/NetBackup/bin/
$ sudo ln -s /usr/TKLC/smac/sbin/bpend_notify
/usr/openv/NetBackup/bin/
```

2. Use the TPD platcfg utility to add the NetBackup server's alias and IP to the **/etc/hosts** file.

Procedure 9. Configure the PMAC Server (NetBackup Only)

5. ☐ **PMAC Command Line**: Perform a PMAC application backup

```
$ sudo pmacadm backup

PM&C backup been successfully initiated as task ID 7
[usradm@pmacDev3 ~]$
```

Note: The **pmacadm backup** command uses a naming convention that includes a date/time stamp in the file name (for example, backupPmac_20111025_100251.pef). In the example provided, the backup file name indicates it was created on October 25, 2011, at 10:02:51 a.m. server time.

1. Verify the backup was successful.

```
$ sudo pmaccli getBgTasks

2: Backup PMAC COMPLETE - PMAC Backup successful
Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4
sinceUpdate: 2 taskRecordNum:
```

2. Copy the backup file to a remote location.

   The backup file is located under **/var/TKLC/smac/backup**.

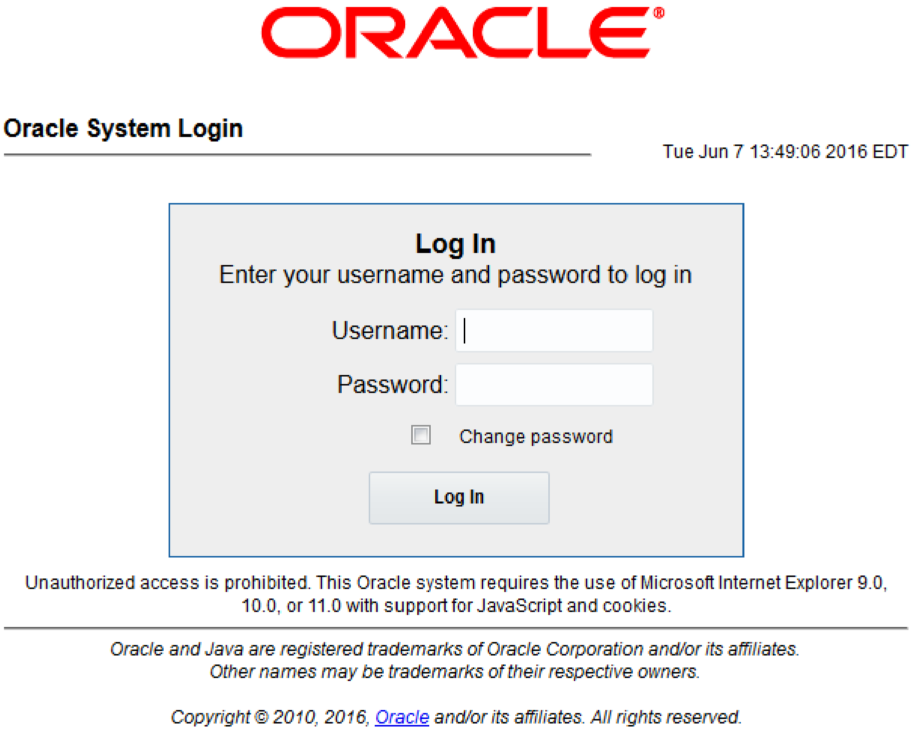
3.7 Add a Rack Mount Server to PMAC

Procedure 10. Add RMS to the PMAC System Inventory

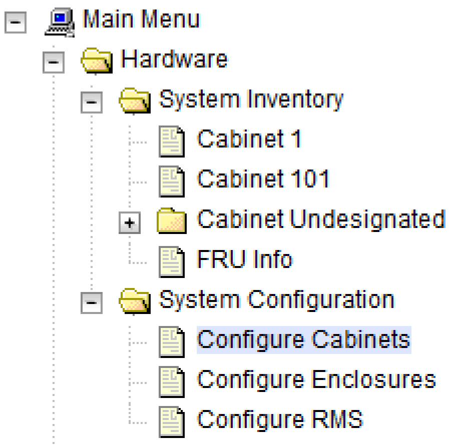
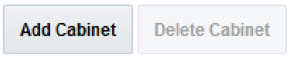
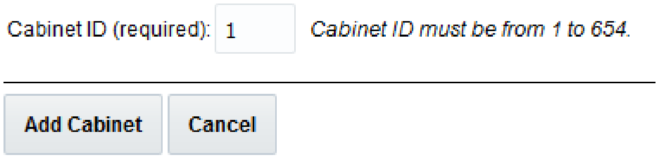
This procedure adds rack mount servers to the PMAC system inventory.

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

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

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

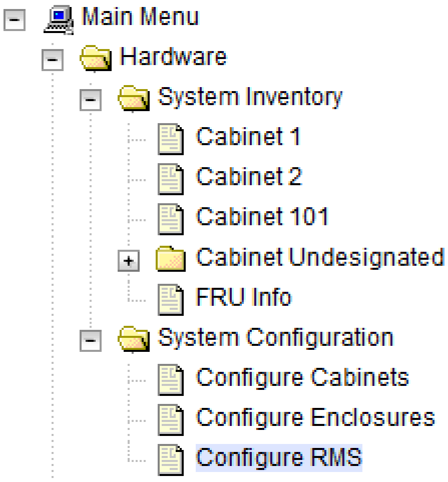
Procedure 10. Add RMS to the PMAC System Inventory

2. ☐	**PMAC GUI**: Configure cabinets	1. Navigate to **Hardware > System Configuration > Configure Cabinets**.  Main Menu Hardware System Inventory Cabinet 1 Cabinet 101 Cabinet Undesignated FRU Info System Configuration Configure Cabinets Configure Enclosures Configure RMS 2. Click **Add Cabinet**.  Add Cabinet Delete Cabinet 3. Type the **Cabinet ID** and click **Add Cabinet**. Cabinet ID (required): 1 *Cabinet ID must be from 1 to 654.* Add Cabinet Cancel

Procedure 10. Add RMS to the PMAC System Inventory

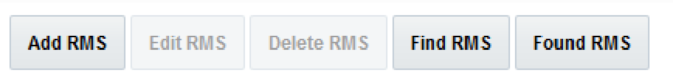
<table>
<tr>
<td>3.
☐</td>
<td>PMAC GUI: Add RMS</td>
<td>

1. Navigate to **Hardware > System Configuration > Configure RMS**.



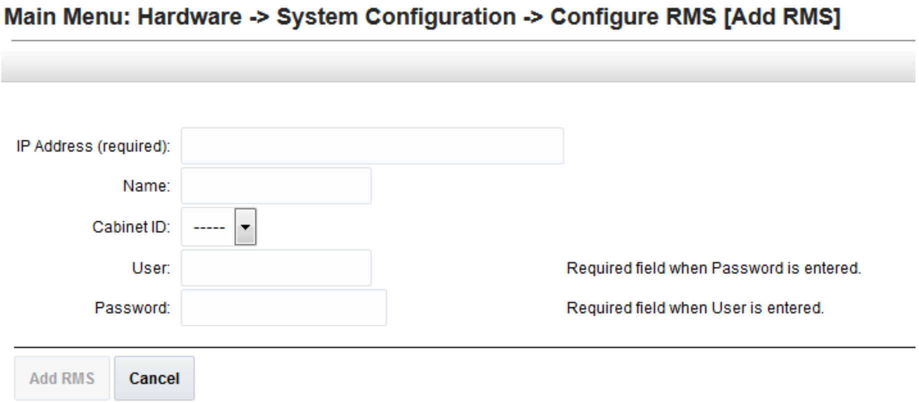
Main Menu
Hardware
System Inventory
Cabinet 1
Cabinet 2
Cabinet 101
Cabinet Undesignated
FRU Info
System Configuration
Configure Cabinets
Configure Enclosures
Configure RMS

2. Click **Add RMS**.



Add RMS
Edit RMS
Delete RMS
Find RMS
Found RMS

3. 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.
4. Click **Add RMS**.



Main Menu: Hardware -> System Configuration -> Configure RMS [Add RMS]
IP Address (required):
Name:
Cabinet ID:

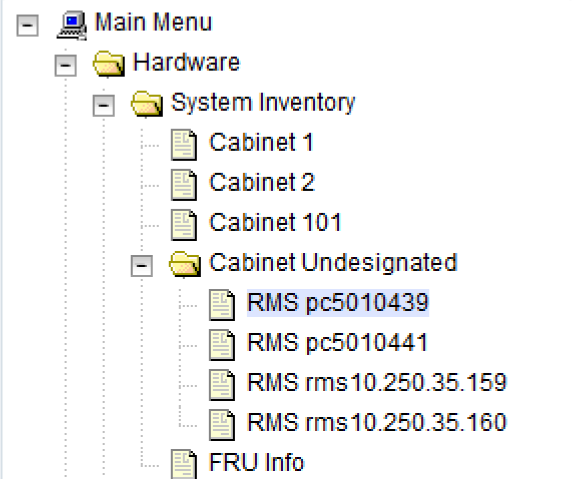
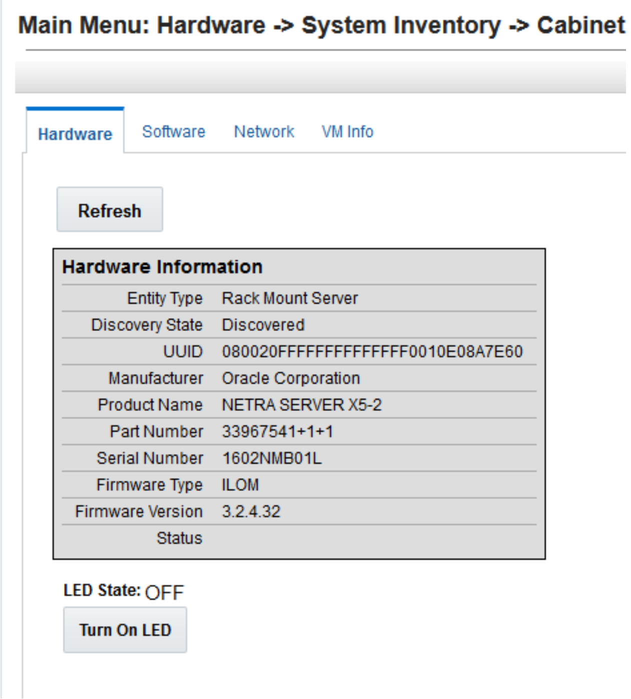
User:
Required field when Password is entered.
Password:
Required field when User is entered.
Add RMS
Cancel

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 do not work, then enter the valid credentials for the rack mount server management port.

5. Repeat this step for additional rack mount servers.

</td>
</tr>
</table>

Procedure 10. Add RMS to the PMAC System Inventory

4. ☐	**PMAC GUI**: Verify RMS discovered	1. Navigate to **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.  Main Menu Hardware System Inventory Cabinet 1 Cabinet 2 Cabinet 101 Cabinet Undesignated RMS pc5010439 RMS pc5010441 RMS rms10.250.35.159 RMS rms10.250.35.160 FRU Info 2. Periodically refresh the hardware information using the double arrow to the right of the **Hardware Information** title until the Discovery State changes from **Undiscovered** to **Discovered**. Main Menu: Hardware -> System Inventory -> Cabinet Hardware Software Network VM Info Refresh **Hardware Information** Entity Type Rack Mount Server Discovery State Discovered UUID 080020FFFFFFFFFFFFFF0010E08A7E60 Manufacturer Oracle Corporation Product Name NETRA SERVER X5-2 Part Number 33967541+1+1 Serial Number 1602NMB01L Firmware Type ILOM Firmware Version 3.2.4.32 Status LED State: OFF Turn On LED ***Note:*** If Status displays an error, contact My Oracle Support (MOS).

3.8 Install TVOE on Additional Rack Mount Servers

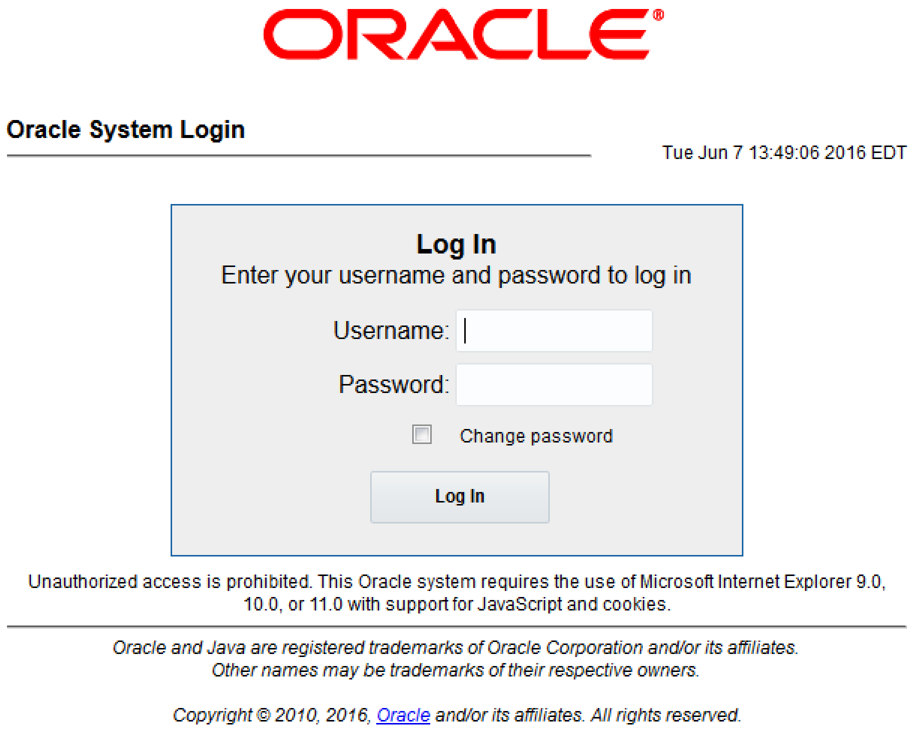
Procedure 11. Restore an Archive That Does Not Contain a Current User

This procedure installs the TVOE operating system on additional mounted servers.

Prerequisite: PMAC (virtualized) has been installed on the first RMS.

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

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

1. ☐	**PMAC GUI**: Login	1. Open the web browser and navigate to the PMAC GUI: `http://<PMAC_network_IP>` 2. Login as the **guiadmin** user:  **Oracle System Login** Tue Jun 7 13:49:06 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password 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.*

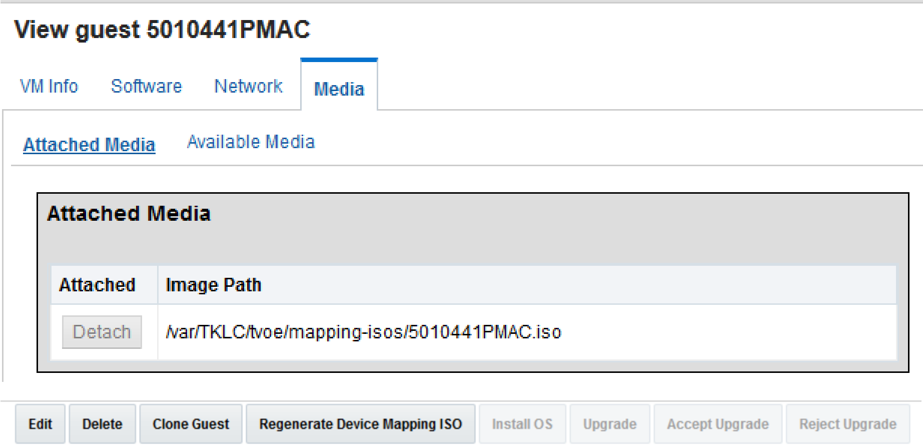
Procedure 11. Restore an Archive That Does Not Contain a Current User

2. ☐	**PMAC’s TVOE**: Load TVOE ISO	Use one of the following two options to add the TVOE ISO image to the PMAC:

Option 1 — Attach the USB device containing the ISO image to a USB port.

1. From the PMAC GUI, navigate to **VM Management > PMAC guest > View VM Guest > Media tab**.
2. Locate the ISO image in the **Available Media** list and click its **Attach** button.

   After a pause, the image displays in the Attached Media list.


View guest 5010441PMAC

VM Info
Software
Network
Media
Attached Media
Available Media

Attached Media

Attached	Image Path
Detach	/var/TKLC/tvoe/mapping-isos/5010441PMAC.iso

Edit
Delete
Clone Guest
Regenerate Device Mapping ISO
Install OS
Upgrade
Accept Upgrade
Reject Upgrade

Option 2 — Use a TVOE 64 bit ISO file.

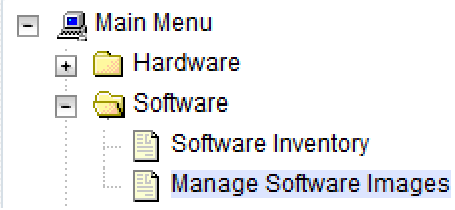
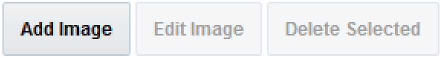
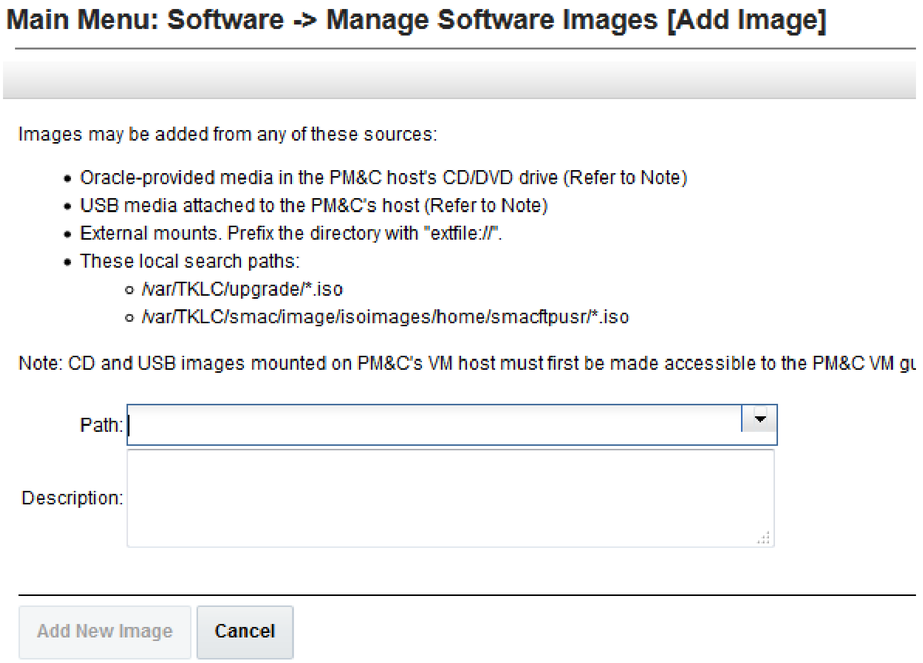
1. Use sftp to transfer the ISO image to the PMAC server in the **/var/TKLC/smac/image/isoimages/home/smacftpusr/** directory as **pmacftpusr** user:
2. cd to the directory where your ISO image is located on the TVOE host (not on the PMAC server).
3. Using sftp, connect to the PMAC management server.

```
> sftp pmacftpusr@<PM&C_management_network_ip>
> put <image>.iso
```

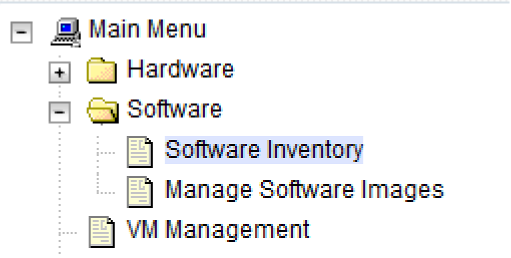
4. After the image transfer is 100% complete, close the connection.

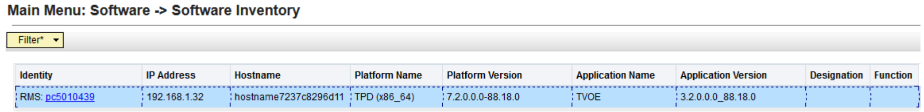
```
> quit
```

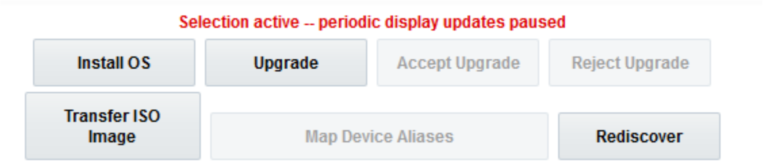
Procedure 11. Restore an Archive That Does Not Contain a Current User

3.
☐
	PMAC GUI: Add TVOE image	1. Navigate to **Software > Manage Software Images**.
		
		 Main Menu
		Hardware
		Software
		Software Inventory
		Manage Software Images
		2. Click **Add Image**.
		3. Select the image from the options.
		
		
		If the image was supplied on a CD or a USB drive, it displays 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 on the second device, **device://dev/sr1**. If one or more CD or USB-based images was already on the TVOE management server before you started this procedure, select a correspondingly higher device number.
		If the image was transferred to PMAC using sftp, it displays in the list as a local file **/var/TKLC/...**.
		
		Main Menu: Software -> Manage Software Images [Add Image]
		Images may be added from any of these sources:
		- Oracle-provided media in the PM&C host's CD/DVD drive (Refer to Note)
		- USB media attached to the PM&C's host (Refer to Note)
		- External mounts. Prefix the directory with "extfile://".
		- These local search paths:
		  ○ /var/TKLC/upgrade/*.iso
		  ○ /var/TKLC/smac/image/isoimages/home/smacftpusr/*.iso
		Note: CD and USB images mounted on PM&C's VM host must first be made accessible to the PM&C VM gu
		
		4. Select the appropriate path and click **Add New Image**.
		5. Check the progress by clicking the Task Monitoring link. Observe the green bar indicating success.
		6. Once complete, remove the TVOE media from the optical drive of the TVOE management server.

Procedure 11. Restore an Archive That Does Not Contain a Current User

<table>
<tr>
<td>4.
☐</td>
<td>PMAC GUI: Select RMS servers for TVOE OS install</td>
<td>
1. Navigate to Software > Software Inventory.

Main Menu
Hardware
Software
Software Inventory
Manage Software Images
VM Management

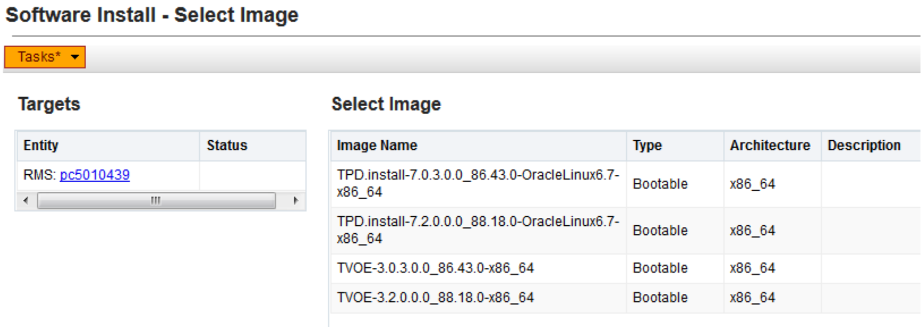
2. Select the RMS servers you want to IPM.
If you want to install the same OS image to more than one server, select multiple servers by clicking on each row. Selected rows are highlighted in green.

Main Menu: Software -> Software Inventory

<table>
<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>
<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>
</table>
3. Click Install OS.

Selection active -- periodic display updates paused
Install OS
Upgrade
Accept Upgrade
Reject Upgrade
Transfer ISO Image
Map Device Aliases
Rediscover
</td>
</tr>
</table>

Procedure 11. Restore an Archive That Does Not Contain a Current User

<table>
<tr>
<td>5.
☐</td>
<td>PMAC GUI: Initiate OS install on RMS server(s)</td>
<td>

1. 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.



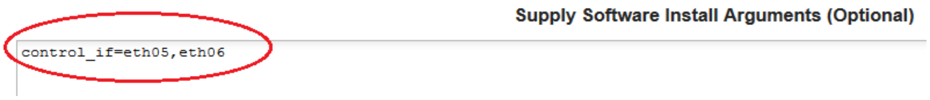
Targets

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	

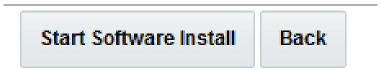
2. HP DL380 Gen9 with 10GB FlexLOM, enter **control_if=eth05,eth06** for the Supply Software Install Arguments (Optional).



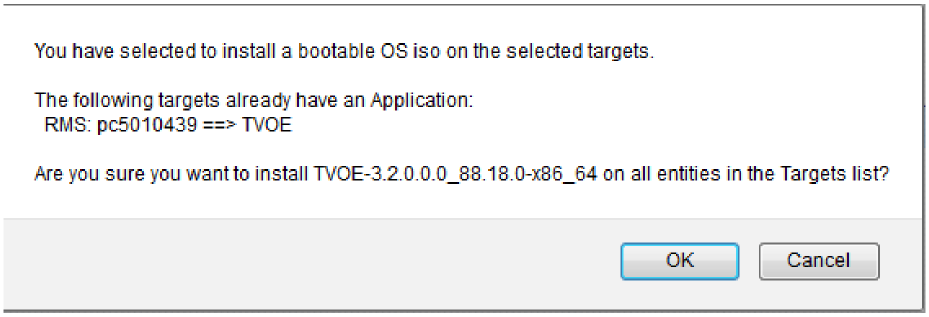
Supply Software Install Arguments (Optional)

```
control_if=eth05,eth06
```

3. Click **Start Software Install**.



4. Select **OK**.



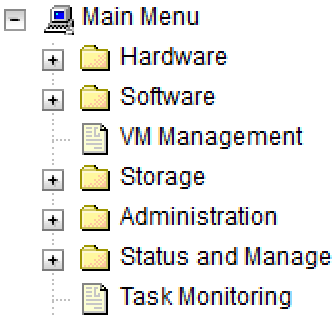
You have selected to install a bootable OS iso on the selected targets.

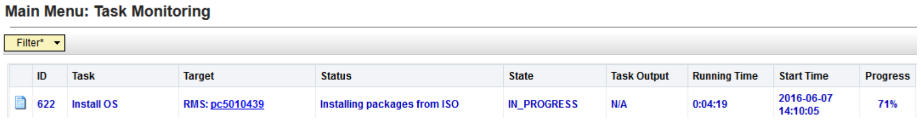
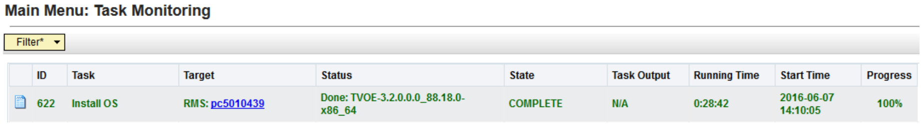
The following targets already have an Application:
RMS: pc5010439 ==> TVOE

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?

</td>
</tr>
</table>

Procedure 11. Restore an Archive That Does Not Contain a Current User

<table>
<tr>
<td>6.
☐</td>
<td>**PMAC GUI**:
Monitor OS install</td>
<td>
Navigate to **Task Monitoring** to monitor the progress of the TVOE Installation background task.
A separate task displays for each server.



Main Menu: Task Monitoring
Filter*
<table>
<tr><th></th><th>ID</th><th>Task</th><th>Target</th><th>Status</th><th>State</th><th>Task Output</th><th>Running Time</th><th>Start Time</th><th>Progress</th></tr>
<tr><td></td><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>
</table>
When the installation is complete, the task changes to green and the progress bar indicates 100%.

Main Menu: Task Monitoring
Filter*
<table>
<tr><th></th><th>ID</th><th>Task</th><th>Target</th><th>Status</th><th>State</th><th>Task Output</th><th>Running Time</th><th>Start Time</th><th>Progress</th></tr>
<tr><td></td><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>
</table>
</td>
</tr>
</table>

3.9 Configure TVOE on Additional Rack Mount Servers

Procedure 12. Configure TVOE on Additional Rack Mount Servers

<table>
<tr><td colspan="3">This procedure configures TVOE on all remaining rack mount servers.
Prerequisite: RMS has been IPMed with TVOE operating system.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>Determine bridge names and interfaces</td><td>Use the network bridge names determined in Procedure 4, step 1.</td></tr>
<tr><td>2.
☐</td><td>**RMS iLO/iLOM**:
Login and start the integrated remote console</td><td>1. Log into iLO/iLOM and follow Appendix D TVOE iLO/iLOM GUI Access to access the iLO/iLOM GUI.
`https://<management_server_iLO_ip>`
2. Login as **admusr**.</td></tr>
</table>

Procedure 12. Configure TVOE on Additional Rack Mount Servers

3. ☐	**RMS iLO/iLOM**: Create the management network	***Note:*** This output is for illustrative purposes only. The site information for this system determines the network interfaces (network devices, bonds, and bond enslaved devices) to configure. ***Note:*** **bond0** should be used, and the **Customer** must configure the control VLAN as the native VLAN on ports connecting to the OAM NICs of each server.

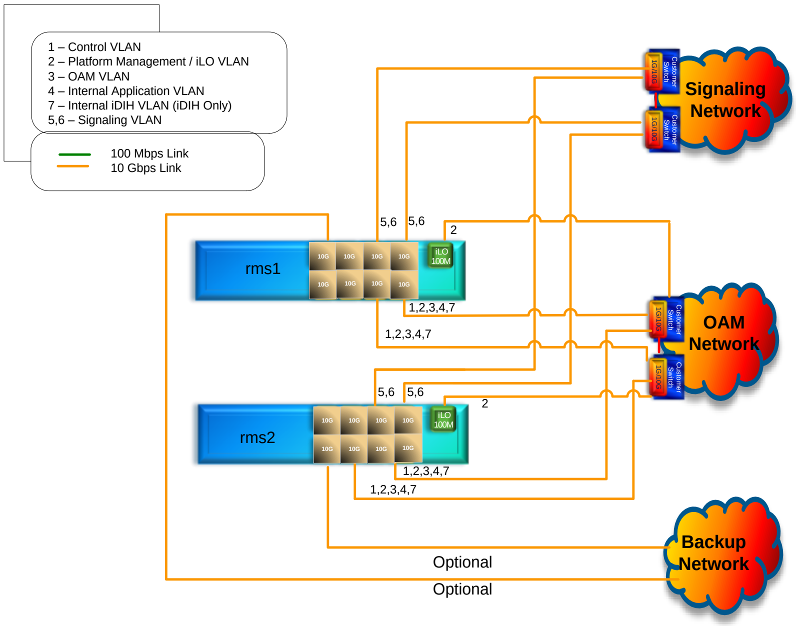
```
$ sudo /usr/TKLC/plat/bin/netAdm add
--device=<TVOE_Management_Bridge_Interface> --
onboot=yes

Interface bond0.2 added
```

```
$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!
```

4. ☐	**RMS iLO/iLOM**: Configure default route	

```
$ sudo /usr/TKLC/plat/bin/netAdm add --route=default
--device=management
--gateway=<Management_Gateway_IP_Address>

Route to management added
```

Procedure 12. Configure TVOE on Additional Rack Mount Servers

5.
☐
	RMS iLO/iLOM: TVOE bond1 configuration (segregated signaling)	If the 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 the OAM related networks share the same physical NICs (non-segregated), skip this step.
		 1 – Control VLAN
		2 – Platform Management / iLO VLAN
		3 – OAM VLAN
		4 – Internal Application VLAN
		7 – Internal iDIH VLAN (iDIH Only)
		5,6 – Signaling VLAN
		100 Mbps Link
		10 Gbps Link
		Signaling Network
		Customer Switch
		1G/10G
		Customer Switch
		1G/10G
		5,6
		5,6
		2
		rms1
		10G
		iLO 100M
		1,2,3,4,7
		1,2,3,4,7
		OAM Network
		Customer Switch
		1G/10G
		Customer Switch
		1G/10G
		5,6
		5,6
		2
		rms2
		10G
		iLO 100M
		1,2,3,4,7
		1,2,3,4,7
		Backup Network
		Optional
		Optional
		Create Bond1 interface:
		Note: Refer to section 2.2.2 for network interface server reference table.
		`$ 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`

Procedure 12. Configure TVOE on Additional Rack Mount Servers

6. ☐	**RMS iLO/iLOM**: Set Ethernet interface ring buffer sizes	***Note:*** Refer to section 2.2.2 for network interface server reference table.

```
$ 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 these commands:

```
$ sudo netAdm set --device=<ethernet_interface_3>  --
ringBufferRx=4096 --ringBufferTx=4096
$ sudo netAdm set --device=<ethernet_interface_4>  --
ringBufferRx=4096 --ringBufferTx=4096
```

Ring Buffer Sizes For X7-2

```
$ sudo netAdm set --device=<ethernet_interface_1> --
ringBufferRx=2047 --ringBufferTx=2047
$ sudo netAdm set --device=<ethernet_interface_2>  --
ringBufferRx=2047 --ringBufferTx=2047
```

If step 5. was executed, execute these commands:

```
$ sudo netAdm set --device=<ethernet_interface_3>  --
ringBufferRx=2047 --ringBufferTx=2047
$ sudo netAdm set --device=<ethernet_interface_4>  --
ringBufferRx=2047 --ringBufferTx=2047
```

Procedure 12. Configure TVOE on Additional Rack Mount Servers

7. ☐	**RMS iLO/iLOM**: Add the NetBackup network — **Option 1** (optional) If NetBackup is used, execute this step; otherwise, skip to step 12.	**Before selecting the configuration option, first read the description in each step to determine which configuration is applicable to your installation and network**. Select only this option or one of the options listed in steps 8. or 9. NetBackup is a tool that allows the customer to take remote backups of the system. ***Notes***: • This output is for illustrative purposes only and shows the control bridge configured. • This example shows a TVOE management server configuration with the NetBackup feature enabled and the NetBackup network configured with a non-default MTU size. • 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.

```
$ 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>
```

8. ☐	**RMS iLO/iLOM**: Add the NetBackup network — **Option 2** (optional)	If NetBackup is used, select only this option or one of the options listed in steps 7. or 9. Create NetBackup bridge using an untagged native interface.

```
$ 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>
```

Procedure 12. Configure TVOE on Additional Rack Mount Servers

9. ☐ **RMS iLO/iLOM**: Add the NetBackup network — **Option 3** (optional)

If NetBackup is used, select only this option or one of the options listed in steps 7. or 8.

Create NetBackup bridge using a tagged device.

```
$ 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>
```

10. ☐ **RMS iLO/iLOM**: Restart network interfaces

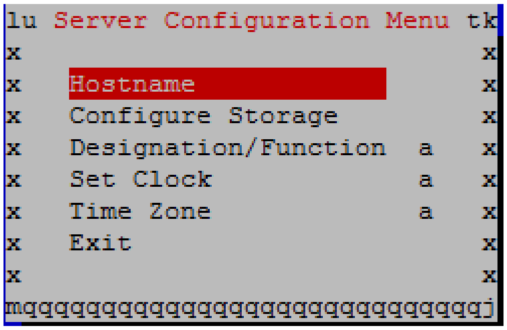
```
$ sudo service network restart
```

11. ☐ **RMS iLO/iLOM**: Set the server hostname

1. Enter the platcfg menu.

```
$ sudo  su - platcfg
```

2. Navigate to **Server Configuration > Hostname >Edit**.

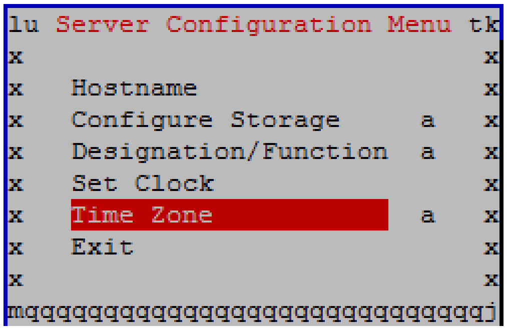

lu Server Configuration Menu tk
Hostname
Configure Storage
Designation/Function
Set Clock
Time Zone
Exit

3. Set the TVOE management server **hostname**.
4. Click **OK**.
5. Navigate out of hostname.

Procedure 12. Configure TVOE on Additional Rack Mount Servers

<table>
<tr>
<td>12.
☐</td>
<td>RMS iLO/iLOM: Set the time zone and/or hardware clock</td>
<td>

1. Navigate to **Server Configuration > Time Zone**.

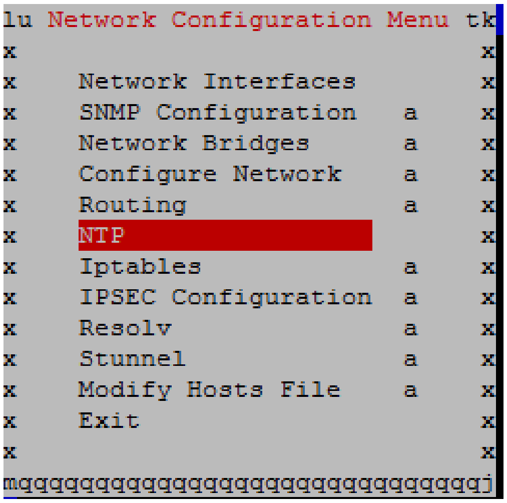

lu Server Configuration Menu tk
x x
x Hostname x
x Configure Storage a x
x Designation/Function a x
x Set Clock x
x Time Zone a x
x Exit x
x x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj

2. Click **Edit**.
3. Set the time zone and/or hardware clock to **UTC** (or appropriate time zone value).
4. Click **OK**.
5. Navigate out of server configuration.

</td>
</tr>
</table>

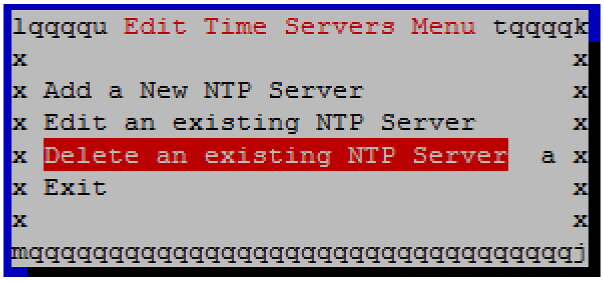
Procedure 12. Configure TVOE on Additional Rack Mount Servers

13. ☐	**RMS iLO/iLOM**: Delete PMAC VM as NTP source on RMS	1. Navigate to **Network Configuration > NTP**.



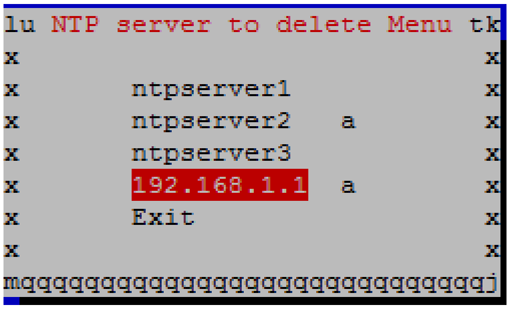
```
lu Network Configuration Menu tk
x                               x
x    Network Interfaces         x
x    SNMP Configuration    a    x
x    Network Bridges       a    x
x    Configure Network     a    x
x    Routing               a    x
x    NTP                        x
x    Iptables              a    x
x    IPSEC Configuration   a    x
x    Resolv                a    x
x    Stunnel               a    x
x    Modify Hosts File     a    x
x    Exit                       x
x                               x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

2. Select **Delete an existing NTP Server**.



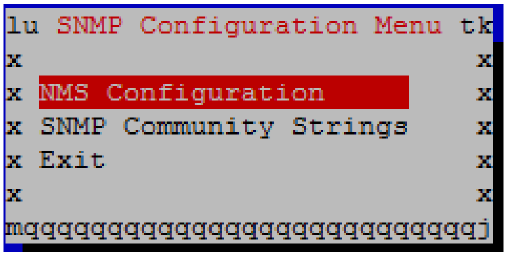
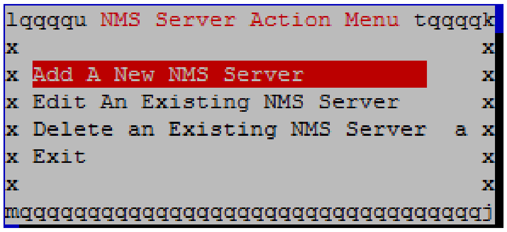
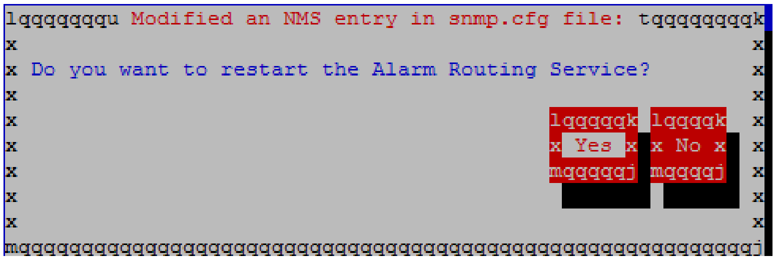
```
lqqqqu Edit Time Servers Menu tqqqqk
x                                  x
x Add a New NTP Server             x
x Edit an existing NTP Server      x
x Delete an existing NTP Server  a x
x Exit                             x
x                                  x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

3. Select the PMAC VM control IP and click **OK**.



```
lu NTP server to delete Menu tk
x                              x
x       ntpserver1             x
x       ntpserver2    a        x
x       ntpserver3             x
x       192.168.1.1   a        x
x       Exit                   x
x                              x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

Procedure 12. Configure TVOE on Additional Rack Mount Servers

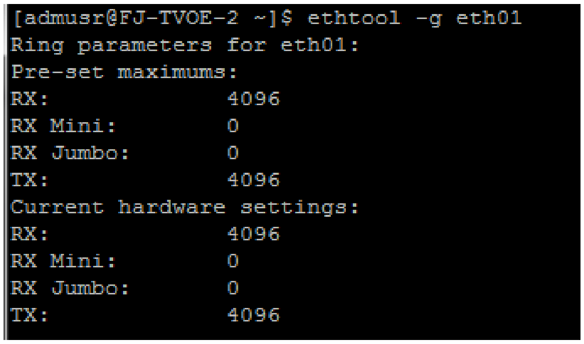
<table>
<tr>
<td>14.
☐</td>
<td>RMS iLO/iLOM:
Set SNMP</td>
<td>
<p><i>Note:</i> Refer to Appendix H SNMP Configuration to understand the preferred SNMP configuration.</p>
<p>1. Navigate to Network Configuration > SNMP Configuration > NMS Configuration.</p>

<pre>
lu SNMP Configuration Menu tk
x   x
x NMS Configuration   x
x SNMP Community Strings   x
x Exit   x
x   x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqj
</pre>
<p>2. Click Edit and select Add a New NMS Server.</p>

<pre>
lqqqqu NMS Server Action Menu tqqqqk
x   x
x Add A New NMS Server   x
x Edit An Existing NMS Server   x
x Delete an Existing NMS Server a x
x Exit   x
x   x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
</pre>
<p>3. Complete the form by entering the NMS server IP, port (default port is 162), and community string provided by the customer about the SNMP trap destination.</p>
<p>4. Click OK to finalize the configuration.</p>
<p>5. Click Exit.</p>
<p>6. Click Yes.</p>

<pre>
lqqqqqqqqu Modified an NMS entry in snmp.cfg file: tqqqqqqqqqk
x   x
x Do you want to restart the Alarm Routing Service?   x
x   x
x   lqqqqqk lqqqqk   x
x   x Yes x x No x   x
x   mqqqqqj mqqqqj   x
x   x
x   x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
</pre>
<p>7. Wait a few seconds while the Alarm Routing Service restarts.</p>
<p>8. Exit platcfg.</p>
</td>
</tr>
<tr>
<td>15.
☐</td>
<td>RMS iLO/iLOM:
Restart the server</td>
<td>
<pre>
$ sudo init 6
</pre>
</td>
</tr>
</table>

Procedure 12. Configure TVOE on Additional Rack Mount Servers

16. ☐	**RMS iLO/iLOM**: Verify ring buffer settings	Verify the ring buffer sizes have been configured correctly (from step 6.) by executing this command for each Ethernet interface configured.

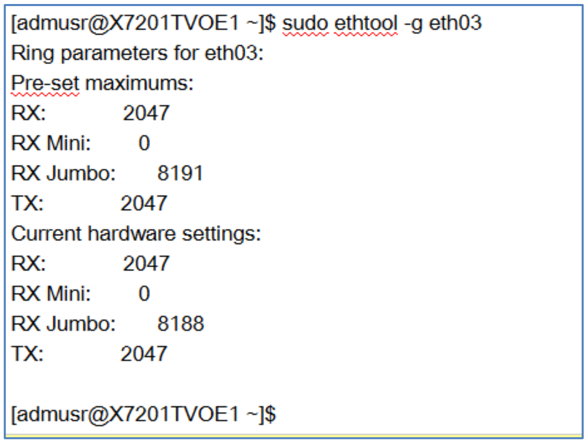
```
$ ethtool -g <eth interfaces configured above>
```

Example output:



```
[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
```

For X7-2 Hardware: Example output:



```
[admusr@X7201TVOE1 ~]$ sudo ethtool -g eth03
Ring parameters for eth03:
Pre-set maximums:
RX:             2047
RX Mini:        0
RX Jumbo:       8191
TX:             2047
Current hardware settings:
RX:             2047
RX Mini:        0
RX Jumbo:       8188
TX:             2047

[admusr@X7201TVOE1 ~]$
```

Procedure 12. Configure TVOE on Additional Rack Mount Servers

17. ☐

RMS iLO/iLOM: Configure NetBackup client on PMAC TVOE host — Part 1 (optional)

Execute this step if the NetBackup feature is enabled for this system; otherwise, skip this step.

1. Open firewall ports for NetBackup.

```
$ sudo ln -s
/usr/TKLC/plat/share/NetBackup/60NetBackup.ipt
/usr/TKLC/plat/etc/iptables/
$ sudo /usr/TKLC/plat/bin/iptablesAdm reconfig
```

2. Enable platcfg to show the NetBackup menu.

```
$ sudo platcfgadm --show NBConfig;
$ sudo platcfgadm --show NBInit;
$ sudo platcfgadm --show NBDeInit;
$ sudo platcfgadm --show NBInstall;
$ sudo platcfgadm --show NBVerifyEnv;
$ sudo platcfgadm --show NBVerify;
```

3. Create LV and file system for NetBackup client software on the vgguests volume group:

```
$ sudo /usr/TKLC/plat/sbin/storageMgr /tmp/nb.lvm
```

This creates the LV, formats it with a filesystem, and mounts it under **/usr/openv/**.

Example output:

```
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!
```

Procedure 12. Configure TVOE on Additional Rack Mount Servers

18.
☐
	RMS iLO/iLOM: Install/Configure NetBackup client software — Part 2 (optional)	Refer to Appendix I Install NetBackup Client for instructions how to install the NetBackup client.
		Note: Skip any steps relating to copying NetBackup **notify** scripts to the **/usr/openv/NetBackup/bin**. The TVOE NetBackup notify scripts are created in the next step.
		Create soft links for TVOE specific NetBackup notify scripts.
		`$sudo ln -s /usr/TKLC/plat/sbin/bpstart_notify /usr/openv/NetBackup/bin/bpstart_notify`
		`$sudo ln -s /usr/TKLC/plat/sbin/bpend_notify /usr/openv/NetBackup/bin/bpend_notify`
		Note: Once the NetBackup client is installed on TVOE, the NetBackup master should be configured to back up the **/var/TKLC/bkp/*.iso** file from the TVOE host.

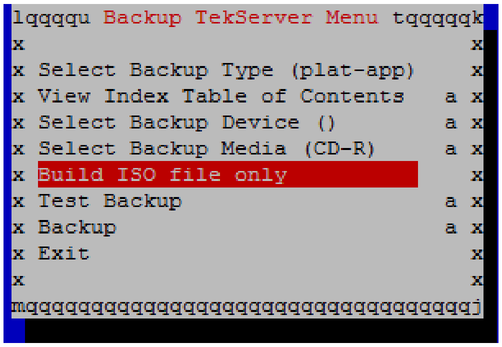
19.
☐
	RMS iLO/iLOM: Set up syscheck	syscheck must be configured to monitor bonded interfaces.
		Replace **bondedInterfaces** with **bond0**, or **bond0,bond1**, if segregated networks are used:
		`$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES --val=<bondedInterfaces>`
		`$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --enable`

20. ☐	**RMS iLO/iLOM**: Verify syscheck	Verify syscheck:

```
$ sudo /usr/TKLC/plat/bin/syscheck net ipbond -v
Expected output should look similar to below:
Running modules in class net...
      ipbond: Bonded interface bond0 is OK
                                 OK
LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

21. ☐	**RMS iLO/iLOM**: Verify server health	`$ alarmMgr –alarmStatus` This command should return no output on a healthy system. If any alarms are reported, contact My Oracle Support (MOS).

Procedure 12. Configure TVOE on Additional Rack Mount Servers

22. ☐	**RMS iLO/iLOM**: Back up TVOE using TPD platcfg utility	1. Enter the platcfg menu from the TVOE server. `$ sudo su – platcfg` 2. Navigate to **Maintenance > Backup and Restore >Backup Platform (CD/DVD)**. ***Note:*** If no cdrom device is found by TPD, a **No disk device available. This is normal on systems without a cdrom device** error displays. Press **Enter**. 3. Navigate to **Build ISO file only** and press **Enter**.  lqqqqu Backup TekServer Menu tqqqqqk Select Backup Type (plat-app) View Index Table of Contents Select Backup Device () Select Backup Media (CD-R) Build ISO file only Test Backup Backup Exit mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj ***Note:*** Creating the ISO image may happen so quickly that this screen may only display for an instant. 4. Exit platcfg by selecting **Exit**. After the ISO is created, platcfg returns to the Backup TekServer menu. The ISO has been created and is located in the **/var/TKLC/bkp/** directory. An example filename of a backup file that was created is **RMS503u14-plat-app-201210301505.iso**. 5. Move the TVOE backup to a customer provided backup server for safe keeping.
23. ☐	Repeat	Repeat this procedure for additional rack mount servers.

3.10 Determine VM Placement

Note: Skip this section if deploying a non-HA lab node of DL380 Gen system**.**

To maximize performance efficiency, customers who are deploying DSR on **Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 (10Gbps)** servers may obtain the DSR VM placement information document. This recommended document can be obtained from an Oracle representative for implementation. If the DSR VM placement information is NOT available, the customer may use [16] DSR VM Placement and CPU Socket Pinning Tool.

Notes:

- Determine the need for VM placement for all components of the DSR installation (PMAC, IDIH, DSR, and SDS).
- HP DL380 Gen 9 equipped with onboard 1Gbps NICs should follow Appendix S VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1Gbps NICs).

3.11 Deploy Redundant PMAC (Optional)

Note: **Non-HA Lab Node Installations Only (Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9)**: Skip this section.

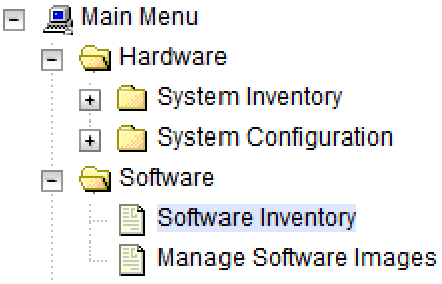
Procedure 13. Install a Redundant PMAC

This procedure is optional and required only if the redundant PMAC server feature is to be deployed.

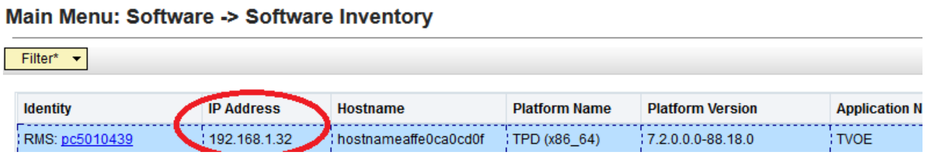
This procedure deploys a redundant PMAC and creates the first backup from the primary PMAC.

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

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

<table>
<tr><td>1.
☐</td><td>Primary PMAC: Login</td><td>Establish an SSH session to the primary PMAC and login as admusr.</td></tr>
<tr><td>2.
☐</td><td>PMAC: Exchange SSH keys between primary PMAC and redundant PMAC’s TVOE host</td><td>Use the PMAC GUI to determine the control network IP address of the redundant PMAC’s TVOE host server.
1. From the PMAC GUI, navigate to Software > Software Inventory.


Main Menu
Hardware
System Inventory
System Configuration
Software
Software Inventory
Manage Software Images

2. Note the IP address for the PMAC’s TVOE host server.

Main Menu: Software -> Software Inventory
Filter*
<table>
<tr><th>Identity</th><th>IP Address</th><th>Hostname</th><th>Platform Name</th><th>Platform Version</th><th>Application N</th></tr>
<tr><td>RMS: pc5010439</td><td>192.168.1.32</td><td>hostnameaffe0ca0cd0f</td><td>TPD (x86_64)</td><td>7.2.0.0.0-88.18.0</td><td>TVOE</td></tr>
</table>
3. Obtain a terminal session to PMAC and login as admusr.
4. Exchange SSH keys for admusr between the primary PMAC and the PMAC’s TVOE host server using the keyexchange utility and the control network IP address for the MP blade server.
<code>$ keyexchange admusr@<MP_Control_Blade_IP Address></code>
5. When asked for the password, type the password for the admusr of the PMAC’s TVOE host server.</td></tr>
<tr><td>3.
☐</td><td>Primary PMAC: Export the PMAC ISO image to the redundant PMAC’s TVOE host</td><td><code>$ sudo /usr/sbin/exportfs <redundant PMAC TVOE Host Control IP>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name></code></td></tr>
</table>

Procedure 13. Install a Redundant PMAC

4. ☐	**Primary PMAC**: SSH to the redundant PMAC's TVOE host	Establish an SSH session to the redundant PMAC's TVOE host server and login as **admusr**. `$ sudo ssh admusr@<redundant PMAC’s TVOE Host server control IP>`
5. ☐	**Redundant PMAC's TVOE Host**: Mount the PMAC upgrade media from the primary PMAC server	`$ sudo /bin/mount <primary_pmac_control_IP>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name> /mnt/upgrade`

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 (NetBackup or isoimagesVolSizeGB) should match the configuration of the primary PMAC.
		Reference Procedure 5, step 3.
		For this example, deploy a PMAC without the NetBackup feature.
		`$ 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>`
		The PMAC deploys and boots. The management and control network displays based on the settings provided to the pmac-deploy script.

7. ☐	**Redundant PMAC's TVOE Host**: Unmount media	`$ cd /` `$ sudo /bin/umount /mnt/upgrade`

Procedure 13. Install 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 :

```
$ sudo /usr/bin/virsh list

Id  Name            State
1   myTPD           running
2   PM&C            running
3   Redundant PM&C running
```

```
$ sudo /usr/bin/virsh console <Redundant PM&C>

[Output Removed]

Starting ntdMgr: [ OK ]
Starting atd: [ OK ]
'TPD Up' notification(s) already sent: [ OK ]
upstart: Starting tpdProvd...
upstart: tpdProvd started.
PM&Cdev7 login:
```

9. ☐ **Redundant PMAC**: Verify the redundant PMAC is configured correctly on first boot

   1. Establish an SSH session to the redundant PMAC and login as **admusr**.
   2. Run this command (there should be no output):

```
$ sudo /bin/ls /usr/TKLC/plat/etc/deployment.d/
```

10. ☐ **Redundant PMAC's TVOE Host**: Error doing verification, if error displays

If an error displays, use this command to delete the redundant PMAC guest and re-deploy the guest again.

```
$ sudo guestMgr –remove < Redundant PMAC_Name>
```

11. ☐ **Redundant PMAC**: Set the PMAC time zone

Note: Valid time zones can be found in Appendix J List of Frequently Used Time Zones.

   1. Run:

```
$ sudo set_pmac_tz.pl <time zone>
```

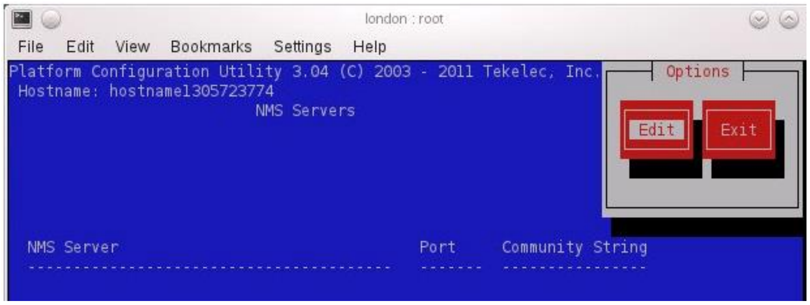
Example:

```
$ sudo set_pmac_tz.pl America/New_York
```

   2. Verify the time zone has been updated.

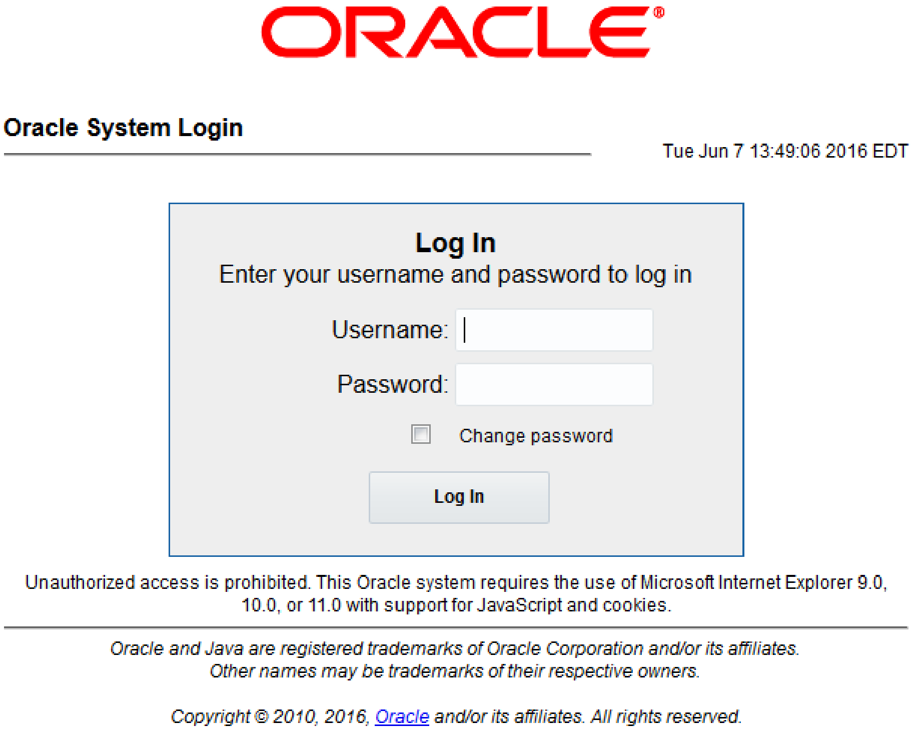
```
$ sudo date
```

Procedure 13. Install a Redundant PMAC

12.
☐
	Redundant PMAC: Set SNMP	1. Enter the platcfg menu.
		`$ sudo su - platcfg`
		2. Navigate to **Network Configuration > SNMP Configuration > NMS Configuration**.
		 london : root
		File Edit View Bookmarks Settings Help
		Options
		Edit
		Exit`Platform Configuration Utility 3.04 (C) 2003 - 2011 Tekelec, Inc.`
		`Hostname: hostname1305723774`
		`NMS Servers`
		`NMS Server                              Port     Community String`
		`--------------------------------------- -------  ----------------`
		3. Select **Edit** > **Add a New NMS Server**.
		4. Enter all the information to complete the form about the SNMP trap destination.
		Refer to Appendix H SNMP Configuration for more information.
		5. Click **OK** to finalize the configuration.
		6. Click **Exit**.
		7. Click **Yes** and wait until the Alarm Routing Service restarts.
		8. Exit platcfg.

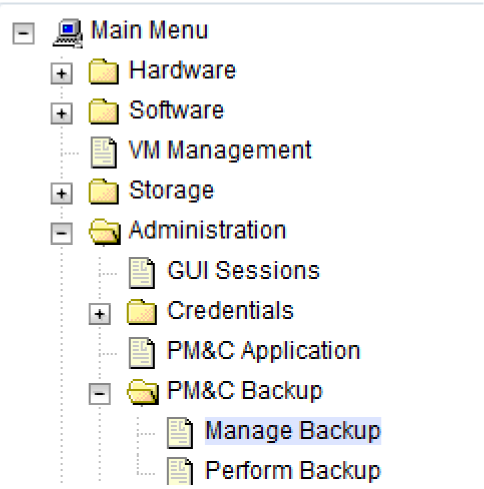
13. ☐	**Redundant PMAC**: Reboot the server	`$ sudo init 6`

Procedure 13. Install a Redundant PMAC

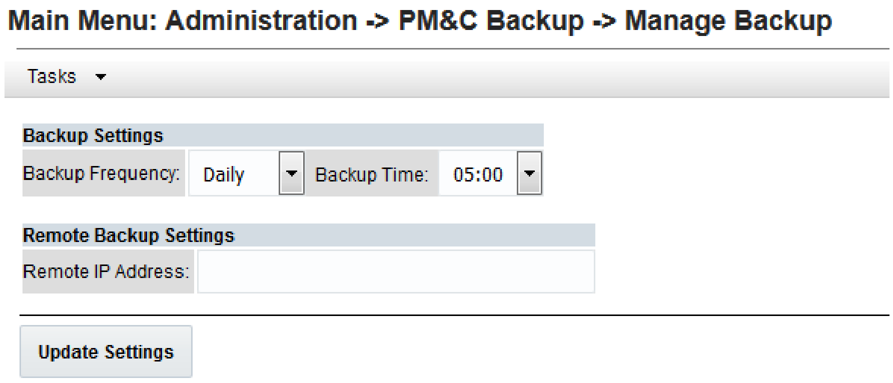
14. ☐	**PMAC GUI**: Login	1. Open the web browser and navigate to the PMAC GUI: `http://<PMAC_network_IP>` 2. Login as the **guiadmin** user:  Oracle System Login Tue Jun 7 13:49:06 2016 EDT Log In Enter your username and password to log in Username: Password: ☐ Change password Unauthorized access is 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 13. Install a Redundant PMAC

<table>
<tr>
<td>15.
☐</td>
<td>**PMAC GUI**:
Configure backups</td>
<td>
1. Navigate to **Administration > PM&C Backup > Manage Backup**.


Main Menu
Hardware
Software
VM Management
Storage
Administration
GUI Sessions
Credentials
PM&C Application
PM&C Backup
Manage Backup
Perform Backup

2. Configure the primary PMAC to send backups to the redundant PMAC by entering the management IP of the redundant PMAC server for the **Remote IP Address**.

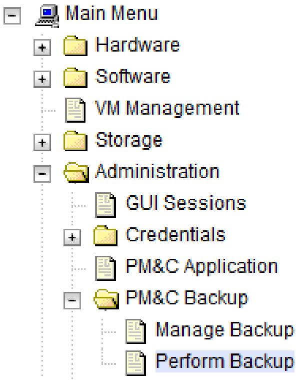

Main Menu: Administration -> PM&C Backup -> Manage Backup
Tasks
Backup Settings
Remote Backup Settings
Update Settings

Backup Frequency: Daily
Backup Time: 05:00
Remote IP Address:
</td>
</tr>
</table>

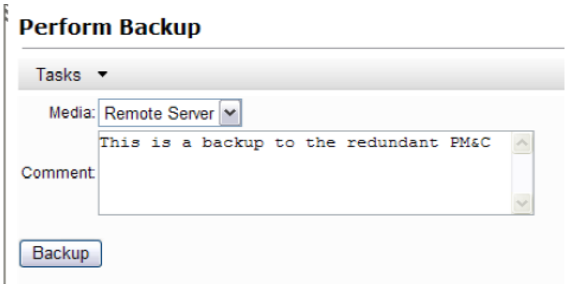
Procedure 13. Install a Redundant PMAC

<table>
<tr>
<td>16.
☐</td>
<td>PMAC GUI: Perform initial backup</td>
<td>

1. Navigate to **Administration > PM&C Backup > Perform Backup**.


Main Menu
Hardware
Software
VM Management
Storage
Administration
GUI Sessions
Credentials
PM&C Application
PM&C Backup
Manage Backup
Perform Backup

2. Select the Remote Server from the Media options
3. Enter any desired comments
4. Click **Backup**.


Perform Backup
Tasks
Backup

Media: Remote Server

Comment: This is a backup to the redundant PM&C

5. Verify the backup was successful by clicking 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.

</td>
</tr>
<tr>
<td>17.
☐</td>
<td>Primary PMAC: Un-Export the PMAC ISO image to the redundant PMAC’s TVOE host server</td>
<td>

```
$ sudo /usr/sbin/exportfs –u <redundant PMAC TVOE Host
Control IP>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name>
```

</td>
</tr>
</table>

3.12 Virtual Machine/Network Fast Deployment

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

This procedure loads the DSR, SDS, and TPD ISOs onto the PMAC server.

Note: If deploying IDIH, the IDIH ISOs can also be loaded.

Needed Material: Application media

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

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

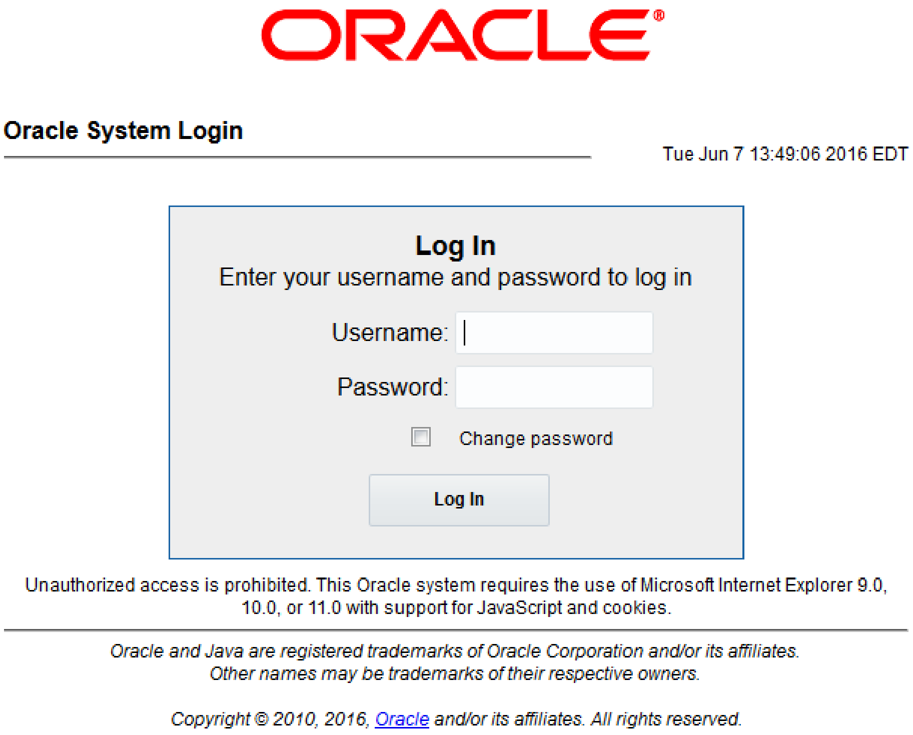
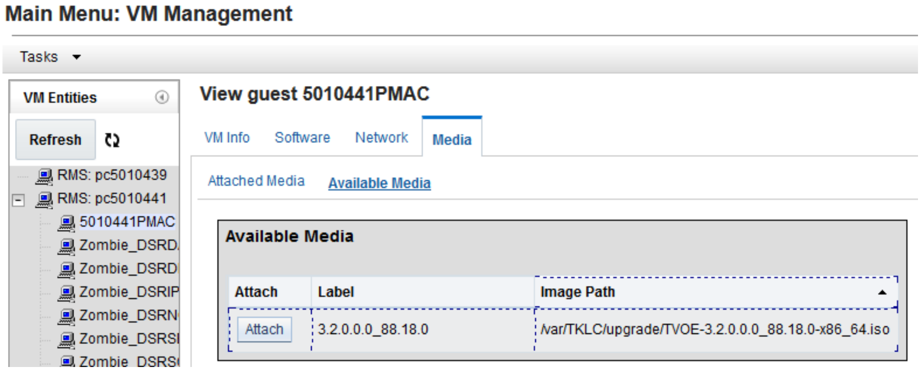
1. ☐	**PMAC's TVOE**: Load application ISO	Use one of the following options to add the TPD ISO image to the PMAC: **Option 1 —** Insert the CD containing the TPD image into the removable media drive. **Option 2 —** Attach the USB device containing the ISO image to a USB port. **Option 3 —** Copy the Application ISO file to the PMAC server into the **/var/TKLC/smac/image/isoimages/home/smacftpusr/** directory as **pmacftpusr** user: cd to the directory where your ISO image is located on the TVOE host (not on the PMAC server). Using sftp, connect to the PMAC server.

```
$ sftp pmacftpusr@<pmac_management_network_ip>
$ put <image>.iso
```

After the image transfer is 100% complete, close the connection.

```
$ quit
```

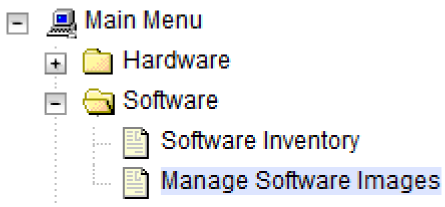
Procedure 14. Load DSR, SDS, and TPD ISOs onto the PMAC Server

2. ☐	**PMAC GUI**: Login	1. Open the web browser and navigate to the PMAC GUI: `http://<PMAC_network_IP>` 2. Login as the **guiadmin** user:  Oracle System Login Tue Jun 7 13:49:06 2016 EDT Log In Enter your username and password to log in Username: Password: ☐ Change password 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.*
3. ☐	**PMAC GUI**: Attach the software Image to the PMAC guest	If the ISO image was transferred directly to the PMAC guest using sftp, skip this step and continue with the next step. 1. From the PMAC GUI, navigate to **VM Management > PMAC guest > View VM Guest > Media tab**. 2. Locate the ISO image in the **Available Media** list and click its **Attach** button.  Main Menu: VM Management Tasks VM Entities Refresh RMS: pc5010439 RMS: pc5010441 5010441PMAC Zombie_DSRD Zombie_DSRD Zombie_DSRIP Zombie_DSRN Zombie_DSRSI Zombie_DSRS View guest 5010441PMAC VM Info Software Network Media Attached Media Available Media Available Media 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

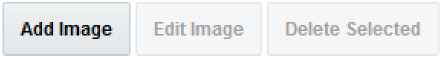
Procedure 14. Load DSR, SDS, and TPD ISOs onto the PMAC Server

4. ☐ **PMAC GUI**: Add TPD image

1. Navigate to **Software > Manage Software Images**.

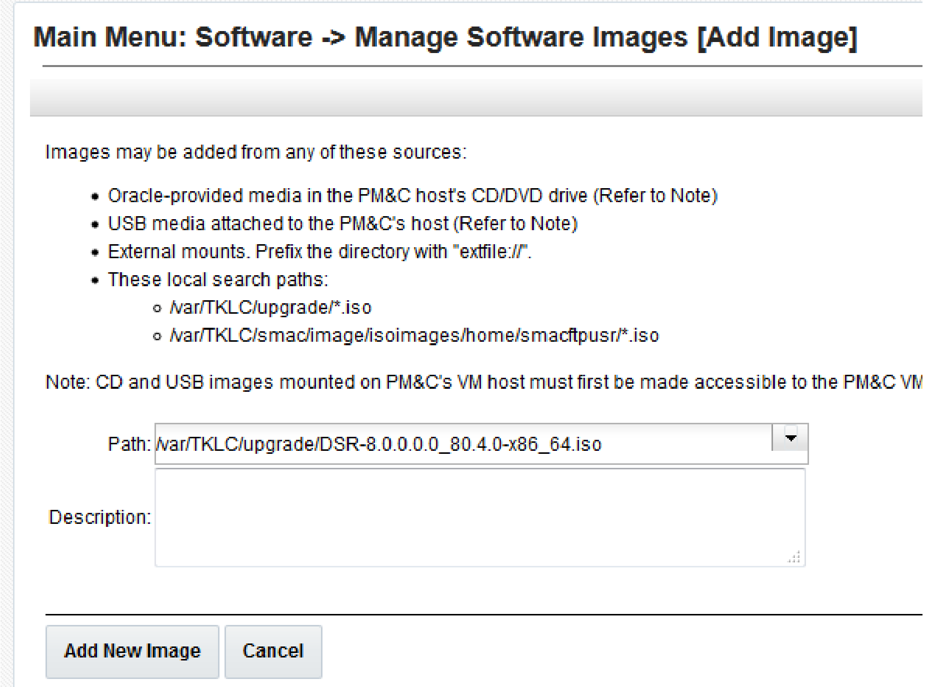


2. Click **Add Image**.
3. Select the image from the options.



If the image was supplied on a CD or a USB drive, it displays 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 on the second device, **device://dev/sr1**. If one or more CD or USB-based images was already on the management server before you started this procedure, select a correspondingly higher device number.

If the image was transferred to PMAC using sftp, it displays in the list as a local file **/var/TKLC/...**.



Main Menu: Software -> Manage Software Images [Add Image]

Images may be added from any of these sources:

- Oracle-provided media in the PM&C host's CD/DVD drive (Refer to Note)
- USB media attached to the PM&C's host (Refer to Note)
- External mounts. Prefix the directory with "extfile://".
- These local search paths:
  - /var/TKLC/upgrade/*.iso
  - /var/TKLC/smac/image/isoimages/home/smacftpusr/*.iso

Note: CD and USB images mounted on PM&C's VM host must first be made accessible to the PM&C VM

Path: /var/TKLC/upgrade/DSR-8.0.0.0.0_80.4.0-x86_64.iso

Description:

4. Select the appropriate path and click **Add New Image**.
5. Check the progress clicking the **Task Monitoring** link. Observe the green bar indicating success.
6. Once complete, remove the TPD Media from the optical drive of the management server.

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

5. ☐	**PMAC GUI**: Load DSR ISO	If the DSR ISO has not 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 h has not 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

This procedure creates network bond interfaces and bridges, sets TVOE host NTP servers, and creates virtual machines.

Note: Refer to section 3.10 for VM placement.

Prerequisites:

- TVOE has been installed and configured on the target RMS
- DSR ISO has been loaded onto PMAC

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

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

1. ☐	**PMAC**: Login	Establish an SSH session to the PMAC server and login as **admusr**.

2.
☐
	PMAC: Transfer script and supporting files	1. Copy script and supporting files from the DSR iso.
		`$ sudo rsync -avz --exclude cpuset.py --exclude irqtune.sh --exclude tuned_tvoe.tar /usr/TKLC/smac/html/TPD/<DSR ISO loaded previous procedure>/upgrade/overlay/RMS/ /usr/TKLC/smac/etc/RMS/`
		2. Change permissions.
		`$ sudo chmod 777 /usr/TKLC/smac/etc/RMS/*`

3. ☐	**PMAC**: Edit/Update configuration file	1. Change directory. `$ cd /usr/TKLC/smac/etc/RMS/` 2. Edit/Update the configuration file (rms.cfg). Read all notes shown here before editing the file. ***Notes***: • Comment out configuration items that are not needed. • Create a separate configuration file for each rack mount server being deployed. • The cabinet ID in the configuration file needs to match the cabinet added in Procedure 10. The following items are mandatory: • siteName • tpdIso

Procedure 15. Execute VM/Network Fast Deployment

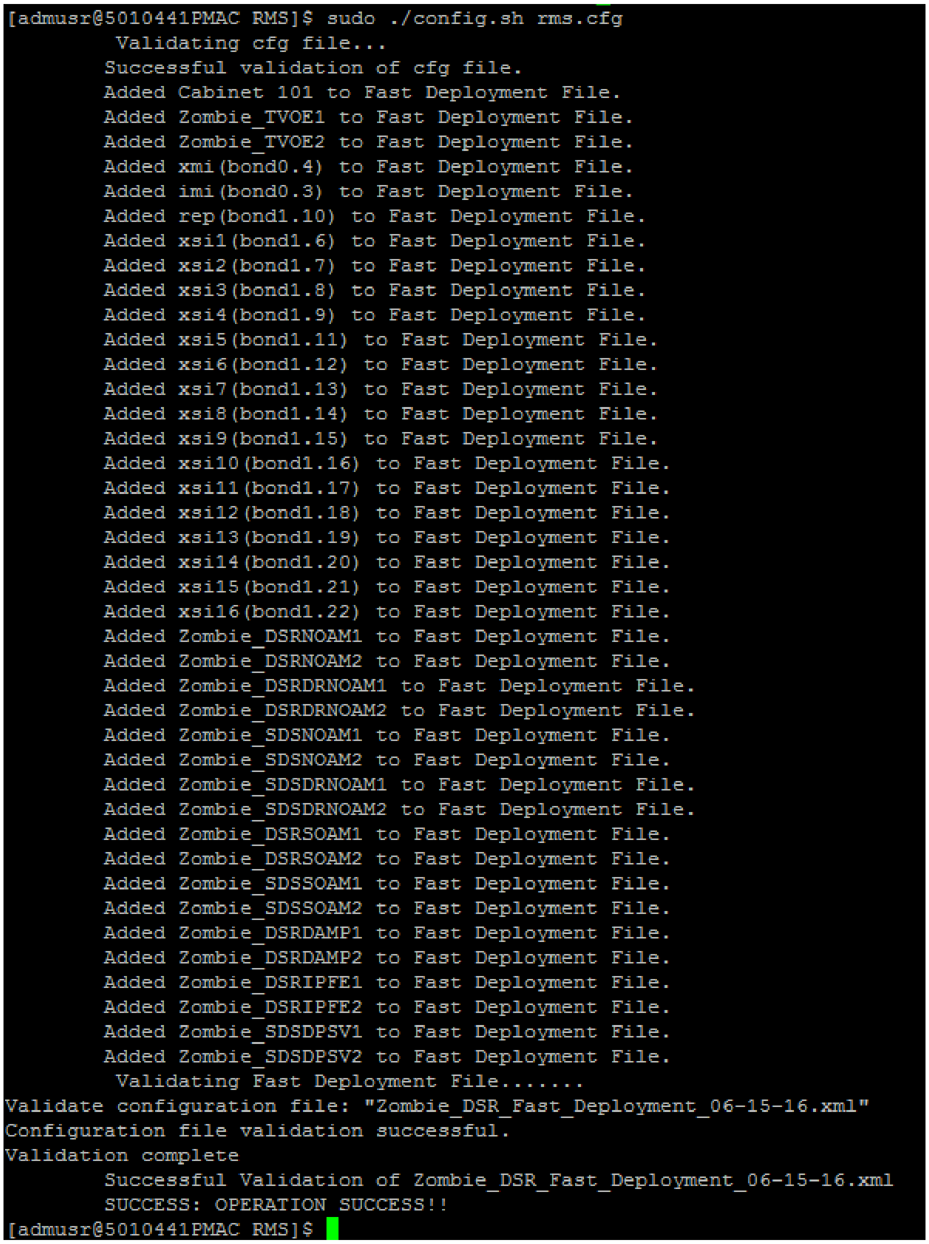
		- dsrIso (if DSR VMs are being configured) - sdsIso (if SDS VMs are being configured) - NETWORK_xmi (if DSR/SDS NOAM/DRNOAMs are being configured) - XMIGATEWAY (if DSR/SDS NOAM/DRNOAMs are being configured) - XMISUBNETMASK (if DSR/SDS NOAM/DRNOAMs are being configured) - DSRNOAM1XMIIPADDRESS (if DSRNOAM1 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) ***Notes***: - Refer to Appendix R VM Automation Profile Values for DSR and SDS profile values with the configuration file. - Comment out SDS and DSR profile items if cooresponding products are not used. - **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. - The VM names should not be modified in the .cfg file. The names are fixed and are prefixed in the siteName. - The VM locations should not be changed from their **RMSx** format. Each RMS should correspond with a separate rack mount server. - Do not change the network bond interfaces from their **bondx.x** format. If bond1 was previously created for segregated signaling, update the bond interface to reflect the base bond interface (for example, bond0.x or bond1.x). 3. To receive the iso names for **tpdIso**, **dsrIso**, and **sdsIso**, execute this command: `$ ls /var/TKLC/smac/image/repository` ***Note:*** DO NOT append **.iso** to the image name.
4. ☐	**PMAC**: Rename/Transfer configuration file	Rename/Copy each of the above created configuration files 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 with the config file	***Note:*** If this command is executed on multiple cfg files, it overwritea the existing xml file. Rename the xml file before running this command again.

```
$ 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_SDSDRNOAM1 to Fast Deployment File.
        Added Zombie_SDSDRNOAM2 to Fast Deployment File.
        Added Zombie_DSRSOAM1 to Fast Deployment File.
        Added Zombie_DSRSOAM2 to Fast Deployment File.
        Added Zombie_SDSSOAM1 to Fast Deployment File.
        Added Zombie_SDSSOAM2 to Fast Deployment File.
        Added Zombie_DSRDAMP1 to Fast Deployment File.
        Added Zombie_DSRDAMP2 to Fast Deployment File.
        Added Zombie_DSRIPFE1 to Fast Deployment File.
        Added Zombie_DSRIPFE2 to Fast Deployment File.
        Added Zombie_SDSDPSV1 to Fast Deployment File.
        Added Zombie_SDSDPSV2 to Fast Deployment File.
         Validating Fast Deployment File.......
Validate configuration file: "Zombie_DSR_Fast_Deployment_06-15-16.xml"
Configuration file validation successful.
Validation complete
        Successful Validation of Zombie_DSR_Fast_Deployment_06-15-16.xml
        SUCCESS: OPERATION SUCCESS!!
[admusr@5010441PMAC RMS]$ 
```

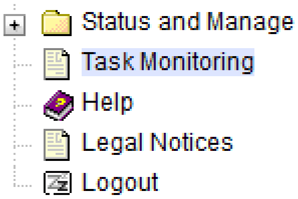
Procedure 15. Execute VM/Network Fast Deployment

6.
☐
	PMAC: Run fast deployment	With the file generated from the config.sh script, execute this command to start fast deployment.
		`$ screen`
		`$ sudo fdconfig config --file=<fd_config.xml>`
		Example:
		`$ sudo fdconfig config --file=tvoe-ferbrms4_01-22-15.xml`
		Note: This is a long duration command (45-90 minutes). If the screen command was run before executing fdconfig, perform a **screen -dr** to resume the screen session in the event of a terminal timeout, etc

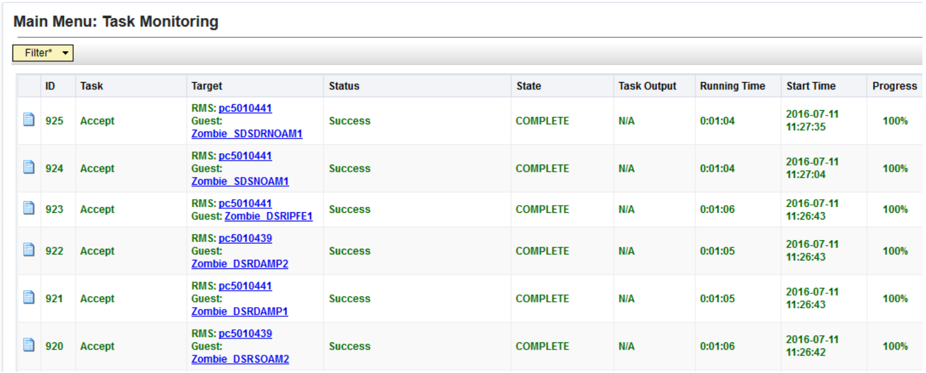
Procedure 15. Execute VM/Network Fast Deployment

7. ☐ PMAC **GUI**: Monitor the configuration

1. If not already done so, establish a GUI session on the PMAC server.
2. Navigate to **Task Monitoring**.



3. Monitor the configuration to completion.



Main Menu: Task Monitoring

	ID	Task	Target	Status	State	Task Output	Running Time	Start Time	Progress
	925	Accept	RMS: pc5010441 Guest: Zombie_SDSDRNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:35	100%
	924	Accept	RMS: pc5010441 Guest: Zombie_SDSNOAM1	Success	COMPLETE	N/A	0:01:04	2016-07-11 11:27:04	100%
	923	Accept	RMS: pc5010441 Guest: Zombie_DSRIPFE1	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:43	100%
	922	Accept	RMS: pc5010439 Guest: Zombie_DSRDAMP2	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%
	921	Accept	RMS: pc5010441 Guest: Zombie_DSRDAMP1	Success	COMPLETE	N/A	0:01:05	2016-07-11 11:26:43	100%
	920	Accept	RMS: pc5010439 Guest: Zombie_DSRSOAM2	Success	COMPLETE	N/A	0:01:06	2016-07-11 11:26:42	100%

Note: If a failure occurs with fdconfig, logs can be accessed in **/var/TKLC/log/fdconfig/fdconfig.log**.

```
[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
```

4. Run command to restart the fdconfig after a failure has occurred and has been resolved:

```
$ sudo fdconfig restart --
file=deploy_melbourne_20170329T202458_701b.fdcdb
```

Procedure 15. Execute VM/Network Fast Deployment

8. ☐	**PMAC**: Repeat for each rack mount server configuration file	Repeat steps 4. through 7. for each rack mount server/configuration file created from step 3.

9.
☐
	PMAC: Back up FDC file	Create the fdc directory so the fdc file is backed up by PMAC.
		1. Create the fdc backup directory.
		`$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/fdc`
		2. Change permissions.
		`$ sudo chmod 777 /usr/TKLC/smac/etc/fdc`
		3. Copy the fdc file to the fdc backup directory.
		`$ sudo cp /usr/TKLC/smac/etc/RMS/<fdc_file> /usr/TKLC/smac/etc/fdc/`
		Note: The fdc file referred to here is the rms.cfg file.
		4. Rename it to **<hostname>.cfg** to identify the correct fdc file during disaster recovery procedure.
		`$ sudo mv /usr/TKLC/smac/etc/fdc/<fdc_file> /usr/TKLC/smac/etc/fdc/<hostname.cfg>`

3.13 CPU Pinning

Notes:

- Skip this section if deploying a non-HA lab node of DL380 Gen system.
- **HP DL380 Gen 8**: Skip this procedure.

Procedure 16. Load DSR, SDS, and TPD ISOs onto the PMAC Server

This procedure configures VM CPU socket pinning on each TVOE host to optimize performance. ***Prerequisite***: Have already created VM guests Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact 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 3.10. ***Note:*** For HP Dl380 Gen 9 equipped with 1Gbps NICs, obtain the CPU socket pinning information from Appendix U CPU Pinning in HP DL380 Gen 9 (Onboard 1Gbps NICs).
2. ☐	**TVOE Host**: Login	Establish an SSH session to the TVOE host and login as **admusr**.
3. ☐	**TVOE Host**: Execute the CPU pinning script	1. Allocate CPU sets for **each** (including the PMACs) configured VM. `$ cd /var/TKLC/upgrade` 2. Print the current CPU pinning allocations.

Procedure 16. Load DSR, SDS, and TPD ISOs onto the PMAC Server

```
$ sudo ./cpuset.py --show
```

Expected output:

```
[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]
```

Notes:

There is known issue with PMAC in this release. PMAC uses all CPUs in the NUMA 0. PMAC will fix this issue in next release.

If this is the case, the command output displays NUMA Node 0 free CPUs count as 0.

```
NUMA node 0 Free CPUs: count = 0 []
```

- Clear the NUMA 0 and pin the CPU again.

  ```
  $ sudo ./cpuset.py --clear=<PMAC Name>
  ```

  For example:

  ```
  $ sudo ./cpuset.py --clear=Sterling-PMAC
  ```

- Set the CPU again for PMAC instance.

  ```
  $ sudo ./cpuset.py --set=<PMAC Name> --numa=0
  ```

  For example:

  ```
  $ sudo ./cpuset.py --set=Sterling-PMAC --numa=0
  Successful.  Domain Sterling-PMAC must be restarted
  for changes to take affect.
  ```

3. Allocate CPU pinning on each VM.

   ```
   $ sudo ./cpuset.py --set=<VM Name> --numa=<0/1>
   ```

   Example:

```
[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
```

Procedure 16. Load DSR, SDS, and TPD ISOs onto the PMAC Server

```
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]
```

Notes:

- If deploying IDIH, note the CPU pinning allocations since CPU pinning will be done as part of IDIH configuration (section 3.16).
- To clear pinning, execute this command on each VM, as necessary.

```
$ sudo ./cpuset.py --clear=<VM NAME>
```

Example:

```
[admusr@Sterling-TVOE-4 admusr]# sudo ./cpuset.py –
clear=Sterling2So-DA-MP4
```

4. ☐ Restart the TVOE host

```
$ sudo init 6
```

Procedure 16. Load DSR, SDS, and TPD ISOs onto the PMAC Server

5.
☐
	TVOE Host: Verify CPU pinning	1. Once the TVOE host is restarted, establish an SSH session to the TVOE host and login as **admusr**.
		2. Verify the CPU pinning is allocated by executing the following commands.
		`$ cd /var/TKLC/upgrade`
		3. 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.

3.14 DSR Application Configuration

3.14.1 NOAM Configuration

Procedure 17. Configure First DSR NOAM NE and Server

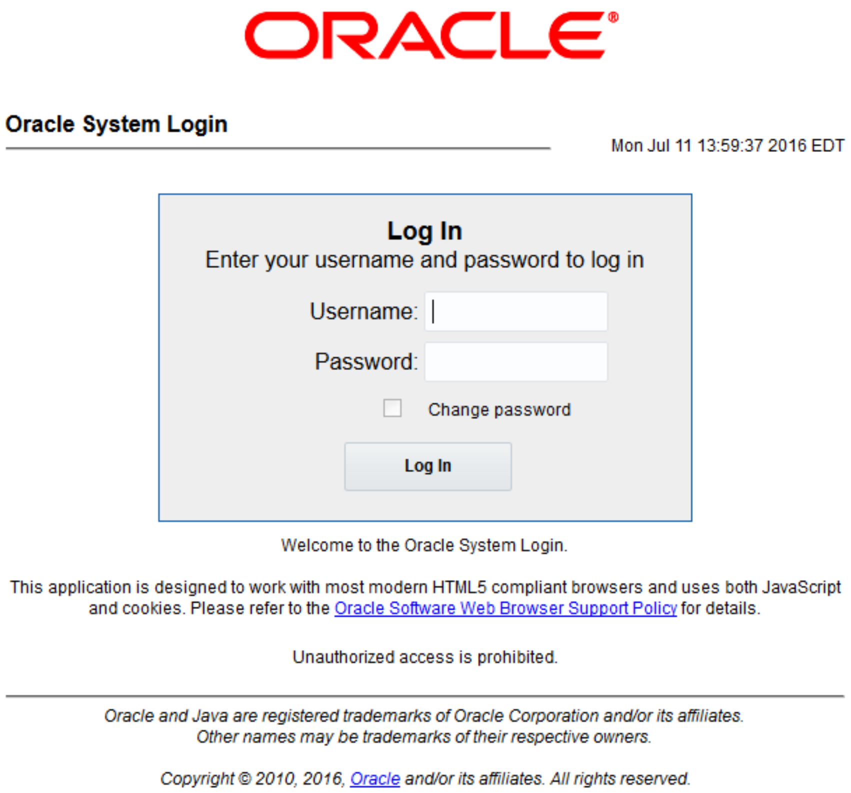
This procedure configures the first DSR NOAM network element and server.

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

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

1. ☐	Save the NOAM network data to an XML file	1. Use a text editor to create a NOAM network element file that describes the networking of the target install environment of your first NOAM server. 2. 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**. For example, a DSR2 NOAM network element XML file would have a **DSR2_NOAM_NetworkElement.xml** filename. Alternatively, you can update the sample DSR network element file. It can be found on the management server at: `/usr/TKLC/smac/html/TPD/<DSR Release>/upgrade/overlay/SAMPLE-NetworkElement.xml` A sample XML file can also be found in Appendix L Sample Network Element. ***Note:*** These 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.

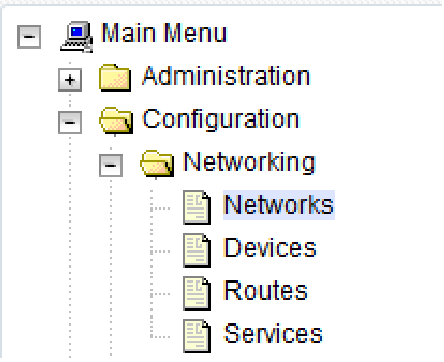
Procedure 17. Configure First DSR NOAM NE and Server

<table>
<tr>
<td>2.
☐</td>
<td>NOAM VIP GUI: Login</td>
<td>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server (defined and configured in the DSR fast deployment rms.cfg file). Open the web browser and enter a URL of:
`https://<Primary_NOAM_VIP_IP_Address>`
2. Login as the guiadmin user.
ORACLE
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.
<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></td>
</tr>
</table>

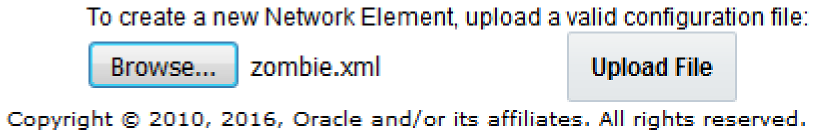
Procedure 17. Configure First DSR NOAM NE and Server

<table>
<tr>
<td>3.
☐</td>
<td>Create the NOAM network element using the XML file</td>
<td>

1. Navigate to **Configuration > Networking > Networks**.


Main Menu
Administration
Configuration
Networking
Networks
Devices
Routes
Services

2. Click **Browse** and type the pathname to the NOAM network XML file.



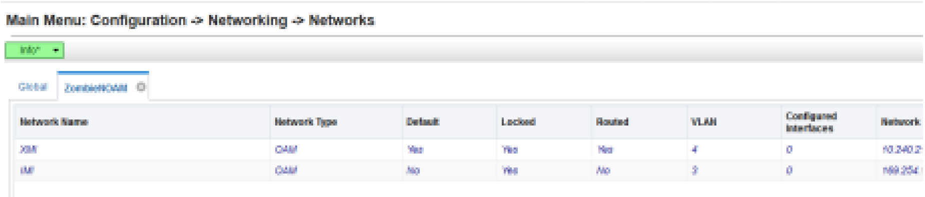
To create a new Network Element, upload a valid configuration file:

Browse...
zombie.xml
Upload File

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

3. Click **Upload File** to upload the XML file and configure the NOAM network element.

4. Once the data has been uploaded, a tab displays with the name of your network element. Click this tab to display a screen with the individual networks that are now configured.



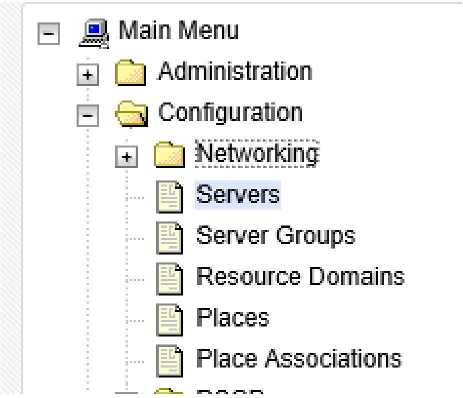
Main Menu: Configuration -> Networking -> Networks

Info
Global
ZombieNOAM

Network Name	Network Type	Default	Locked	Routed	VLAN	Configured Interfaces	Network
XMI	OAM	Yes	Yes	Yes	4	0	10.240.2
IMI	OAM	No	Yes	No	3	0	169.254

</td>
</tr>
<tr>
<td>4.
☐</td>
<td>Map services to networks</td>
<td>

1. Navigate to **Configuration > Services**.


Main Menu
Administration
Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Click **Edit** and set the services as shown in the table.

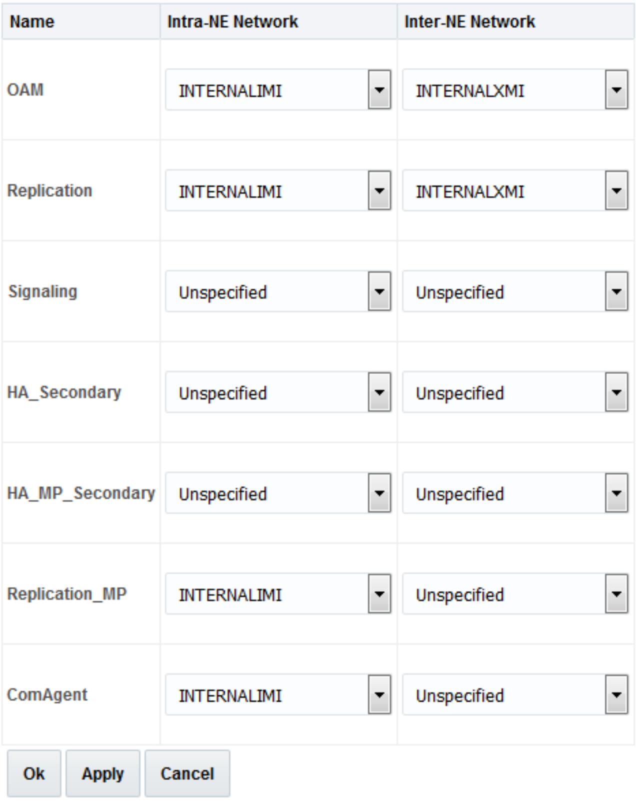
Name	Intra-NE Network	Inter-NE Network
OAM	<IMI Network>	<XMI Network>

</td>
</tr>
</table>

Procedure 17. Configure First DSR NOAM NE and Server

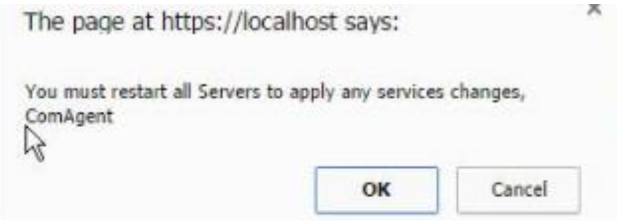
Replication	<IMI Network>	<XMI Network>
Signaling	Unspecified	Unspecified
HA_Secondary	Unspecified	Unspecified
HA_MP_Secondary	Unspecified	Unspecified
Replication_MP	<IMI Network>	Unspecified
ComAgent	<IMI Network>	Unspecified

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:



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

3. Click **OK** to apply the Service-to-Network selections.
4. Click **OK** when asked to restart all servers.



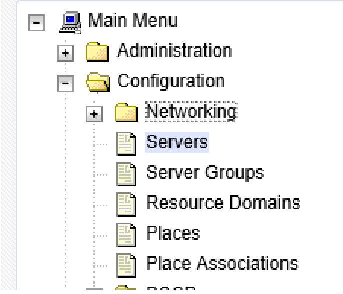
The page at https://localhost says:

You must restart all Servers to apply any services changes, ComAgent

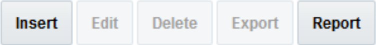
Procedure 17. Configure First DSR NOAM NE and Server

<table>
<tr>
<td>5.
☐</td>
<td>Insert the 1st NOAM server</td>
<td>

1. Navigate to **Configuration > Servers**.

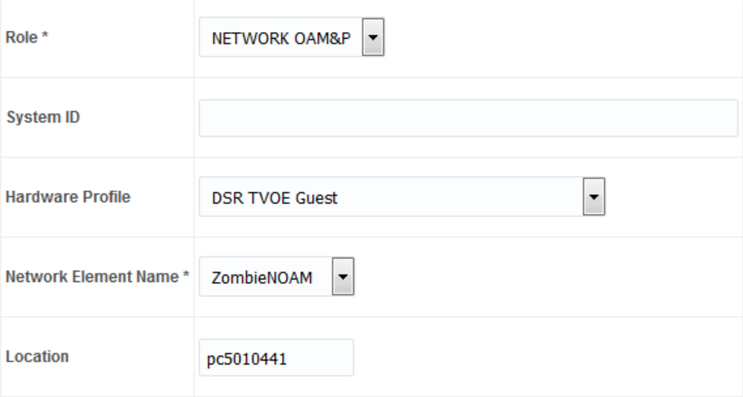

Main Menu
Administration
Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Click **Insert** to insert the new NOAM server into servers table.


Insert
Edit
Delete
Export
Report

3. Enter these values:

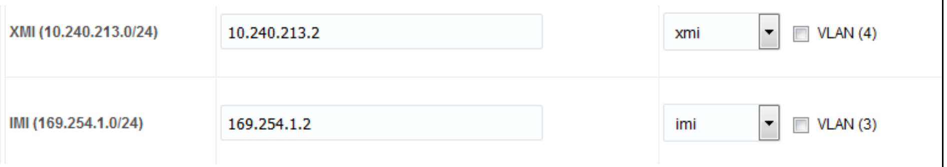
Hostname:	<Hostname>
Role:	Network OAM
System ID:	<Site System ID>
Hardware Profile:	DSR TVOE Guest
Network Element Name:	[Select NE]
Location:	<Enter an optional location description>



Role * NETWORK OAM&P
System ID
Hardware Profile DSR TVOE Guest
Network Element Name * ZombieNOAM
Location pc5010441

4. For the **XMI** network, type the server XMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.

5. For the **IMI** network, type the server IMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.



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)

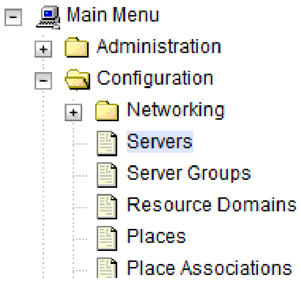
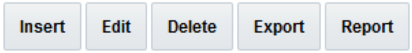
6. Add this NTP server:

NTP Server	Preferred?
First-NOAM-TVOE-IP-Address>	Yes

7. Click **OK**.

</td>
</tr>
</table>

Procedure 17. Configure First DSR NOAM NE and Server

6. ☐	Export the initial configuration	1. Navigate to **Configuration > Servers**.  Main Menu Administration Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. From the GUI screen, select the NOAM server and click **Export** to generate the initial configuration data for that server. 
7. ☐	**NOAM**: Copy configuration file to 1st NOAM server	1. 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 and login as **admusr**. 2. 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 has a filename like **TKLCConfigData.<hostname>.sh**. The following is an example: `$ sudo cp /var/TKLC/db/filemgmt/TKLCConfigData.blade01.sh /var/tmp/TKLCConfigData.sh` ***Note:*** The file in **/var/tmp/** directory **MUST** be **TKLCConfigData.sh**. The automatic configuration daemon looks for the **TKLCConfigData.sh** file in the **/var/tmp** directory, implements the configuration in the file, and asks the user to reboot the server.
8. ☐	**NOAM**: Wait for configuration to complete	Wait to be prompted to reboot the server, but DO NOT reboot the server, it is rebooted later in this procedure. ***Note:*** Ignore the warning about removing the USB key, since no USB key is present.

9.
☐
	SDS NOAM iLO: Set the time zone and reboot the server	***Note:*** Valid time zones can be found in Appendix J List of Frequently Used Time Zones.
		1. Run:
		`$ sudo set_pmac_tz.pl <time zone>`
		Example:
		`$ sudo set_pmac_tz.pl America/New_York`
		2. Reboot the server.
		`$ sudo init 6`

Procedure 17. Configure First DSR NOAM NE and Server

10. ☐	**MP Server**: Verify server health	Login as **admusr** to the first SDS NOAM server and make sure no errors are returned.

```
$ 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
```

Procedure 18. Configure the DSR NOAM Server Group

This procedure configures the DSR NOAM server group.

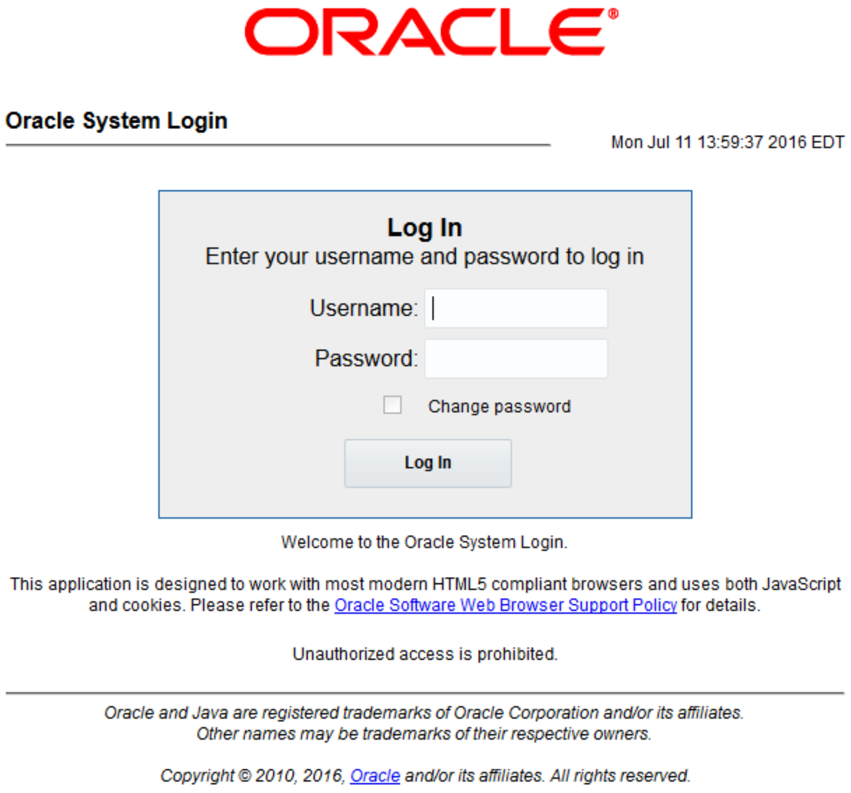
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.

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

1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:

```
https://<Primary_NOAM_XMI_VIP_IP_Address>
```

2. Login as the **guiadmin** user.



Oracle System Login

Mon Jul 11 13:59:37 2016 EDT

Log In

Enter your username and password to log in

Welcome to the Oracle System Login.

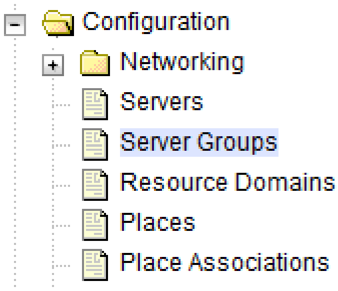
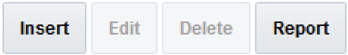
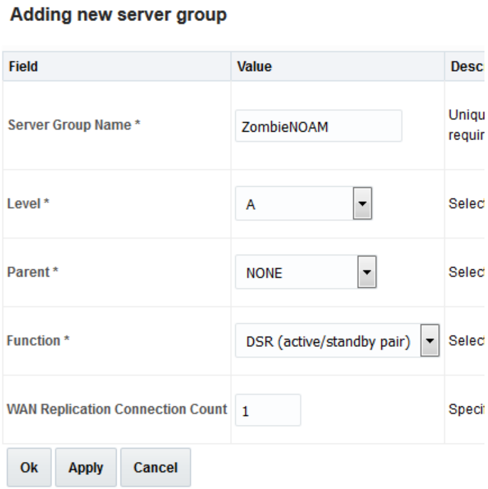
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

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.

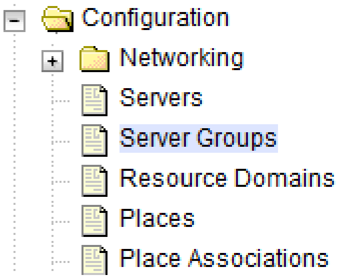
Procedure 18. Configure the DSR NOAM Server Group

2. ☐	**NOAM GUI**: Enter the NOAM server group data	1. Navigate to **Configuration > Server Groups**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Click **Insert**.  Insert Edit Delete Report 3. Enter these values: **Server Group Name**: <Server Group Name> **Level**: A **Parent**: None **Function**: DSR (Active/Standby Pair) **WAN Replication Connection Count**: Use Default Value  Adding new server group 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 Ok Apply Cancel 4. Click **OK**.

Procedure 18. Configure the DSR NOAM Server Group

3. ☐ **NOAM GUI**: Edit the NOAM server group

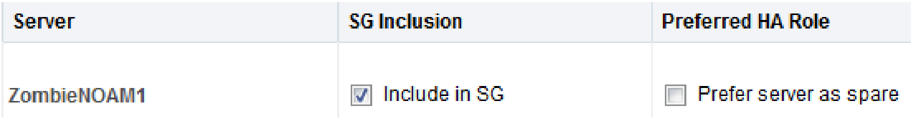
1. Navigate to **Configuration > Server Groups**.



2. Select the new server group and click **Edit**.

Insert
Edit
Delete
Report

3. Select the network element that represents the NOAM.
4. Mark the **Include in SG** checkbox for the NOAM server.
5. Leave other checkboxes blank.



Server	SG Inclusion	Preferred HA Role
ZombieNOAM1	☑ Include in SG	☐ Prefer server as spare

6. Click **OK**.

4. ☐ **NOAM**: Verify NOAM blade server role

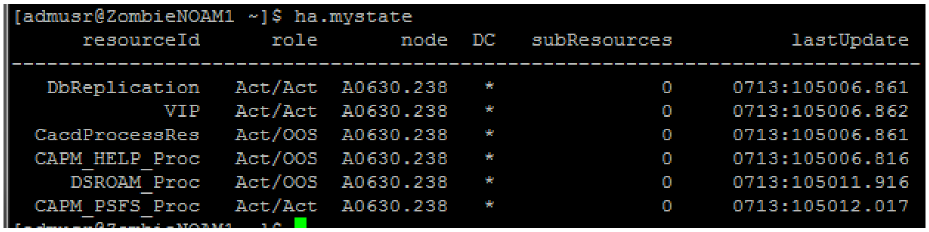
1. From terminal session on the first NOAM server, execute this command:

```
$ ha.mystate
```

2. Verify the **DbReplication** and **VIP** items under the **resourceId** column have a value of **Active** under the **role** column.

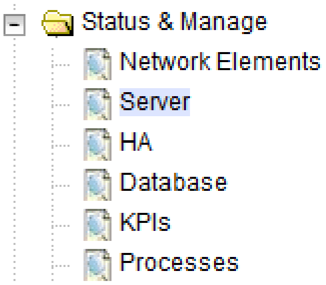
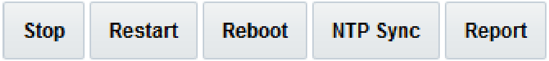
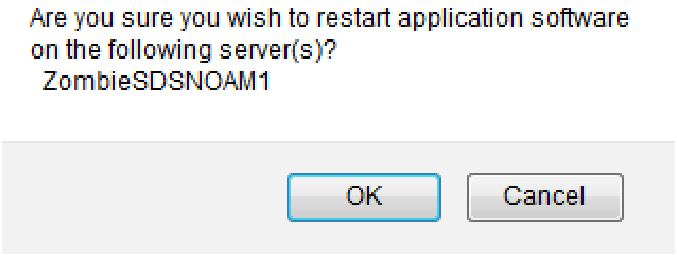
You may have to wait a few minutes for it to become in that state.

Example:



```
[admusr@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
```

Procedure 18. Configure the DSR NOAM Server Group

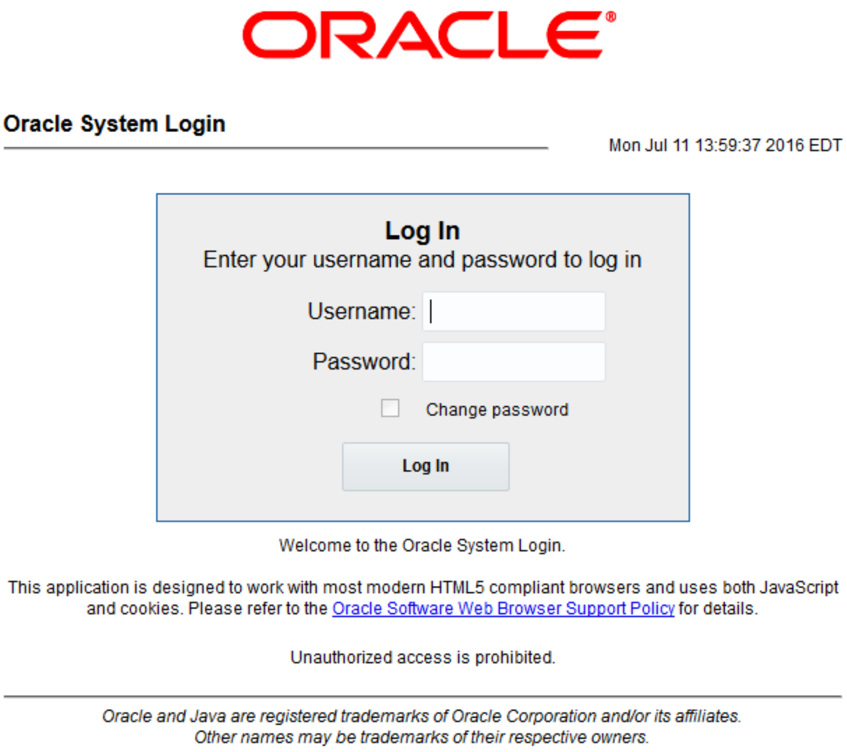
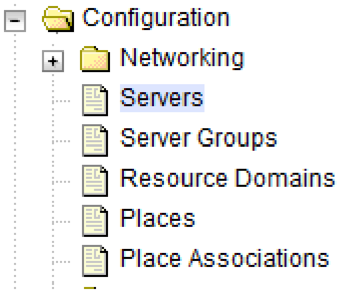
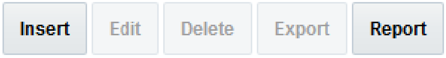
5. ☐	**NOAM VIP GUI**: Restart the 1st NOAM servers	1. From the NOAM GUI, navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the first NOAM server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm. Are you sure you wish to restart application software on the following server(s)? ZombieSDSNOAM1 .

Procedure 19. Configure Second DSR NOAM Server

This procedure configures the second DSR NOAM server.

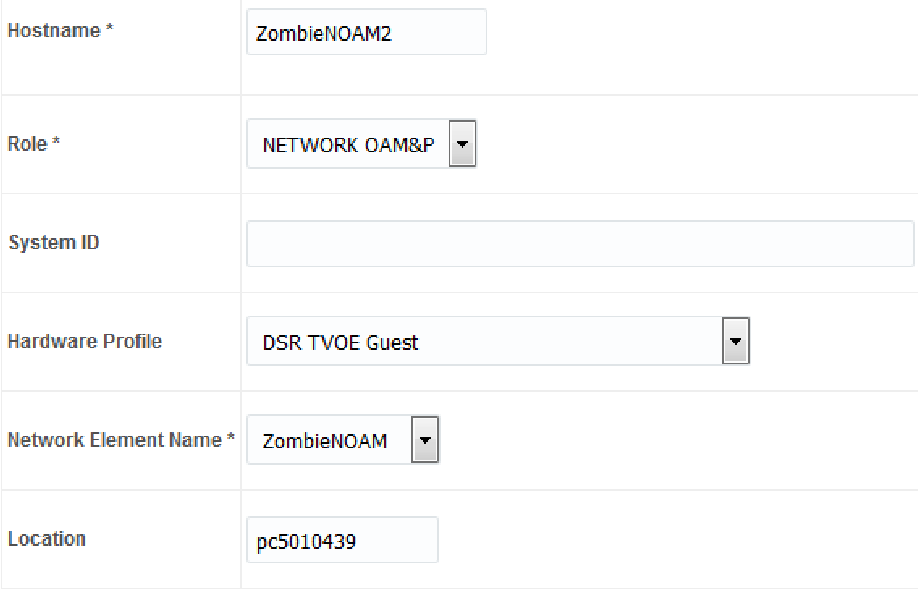
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.

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

1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_XMI_VIP_IP_Address>` 2. Login as the **guiadmin** user.  Oracle System Login Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.*
2. ☐	**NOAM VIP GUI**: Insert the 2nd NOAM server	1. Navigate to **Configuration > Servers**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Click **Insert** to insert the second NOAM server into the servers table.  3. Enter these values:

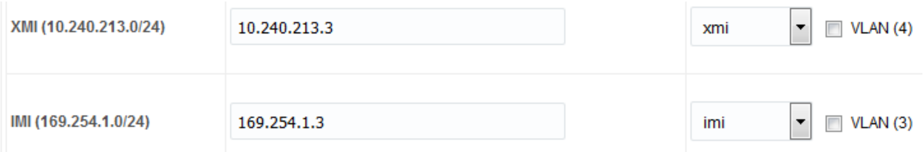
Procedure 19. Configure Second DSR NOAM Server

Hostname: <Hostname>
Role: Network OAM
System ID: <Site System ID>
Hardware Profile: DSR TVOE Guest
Network Element Name: [Select NE]
Location: <Enter an optional location description>



Hostname * ZombieNOAM2
Role * NETWORK OAM&P
System ID
Hardware Profile DSR TVOE Guest
Network Element Name * ZombieNOAM
Location pc5010439

4. For the **XMI** network, type the server XMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.
5. For the **IMI** network, type the server IMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.



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)

6. Add this NTP server.

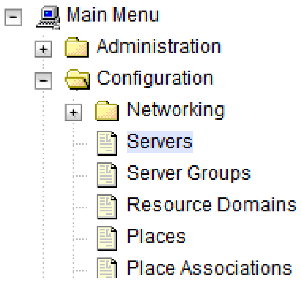
NTP Server	Preferred?
<Second-NOAM-TVOE-IP-Address>	Yes

7. Click **OK**.

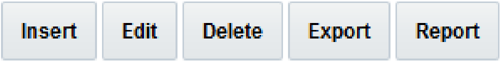
Procedure 19. Configure Second DSR NOAM Server

3. ☐ **NOAM GUI**: Export the initial configuration

1. Navigate to **Configuration > Servers**.


Main Menu
Administration
Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. From the GUI screen, select the second NOAM server and click **Export** to generate the initial configuration data for that server.


Insert
Edit
Delete
Export
Report

4. ☐ **1st NOAM VIP GUI**: Copy the configuration file to the 2nd NOAM server

1. Obtain a terminal session to the first NOAM server console and login as **admusr**.
2. Configure the second NOAM server.

```
$ sudo scp -r
/var/TKLC/db/filemgmt/TKLCConfigData.<NOAM2_Hostname>
.sh
admusr@<NOAM2_xmi_IP_address>:/var/tmp/TKLCConfigData
.sh
```

The automatic configuration daemon looks for the **TKLCConfigData.sh** file in the **/var/tmp** directory, implements the configuration in the file, and asks the user to reboot the server.

5. ☐ **2nd DR NOAM Server**: Verify server configuration was called and reboot the configured server

1. Verify server configuration was called by checking the log file.

```
$ sudo cat /var/TKLC/appw/logs/Process/install.log
```

Verify this message displays:

```
[SUCCESS] script completed successfully!
```

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.

2. Reboot the server.

```
$ sudo init 6
```

3. Proceed to the next step once the server finishes rebooting. The server is done rebooting once the login prompt displays.

Procedure 19. Configure Second DSR NOAM Server

6. ☐	**2nd NOAM Server**: Verify server health	Login as **admusr** to the second NOAM server and make sure no errors are returned.

```
$ 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
```

Procedure 20. Complete DSR NOAM Server Group Configuration

This procedure finishes configuration for the DSR NOAM server group.

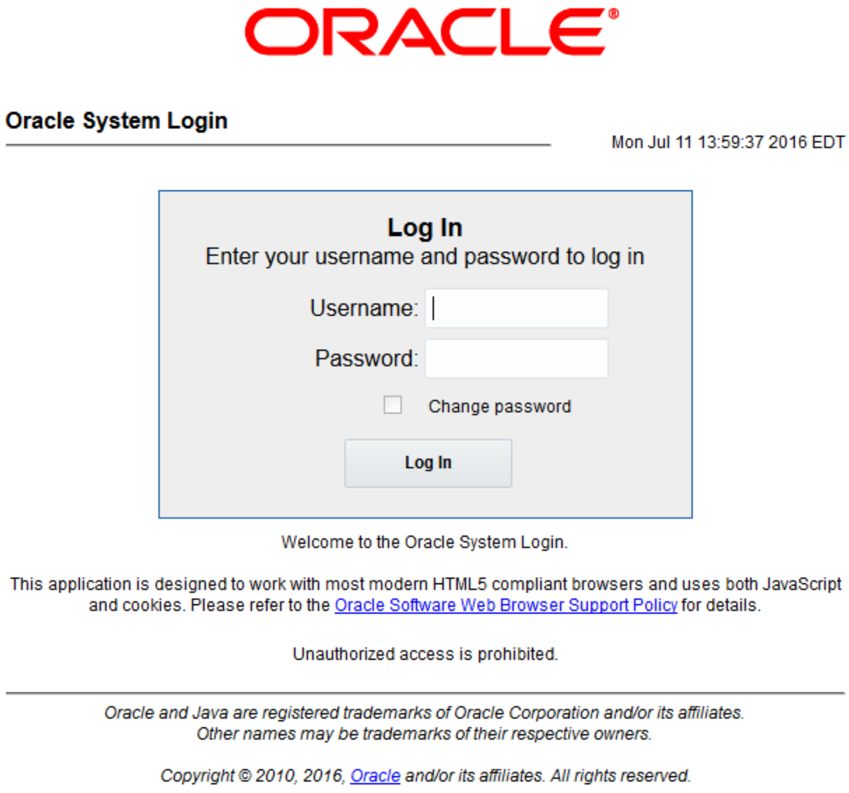
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.

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

1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:

```
https://<Primary_NOAM_XMI_VIP_IP_Address>
```

2. Login as the **guiadmin** user.



Oracle System Login

Mon Jul 11 13:59:37 2016 EDT

Enter your username and password to log in

Welcome to the Oracle System Login.

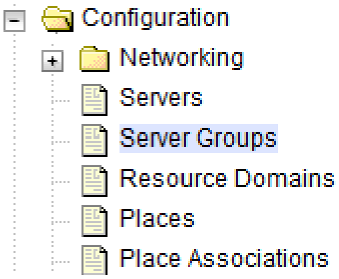
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

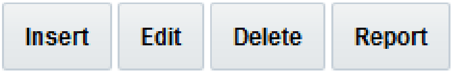
Unauthorized access is prohibited.

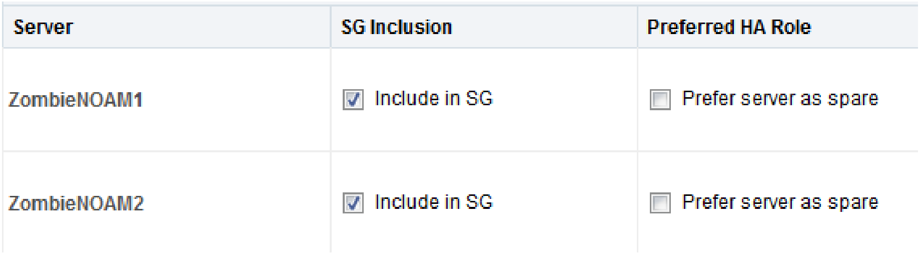
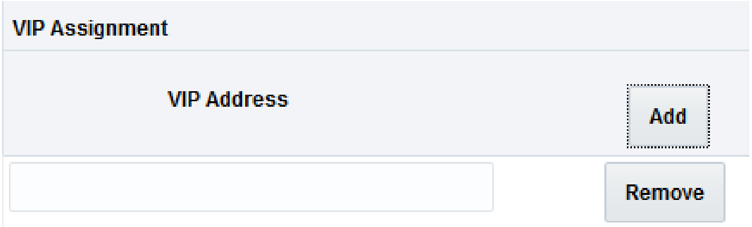
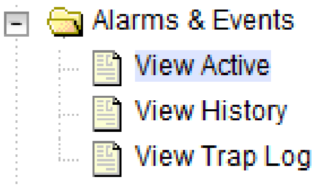
Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

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

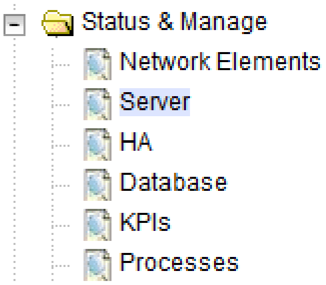
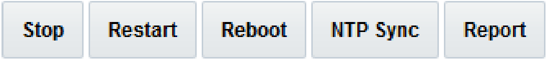
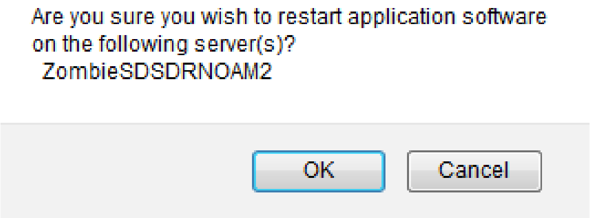
Procedure 20. Complete DSR NOAM Server Group Configuration

<table>
<tr>
<td>2.
☐</td>
<td>**NOAM GUI**: Edit the NOAM server group and VIP</td>
<td>
1. Navigate to **Configuration > Server Groups**.

Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Select the server group you just created and click **Edit**.

Insert
Edit
Delete
Report

3. Add the second SDS NOAM server to the server group by marking the **Include in SG** checkbox for the second SDS NOAM server.
Do **not** mark any of the **Preferred Spare** checkboxes.

<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<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>
</table>
4. Click **Apply**.
5. Click **Add**.
6. Type the **VIP Address** and click **OK**.

VIP Assignment
VIP Address
Add
Remove
</td>
</tr>
<tr>
<td>3.
☐</td>
<td>**NOAM VIP GUI**: Wait for remote database alarm to clear</td>
<td>
Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding.
Monitor progress by navigating to **Alarms & Events > View Active**.

Alarms & Events
View Active
View History
View Trap Log
</td>
</tr>
</table>

Procedure 20. Complete DSR NOAM Server Group Configuration

4. ☐	**SDS NOAM VIP GUI**: Restart the 2nd NOAM server	1. From the NOAM GUI, navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the second NOAM server and click **Restart**.  3. Click **OK** to confirm. Are you sure you wish to restart application software on the following server(s)? ZombieSDSDRNOAM2

3.14.2 NetBackup Client Installation (Optional)

Procedure 21. Install NetBackup Client (Optional)

<table>
<tr><td colspan="3">This procedure downloads and installs the 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 ach step number.
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>Install NetBackup Client Software</td><td>If a customer has a way of transferring and installing the NetBackup client without using TPD tools (push configuration), then use Appendix I.2 Install NetBackup Client Using NBAutoInstall.
<i>Note:</i> This is not common. If the answer to the previous question is not known, then use Appendix I.1 Install NetBackup Client Using platcfg.</td></tr>
<tr><td>2.
☐</td><td>Install NetBackup Client Software</td><td>Choose the same method used in step 1. to install NetBackup on the 2nd NOAM.</td></tr>
</table>

3.14.3 Disaster Recovery NOAM (Optional)

Procedure 22. Configure DSR NOAM for DR Site (Optional)

This procedure configures the first DR NOAM server.

Prerequisites:

- TVOE is configured (section 3.2)
- Site OMAC is installed and deployed (sections 3.3, 3.4, and 3.6)
- Additional rack mount servers are installed and configured (sections 3.7, 3.8, and 3.9)
- VM have been placed and deployed; and network has been configured (sections 3.10, 3.12, and 3.13)

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

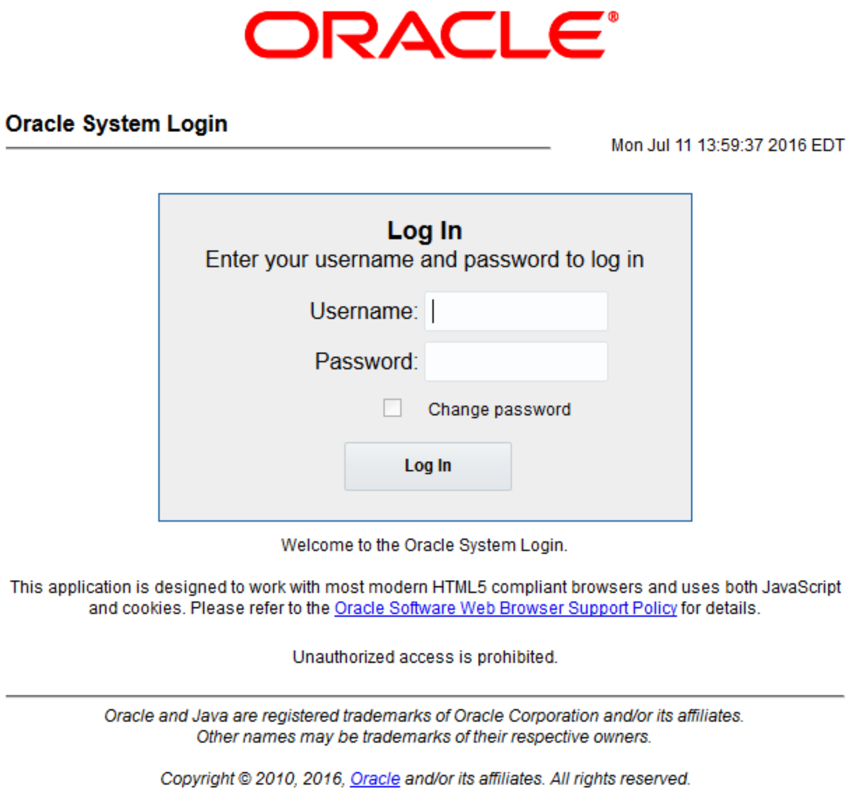
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐ **NOAM VIP GUI**: Login

1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:

```
https://<Primary_NOAM_XMI_VIP_IP_Address>
```

2. Login as the **guiadmin** user.



Enter your username and password to 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.

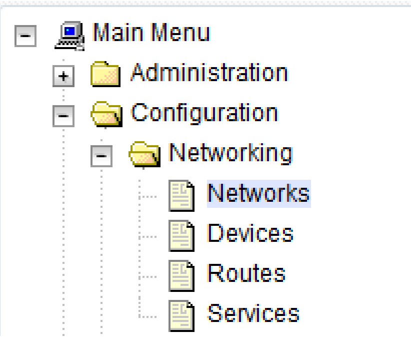
Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.

Procedure 22. Configure DSR NOAM for DR Site (Optional)

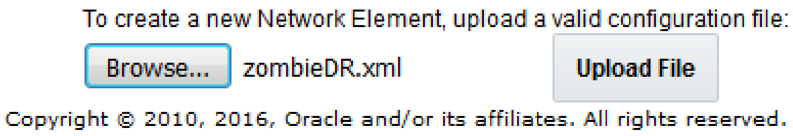
<table>
<tr>
<td>2.
☐</td>
<td>Primary NOAM VIP GUI: Create the DR NOAM network element using an XML file</td>
<td>

Note: The NOAM network element file that describes the networking of the target install environment of the NOAM server should already be created. Refer Procedure 17, step 1. to create the xml file, if necessary.

1. Navigate to **Configuration > Networking > Networks**.


Main Menu
Administration
Configuration
Networking
Networks
Devices
Routes
Services

2. Click **Browse** and enter the **Pathname** of the SOAM network XML file.
3. Click **Upload File**.



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

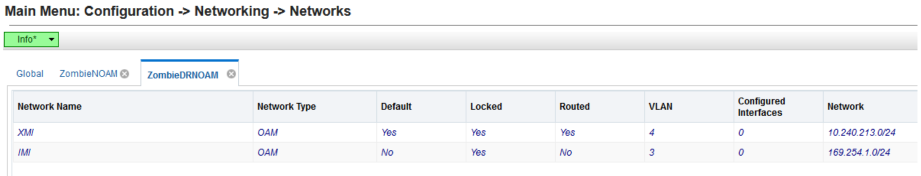
Browse...

zombieDR.xml

Upload File

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

4. Click on the tab to display the configured network.



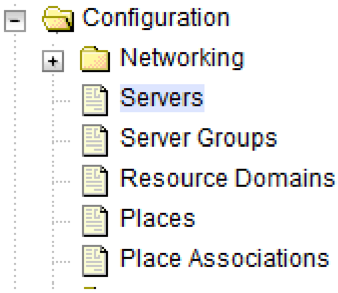
Main Menu: Configuration -> Networking -> Networks

Info*
Global
ZombieNOAM
ZombieDRNOAM

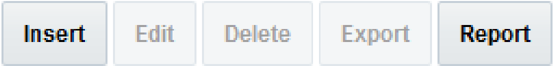
<table>
<tr><th>Network Name</th><th>Network Type</th><th>Default</th><th>Locked</th><th>Routed</th><th>VLAN</th><th>Configured Interfaces</th><th>Network</th></tr>
<tr><td>XMI</td><td>OAM</td><td>Yes</td><td>Yes</td><td>Yes</td><td>4</td><td>0</td><td>10.240.213.0/24</td></tr>
<tr><td>IMI</td><td>OAM</td><td>No</td><td>Yes</td><td>No</td><td>3</td><td>0</td><td>169.254.1.0/24</td></tr>
</table>

</td>
</tr>
<tr>
<td>3.
☐</td>
<td>Primary NOAM VIP GUI: Insert the 1st DR NOAM server</td>
<td>

1. Navigate to **Configuration > Servers**.


Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Click **Insert** to insert the new SDS NOAM server into the servers table.

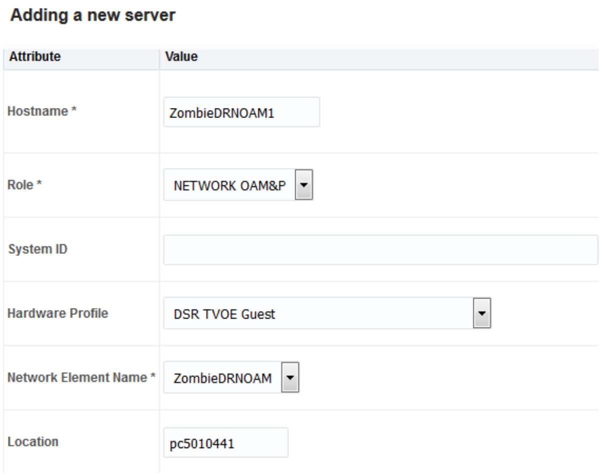
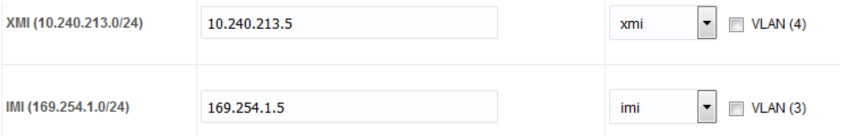
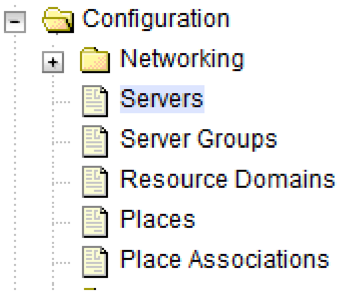

Insert
Edit
Delete
Export
Report

3. Enter these values:

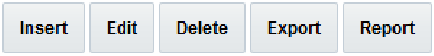
Hostname: <Hostname>
Role: Network OAM

</td>
</tr>
</table>

Procedure 22. Configure DSR NOAM for DR Site (Optional)

<table>
<tr>
<td></td>
<td></td>
<td>**System ID**: <Site System ID>
Hardware Profile: DSR TVOE Guest
Network Element Name: [Select NE]
Location: <Enter an optional location description>

Adding a new server
Attribute Value
Hostname *: ZombieDRNOAM1
Role *: NETWORK OAM&P
System ID:
Hardware Profile: DSR TVOE Guest
Network Element Name *: ZombieDRNOAM
Location: pc5010441
4. For the **XMI** network, type the server XMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.
5. For the **IMI** network, type the server IMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.

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)
6. Add this NTP server.
NTP Server Preferred?
<First-DR-NOAM-TVOE-IP-Address> Yes
7. Click **OK**.</td>
</tr>
<tr>
<td>4.
☐</td>
<td>**Primary NOAM VIP GUI**: Export the initial configuration</td>
<td>1. Navigate to **Configuration > Servers**.


Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. From the GUI screen, select the DR NOAM server and click **Export** to generate the initial configuration data for that server.


Insert
Edit
Delete
Export
Report

</td>
</tr>
</table>

Procedure 22. Configure DSR NOAM for DR Site (Optional)

5. ☐ **1st NOAM Server**: Copy configuration file to DR NOAM NOAM server

1. Obtain a terminal session to the primary NOAM server console and login as **admusr**.
2. Execute the following command to configure the DR NOAM server.

```
$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<DR-
NOAM_Hostname>.sh admusr@<DR-
NOAM_xmi_IP_address>:/var/tmp/TKLCConfigData.sh
```

The automatic configuration daemon looks for the **TKLCConfigData.sh** file in the **/var/tmp** directory, implements the configuration in the file, and asks the user to reboot the server.

6. ☐ **1st DR NOAM Server**: Verify server configuration was called and reboot the configured server

1. Verify server configuration was called by checking the log file.

```
$ sudo cat /var/TKLC/appw/logs/Process/install.log
```

Verify this message displays:

```
[SUCCESS] script completed successfully!
```

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.

2. Reboot the server.

```
$ sudo init 6
```

3. Proceed to the next step once the server finishes rebooting. The server is done rebooting once the login prompt displays.

7. ☐ **1st DR NOAM Server**: Verify server health

Login as **admusr** to the first DR NOAM server and make sure that no errors are returned.

```
$ 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
```

8. ☐ Repeat for 2nd DR NOAM server

Repeat steps 2. through 7. to configure second DR NOAM server. When inserting the second DR NOAM server, change the NTP server address to the following:

NTP Server	Preferred?
<2nd DR NOAM-RMS-TVOE-IP-Address>	Yes

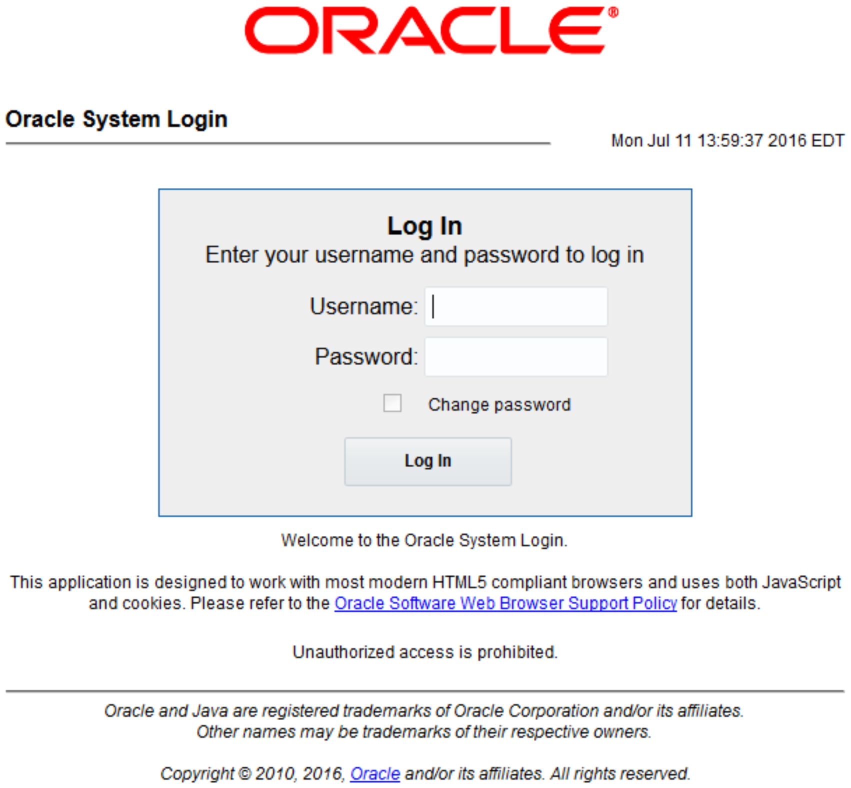
Procedure 23. Pairing for DSR DR NOAM Site (Optional)

This procedure pairs the DSR DR NOAM site.

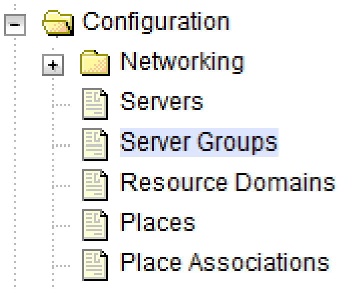
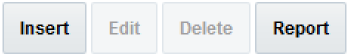
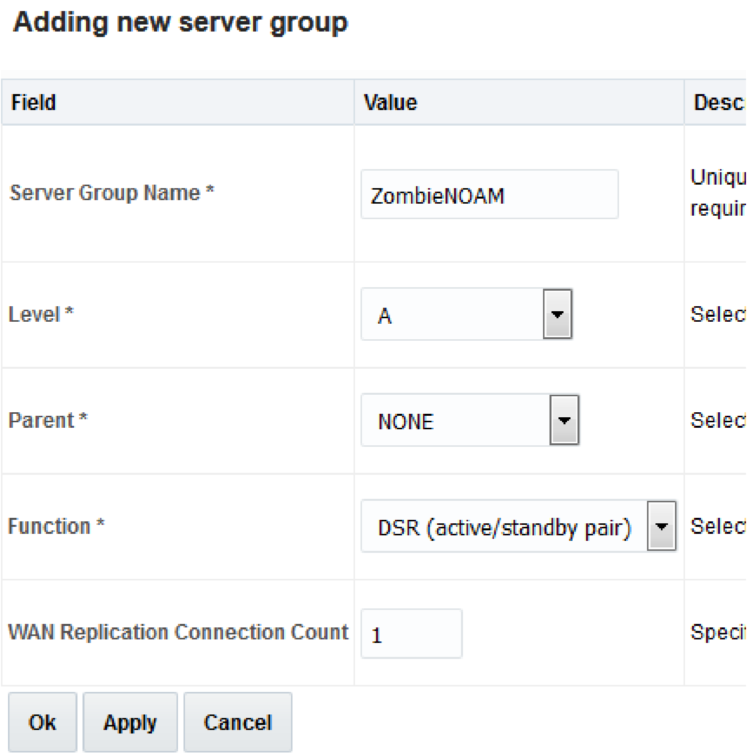
Prerequisite: The DSR DR NOAM site has been installed.

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

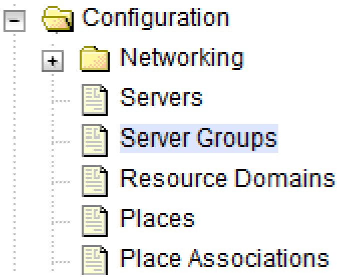
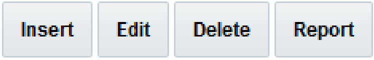
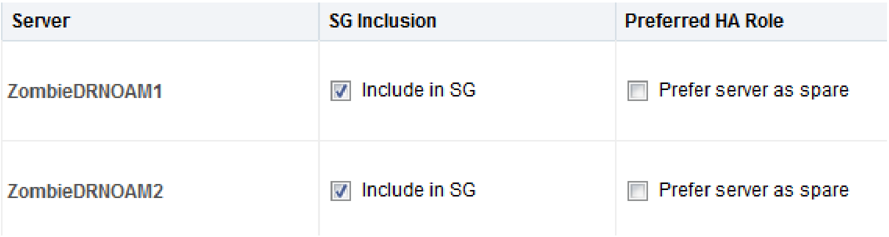
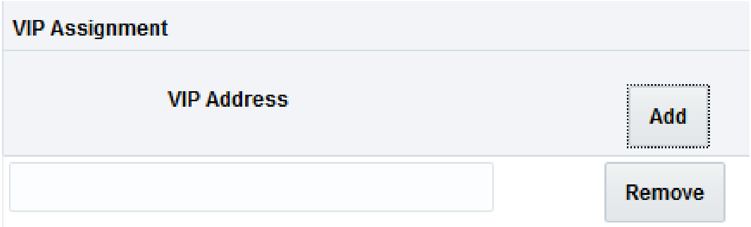
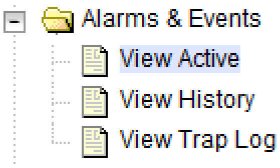
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_XMI_VIP_IP_Address>` 2. Login as the **guiadmin** user.  ORACLE Oracle System Login Log In Username: Password: ☐ Change password Log In Mon Jul 11 13:59:37 2016 EDT Enter your username and password to 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.*

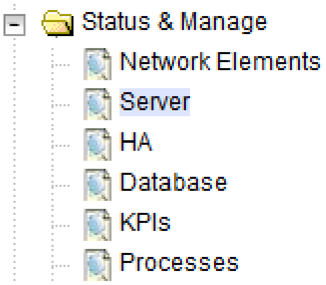
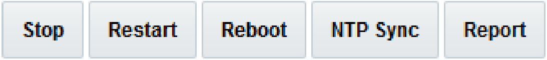
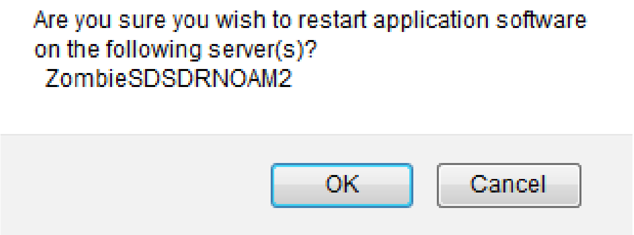
Procedure 23. Pairing for DSR DR NOAM Site (Optional)

2. ☐	**NOAM GUI**: Enter DR NOAM server group data	1. Navigate to **Configuration > Server Groups**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Click **Insert**.  Insert Edit Delete Report 3. Enter these values: **Server Group Name**: <Server Group Name> **Level**: A **Parent**: None **Function**: DSR (Active/Standby Pair) **WAN Replication Connection Count**: Use Default Value  Adding new server group 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 Ok Apply Cancel 4. Click **OK**.

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

3. ☐	**Primary NOAM GUI**: Edit the NOAM server group and VIP	1. Navigate to **Configuration > Server Groups**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Select the server group you just created and click **Edit**.  Insert Edit Delete Report 3. Add the second SDS NOAM server to the server group by marking the **Include in SG** checkbox for the second SDS NOAM server. Do **not** mark any of the **Preferred Spare** checkboxes.  Server / SG Inclusion / Preferred HA Role ZombieDRNOAM1 ☑ Include in SG ☐ Prefer server as spare ZombieDRNOAM2 ☑ Include in SG ☐ Prefer server as spare 4. Click **Apply**. 5. Click **Add**. 6. Type the **VIP Address** and click **OK**.  VIP Assignment VIP Address Add Remove
4. ☐	**Primary NOAM VIP GUI**: Wait for remote database alarm to clear	Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding. Monitor progress by navigating to **Alarms & Events > View Active**.  Alarms & Events View Active View History View Trap Log

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

5. ☐	**Primary NOAM VIP GUI**: Restart the DR NOAM servers	1. From the NOAM GUI, navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the first DR NOAM server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm.  Are you sure you wish to restart application software on the following server(s)? ZombieSDSDRNOAM2 4. Repeat this step selecting the second DR NOAM server.
6. ☐	**Primary NOAM**: Modify DSR OAM process	1. Establish an SSH session to the primary NOAM, login as **admusr**. 2. Retrieve the cluster ID of the DR NOAM. 3. Start the DSR OAM process on the DR NOAM.

6.

2. Retrieve the cluster ID of the DR NOAM.

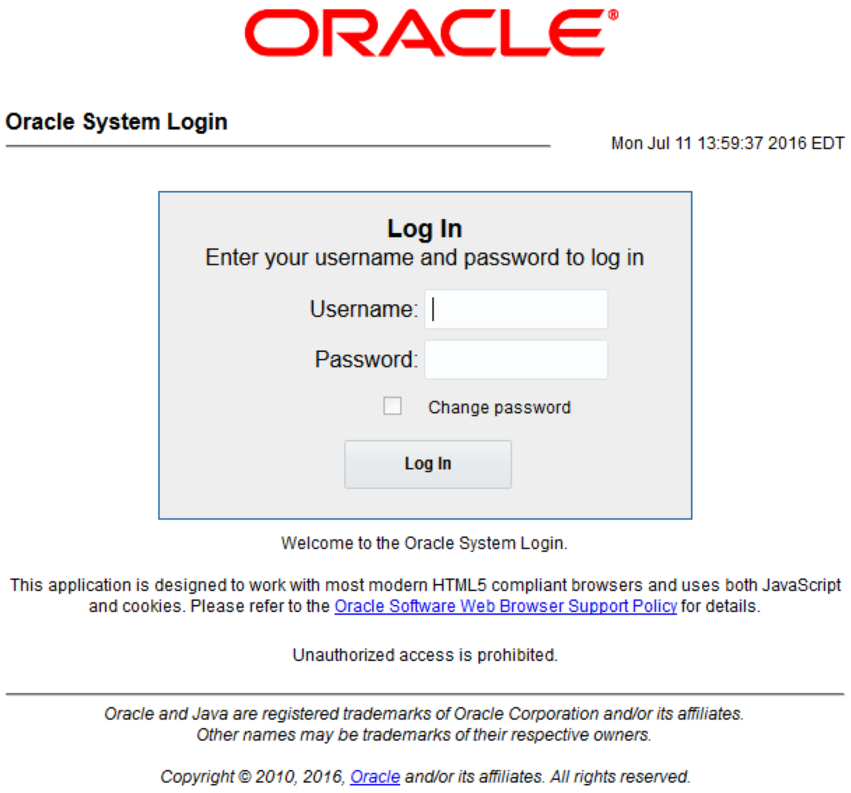
```
$ sudo iqt -fClusterID TopologyMapping where
"NodeID='<DR_NOAM_Host_Name>'"
  Server_ID           NodeID ClusterID
          1 Oahu-DSR-DR-NOAM-2      A1055
```

3. Start the DSR OAM process on the DR NOAM.

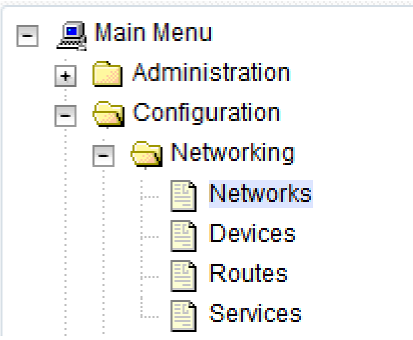
```
$ echo "<clusterID>|DSROAM_Proc|Yes" | iload -ha -xun -
fcluster -fresource -foptional HaClusterResourceCfg
```

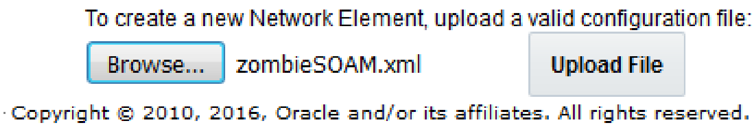
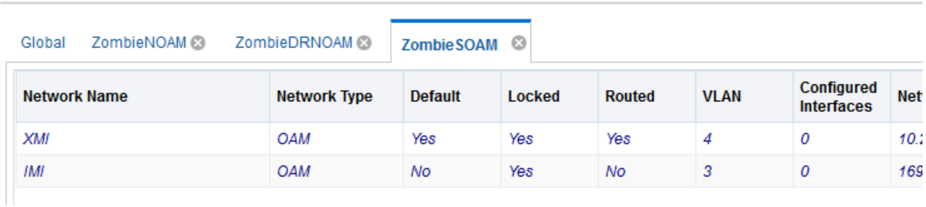
3.14.4 SOAM Configuration

Procedure 24. Configure DSR SOAM NE

This procedure configures the first DSR SOAM network element. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Primary NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of: `https://<NOAM_XMI_VIP_IP_Address>` 2. Login as the **guiadmin** user.  **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.* *Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

Procedure 24. Configure DSR SOAM NE

<table>
<tr>
<td>2.
☐</td>
<td>NOAM SDS VIP GUI: Create the SOAM network element using an XML file</td>
<td>
<i>Note:</i> The SOAM network element file that describes the networking of the target install environment of the SOAM server should already be created. Refer Procedure 17, step 1. to create the xml file, if necessary.
1. Navigate to Configuration > Networking > Networks.

Main Menu
Administration
Configuration
Networking
Networks
Devices
Routes
Services

2. Click Browse and enter the Pathname of the SOAM network XML file.
3. Click Upload File.

To create a new Network Element, upload a valid configuration file:
Browse...
zombieSOAM.xml
Upload File
Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.
4. Click on the tab to display the configured network.

Global
ZombieNOAM
ZombieDRNOAM
ZombieSOAM
<table>
<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>Net</th></tr>
<tr><td>XMI</td><td>OAM</td><td>Yes</td><td>Yes</td><td>Yes</td><td>4</td><td>0</td><td>10.</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</td></tr>
</table>
</td>
</tr>
</table>

Procedure 25. Configure DSR SOAM Server

This procedure configures the DSR SOAM server.

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

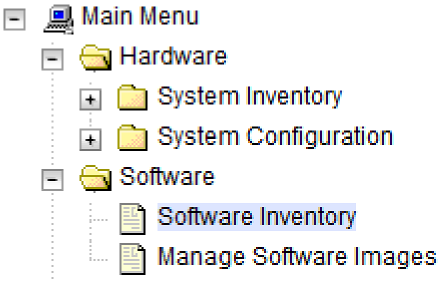
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1.
☐

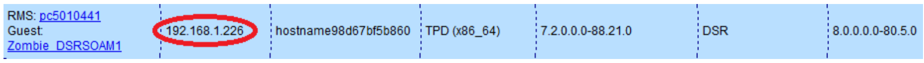
PMAC: Exchange SSH keys between the SOAM site's local PMAC and the SOAM server

Use the PMAC GUI to determine the control network IP address of the blade server that is to be the SOAM server.

1. From the PMAC GUI, navigate to **Software** > **Software Inventory**.



2. Note the **IP address** for the SOAM server.



RMS: pc5010441 Guest: Zombie_DSRSOAM1	192.168.1.226	hostname98d67bf5b860	TPD (x86_64)	7.2.0.0.0-88.21.0	DSR	8.0.0.0.0-80.5.0

3. Obtain a terminal session to PMAC and login as **admusr**.
4. Exchange SSH keys for admusr between the PMAC and the SOAM server using the keyexchange utility and the control network IP address for the SOAM server.

```
$ keyexchange admusr@<SO1_Control_IP Address>
```

5. Enter the password for the admusr user of the NOAM server.

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 skip this step.

1. Obtain a terminal session to the NOAM VIP and login as **admusr**.
2. Exchange SSH keys for admusr between the PMAC and NOAM for this SOAM site using the keyexchange utility.

```
$ keyexchange admusr@<SO1_Site_PMAC_Mgmt_IP_Address>
```

3. Enter the password for the admusr user of the PMAC server.
4. Repeat this step for the standby SOAM server.

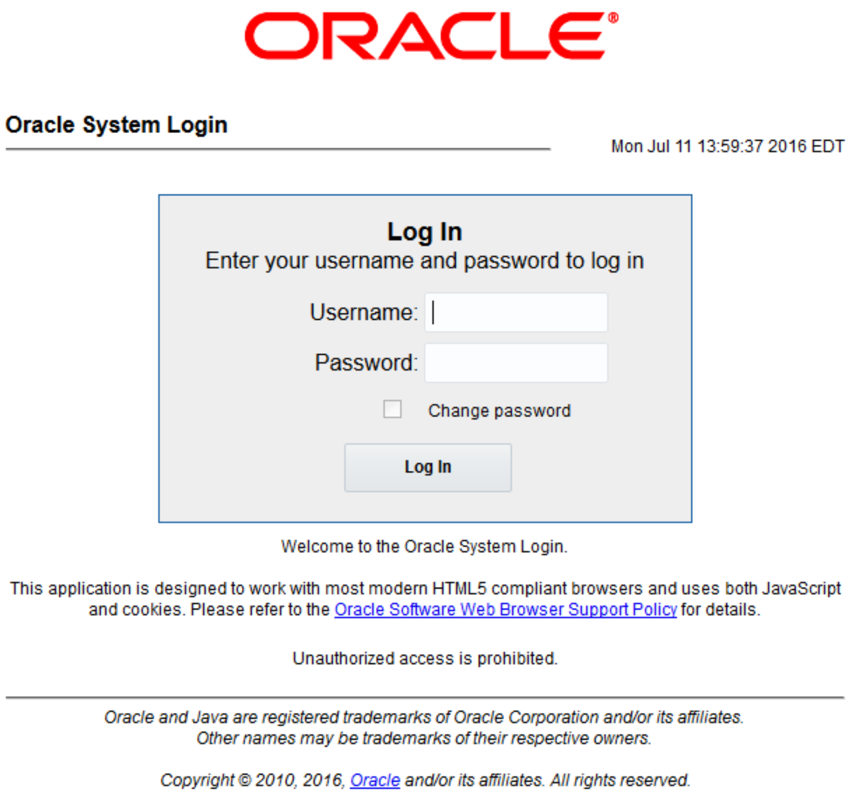
Procedure 25. Configure DSR SOAM Server

<table>
<tr>
<td>3.
☐</td>
<td>Primary NOAM VIP GUI: Login</td>
<td>

1. Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of:

```
https://<NOAM_XMI_VIP_IP_Address>
```

2. Login as the **guiadmin** user.



Oracle System Login

Mon Jul 11 13:59:37 2016 EDT

Log In

Enter your username and password to log in

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.

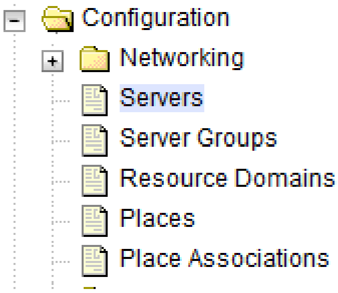
</td>
</tr>
</table>

Procedure 25. Configure DSR SOAM Server

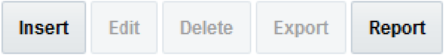
4. ☐

SOAM VIP GUI: Insert the 1st SOAM server

1. Navigate to **Configuration > Servers**.

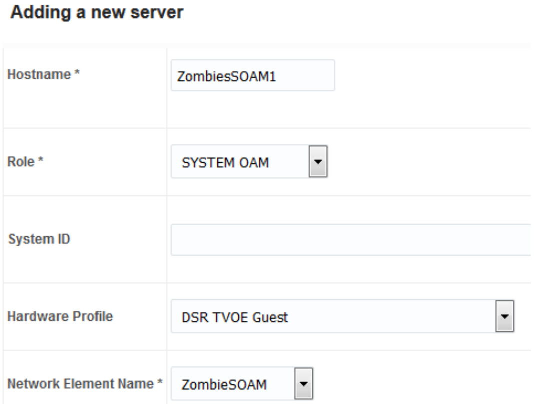

Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Click **Insert** to insert the first first SOAM server into the servers table.


Insert
Edit
Delete
Export
Report

3. Enter these values:

Hostname:	<Hostname>
Role:	System OAM
System ID:	<Site System ID>
Hardware Profile:	DSR TVOE Guest
Network Element Name:	[Select NE]
Location:	<Enter an optional location description>

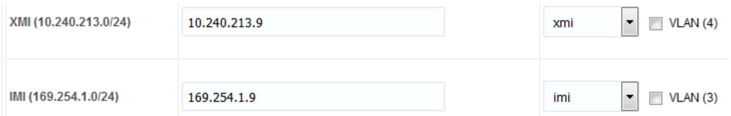


Adding a new server

Hostname *	ZombiesSOAM1
Role *	SYSTEM OAM
System ID	
Hardware Profile	DSR TVOE Guest
Network Element Name *	ZombieSOAM

4. For the **XMI** network, type the server's XMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.

5. For the **IMI** network, type the server's IMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.



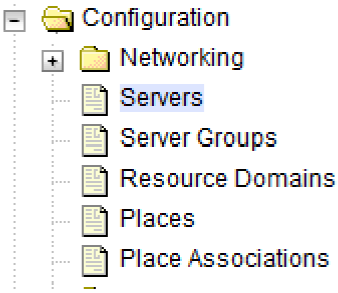
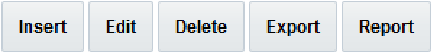
XMI (10.240.213.0/24)	10.240.213.9	xmi	☐ VLAN (4)
IMI (169.254.1.0/24)	169.254.1.9	imi	☐ VLAN (3)

6. Add this NTP server.

NTP Server	Preferred?
<First-SOAM-TVOE-IP-Address>	Yes

7. Click **OK**.

Procedure 25. Configure DSR SOAM Server

5. ☐	**NOAM VIP GUI**: Export the initial configuration	1. Navigate to **Configuration > Servers**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. From the GUI screen, select the SOAM server and click **Export** to generate the initial configuration data for that server.  Insert Edit Delete Export Report
6. ☐	**NOAM VIP GUI**: Copy configuration file to 1st SDS DP SOAM server	1. Obtain a terminal session to the NOAM VIP as the **admusr** user. 2. Use the **awpushcf**g utility to copy the configuration file, created in the previous step from the **/var/TKLC/db/filemgmt** directory on NOAM to the first SOAM server, using the control network IP address for the first SOAM server. The configuration file has a filename like **TKLCConfigData.<hostname>.sh**. `$ sudo awpushcfg` The awpushcfg utility is interactive, so the user is asked 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 first SOAM server. • **Hostname of the target server**: Enter the server name configured in step 4.

Procedure 25. Configure DSR SOAM Server

7. ☐ **1st SOAM Server**: Verify awpushcfg was called and reboot the configured server

1. Obtain a terminal session to the first SOAM server console by establishing an ssh session from the site PMAC terminal console.

```
$ ssh admusr@<SO1_Control_IP>
```

2. Login as **admusr**.

   The automatic configuration daemon looks for the **TKLCConfigData.sh** file in the **/var/tmp** directory, implements the configuration in the file, and asks the user to reboot the server.

3. Verify awpushcfg was called by checking the log file.

```
$ sudo cat /var/TKLC/appw/logs/Process/install.log
```

   Verify this message displays:

```
[SUCCESS] script completed successfully!
```

   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.

4. Reboot the server.

```
$ sudo init 6
```

5. Proceed to the next step once the server finishes rebooting. The server is done rebooting once the login prompt displays.

8. ☐ **1st SOAM Server**: Login

Obtain a terminal session to the first SOAM server console by establishing an ssh session from the site PMAC terminal console.

```
$ ssh admusr@<SO1_Control_IP>
```

9. ☐ **1st SOAM Server**: Verify server health

Login as **admusr** to the first SOAM server and make sure no errors are returned.

```
$ 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
```

10. ☐ Insert and configure the 2nd SOAM server

Repeat this procedure to insert and configure the second SOAM server with the exception of the NTP server, which should be configured as:

NTP Server	Preferred?
<Guest-TVOE-Host-IP-Address>	Yes

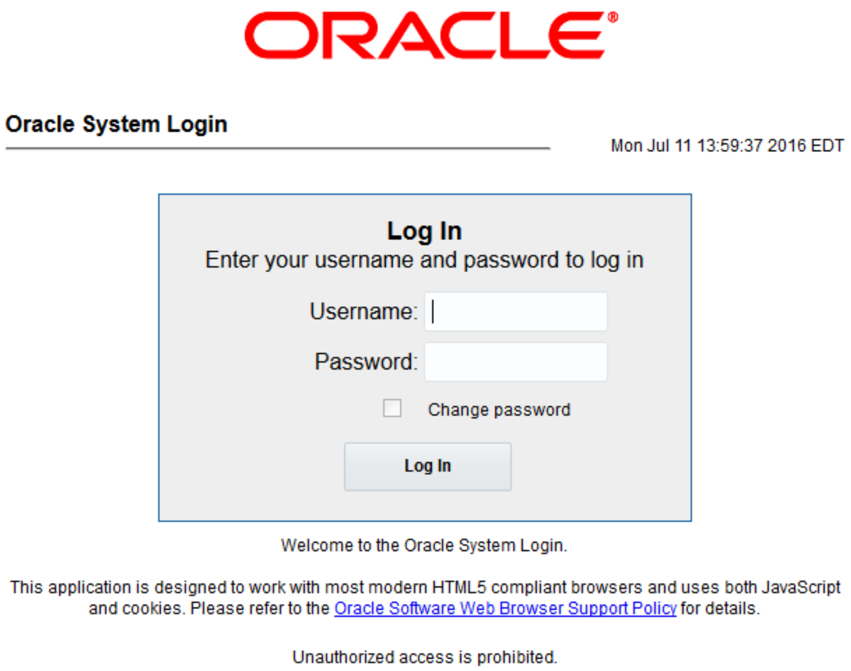
Instead of data for the first SOAM server, insert the network data for the second SOAM server, transfer the **TKLCConfigData** file to the second SOAM server and reboot the second SOAM server when prompted at a terminal window.

Procedure 25. Configure DSR SOAM Server

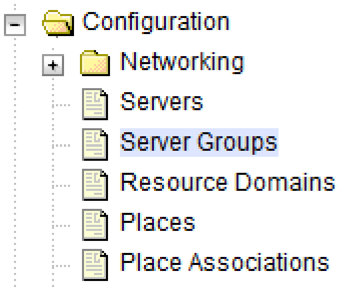
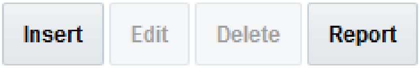
<table>
<tr><td>11.
☐</td><td>Insert and configure the spare SOAM server</td><td>Repeat this procedure to insert and configure the spare SOAM server with the exception of the NTP server, which should be configured as:
<table>
<tr><th>NTP Server</th><th>Preferred?</th></tr>
<tr><td><Guest-TVOE-Host-IP-Address></td><td>Yes</td></tr>
</table>
<i>Note:</i> 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 first SOAM server, insert the network data for the spare SOAM server, transfer the TKLCConfigData file to the spare SOAM server and reboot the spare SOAM server when prompted at a terminal window.</td></tr>
<tr><td>12.
☐</td><td>Install NetBackup client software on SOAMs (optional)</td><td>If you are using NetBackup at this site, then execute Appendix I Install NetBackup Client again to install the NetBackup client on all SOAM servers.</td></tr>
</table>

Procedure 26. Configure the DSR SOAM Server Group

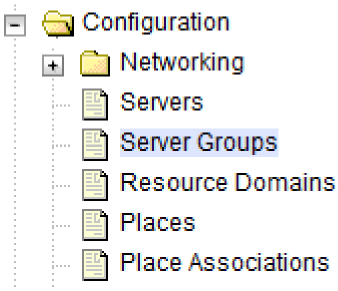
<table>
<tr><td colspan="3">This procedure configures the DSR SOAM server group.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>Primary NOAM VIP GUI: Login</td><td>1. 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>https://<NOAM_XMI_VIP_IP_Address></code>
2. Login as the guiadmin user.

Oracle System Login
Mon Jul 11 13:59:37 2016 EDT
Log In
Enter your username and password to log in
Username:
Password:
☐ Change password
Log In
Welcome to the Oracle System Login.
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.
Unauthorized access is prohibited.</td></tr>
</table>

Procedure 26. Configure the DSR SOAM Server Group

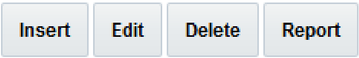
2. ☐	**NOAM VIP GUI**: Enter SDS DP SOAM server group data	1. Navigate to **Configuration > Server Groups**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Click **Insert**.  Insert Edit Delete Report 3. Enter these values: **Server Group Name**: <Server Group Name> **Level**: B **Parent**: Select the NOAM Server Group **Function**: DSR (Active/Standy Pair) **WAN Replication Connection Count**: Use default value 4. Click **OK**. 5. For DSR mated sites, repeat this step for additional SOAM server groups where the preferred SOAM spares may be entered before the active/standby SOAMs.

Procedure 26. Configure the DSR SOAM Server Group

<table>
<tr>
<td>3.
☐</td>
<td>**NOAM VIP GUI**: Edit the SDS DP SOAM server groups and VIP</td>
<td>
1. Navigate to **Configuration > Server Groups**.

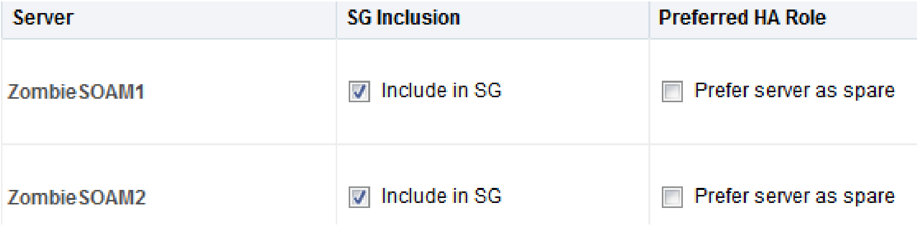

Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Select the server group you just created and click **Edit**.


Insert
Edit
Delete
Report

3. Add both SOAM servers to the server group primary site by marking the **Include in SG** checkbox for each SDS DP server.

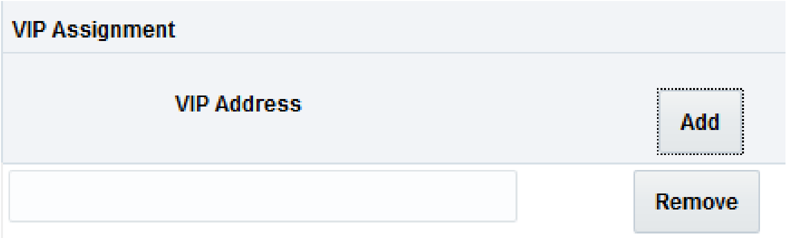
Do **not** mark any of the **Preferred Spare** checkboxes.


<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<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>
</table>

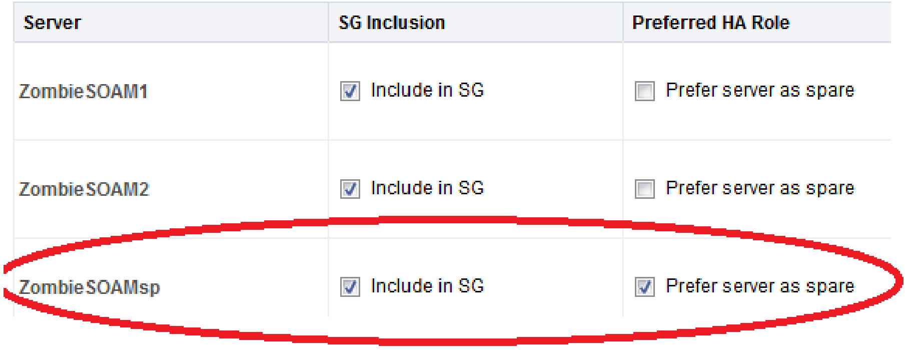
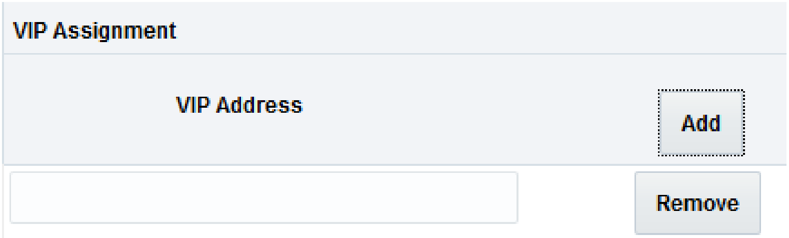
4. Click **Apply**.

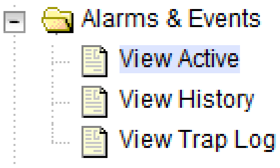
5. Click **Add**.

6. Type the **VIP Address** and click **OK**.


VIP Assignment
VIP Address
Add
Remove
</td>
</tr>
</table>

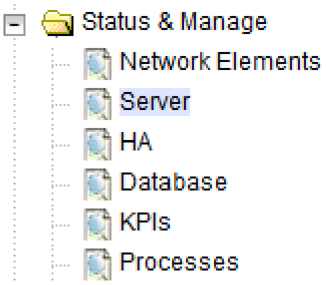
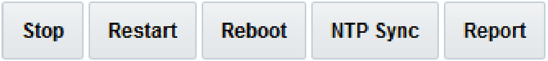
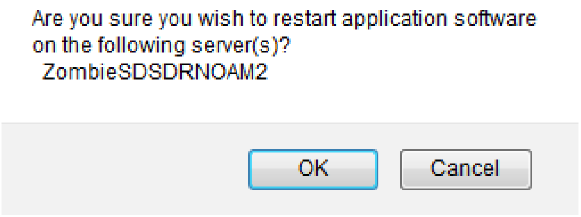
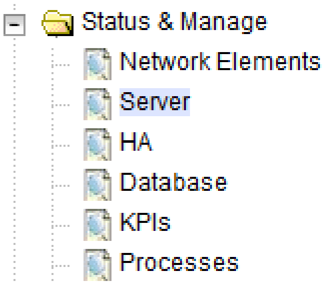
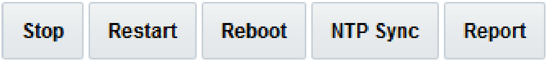
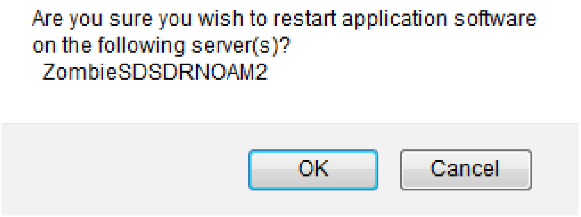
Procedure 26. Configure the DSR SOAM Server Group

<table>
<tr>
<td>4.
☐</td>
<td>NOAM VIP GUI: Edit the SOAM server group and add preferred spares for site redundancy (optional)</td>
<td>
<p>If the Two Site Redundancy feature for the SOAM server group is wanted, add a SOAM server that is located in its server group secondary site by marking the Include in SG checkbox. Also, mark the Preferred Spare checkbox.</p>

<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<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>
</table>
<p>If the Three Site Redundancy feature for the SOAM server group is wanted, add an additional SOAM server that is located in its server group tertiary site by marking the Include in SG checkbox. Also, mark the Preferred Spare checkbox.</p>
<p><i>Note:</i> The preferred spare servers must be server group secondary and tertiary sites. There should be servers from three separate sites (locations).</p>
<p>For more information about server group secondary site, tertiary site, or site redundancy, see section 1.3 Terminology.</p>
</td>
</tr>
<tr>
<td>5.
☐</td>
<td>NOAM VIP GUI: Edit the SOAM server group and add additional SOAM VIPs (optional)</td>
<td>
<p>1. To add additional SOAM VIPs, click Add.</p>
<p>2. Type the VIP Address.</p>
<p>3. Click OK.</p>
<p><i>Note:</i> Additional SOAM VIPs only apply to SOAM server groups with preferred spare SOAMs.</p>


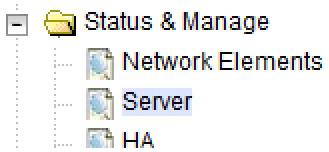
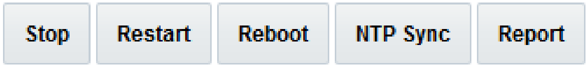
</td>
</tr>
<tr>
<td>6.
☐</td>
<td>NOAM VIP GUI: Wait for remote database alarm to clear</td>
<td>
<p>Wait for the Remote Database re-initialization in progress alarm to clear before proceeding.</p>
<p>Monitor progress by navigating to Alarms & Events > View Active.</p>


</td>
</tr>
</table>

Procedure 26. Configure the DSR SOAM Server Group

7. ☐	**NOAM VIP GUI**: Restart the 1st SOAM server	1. From the NOAM GUI, navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the first SOAM server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm.  Are you sure you wish to restart application software on the following server(s)? ZombieSDSDRNOAM2
8. ☐	**NOAM VIP GUI**: Restart the 2nd NOAM server	1. From the NOAM GUI, navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the second SOAM server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm.  Are you sure you wish to restart application software on the following server(s)? ZombieSDSDRNOAM2

Procedure 26. Configure the DSR SOAM Server Group

9. ☐	**NOAM VIP GUI**: Restart all preferred spare SOAM servers	If additional preferred spare servers are not configured for Secondary or Tertiary Sites, skip this step. 1. If additional preferred spare servers are configured for Secondary and/or Tertiary Sites, navigate to **Status & Manage > Server**.  2. Select all **Preferred Spare** SOAM servers. 3. Click **Restart**.  4. Click **OK** to confirm.

Procedure 27. Configure RMS-Specific B-Level Resources (HP DL380 Gen 8 Servers Only)

This procedure configures RMS-specific B-level resources. ***Note:*** **Oracle X5-2/NETRA X5-2/X6-2/HP DL380 GEN 9**: Skip this procedure. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Active SOAM**: Login	Obtain a terminal session to the active SOAM server and login as **admusr**.
2. ☐	**Active SOAM**: Execute B-level resource script	`$ sudo /usr/TKLC/dsr/bin/rmsResourceConfig.sh` 1. Wait until the script completes and you are returned to the command line. 2. Verify no errors display. If any errors displayed, stop this procedure and contact My Oracle Support (MOS).

3.14.5 Activate PCA

Procedure 28. Activate PCA

This procedure activates PCA. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Activate PCA feature (PCA only)	If you are installing PCA, execute applicable procedures (Added SOAM site activation or complete system activation) in [12] DSR PCA Activation Guide to activate PCA. ***Notes***: • If not all SOAM sites are ready at this point, then you should repeat activation for each **new** SOAM site that comes online. • Ignore steps to restart SBRs that have yet to be configured.

3.14.6 Activate DCA

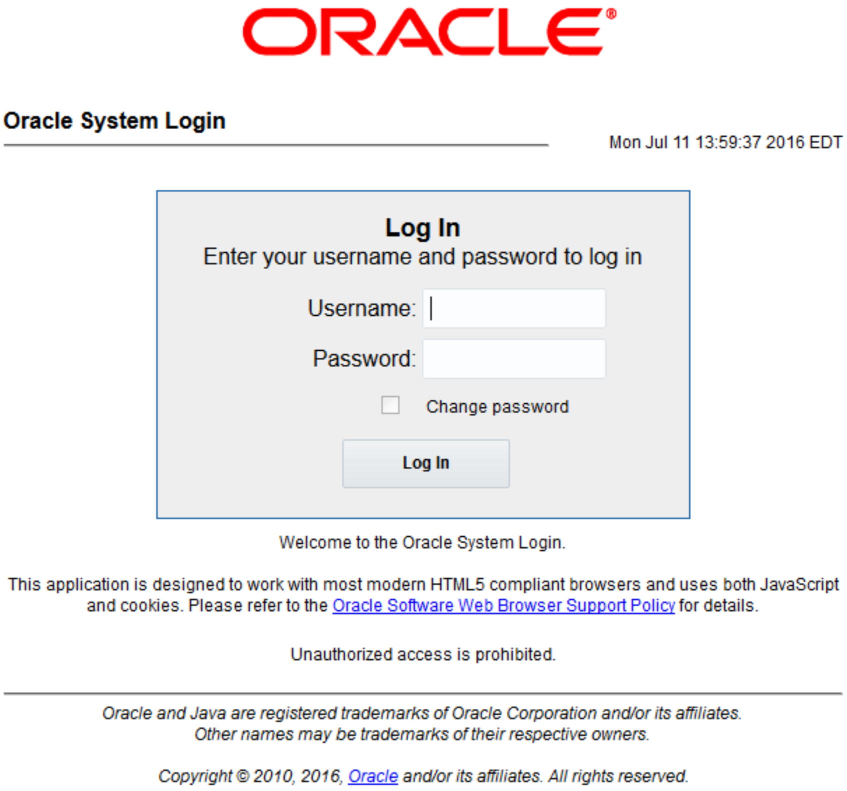
Procedure 29. Activate DCA

This procedure activates DCA. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Activate DCA feature (DCA only)	If you are installing DCA, execute procedures in [20] DCA Framework and Application Activation and Deactivation Guide to activate the DCA framework and feature. ***Notes***: • If not all SOAM sites are ready at this point, then you should repeat activation for each **new** SOAM site that comes online. • Ignore steps to restart DA-MPs and SBRs that have yet to be configured.

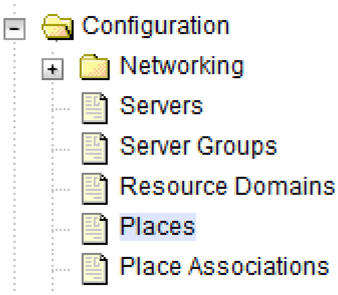
3.14.7 MP Configuration

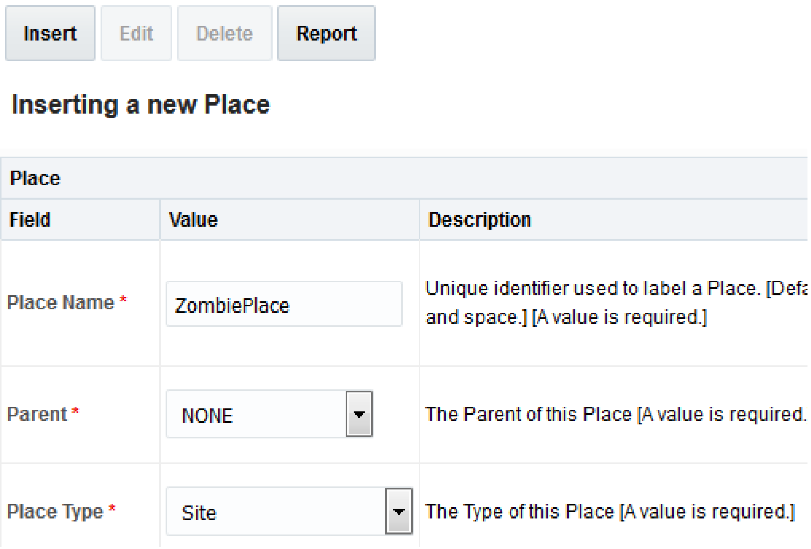
To configure MP blade servers (IPFE, SBR, DA-MP), refer to the procedure Configure MP Blade Servers in the C-Class Software Installation and Configuration Procedure 2/2.

Procedure 30. Configure Places and Assign MP Servers to Places (PCA and DCA Only)

This procedure adds places in the PCA/DCA network. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Primary NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of: `https://<NOAM_XMI_VIP_IP_Address>` 2. Login as the **guiadmin** user.  ORACLE Username: Password: ☐ Change password Log In Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to 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.*

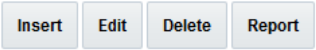
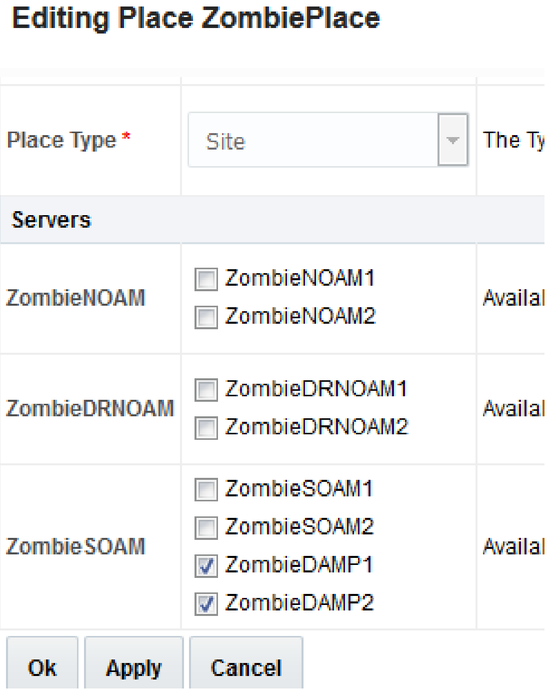
Procedure 30. Configure Places and Assign MP Servers to Places (PCA and DCA Only)

<table>
<tr>
<td>1.
☐</td>
<td>**NOAM VIP GUI**: Configure Places</td>
<td>
1. Navigate to **Configuration > Places**.

Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

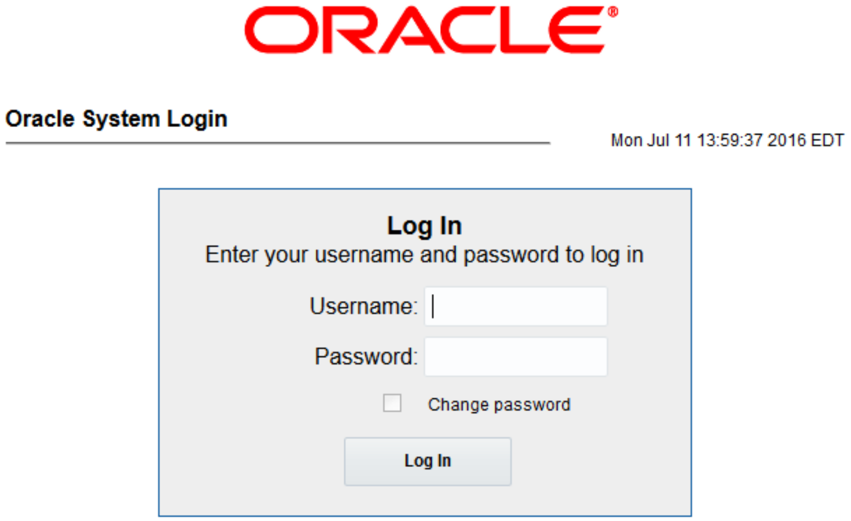
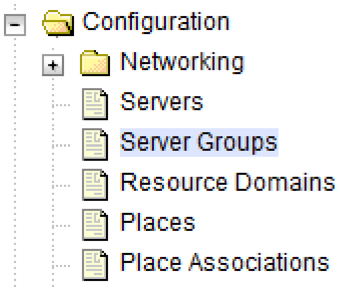
2. Click **Insert**.

Insert
Edit
Delete
Report

Inserting a new Place
<table>
<tr><th colspan="3">Place</th></tr>
<tr><th>Field</th><th>Value</th><th>Description</th></tr>
<tr><td>Place Name *</td><td>ZombiePlace</td><td>Unique identifier used to label a Place. [Defa
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>
</table>
3. Enter the fields as follows:
Place Name: <Site Name>
Parent: NONE
Place Type: Site
4. Repeat this step for each of the PCA places (sites) in the network.
See section 1.3 Terminology for more information on sites and places.
</td>
</tr>
</table>

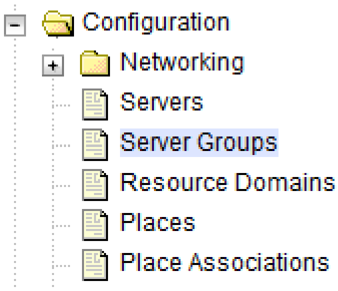
Procedure 30. Configure Places and Assign MP Servers to Places (PCA and DCA Only)

2. ☐	**NOAM VIP GUI**: Assign MP servers to places	1. Select the place just configured and click **Edit**.  2. For each place you have defined, select the set of MP servers that are assigned to those places.  Editing Place ZombiePlace Place Type * Site The Ty Servers ZombieNOAM ☐ ZombieNOAM1 ☐ ZombieNOAM2 Availal ZombieDRNOAM ☐ ZombieDRNOAM1 ☐ ZombieDRNOAM2 Availal ZombieSOAM ☐ ZombieSOAM1 ☐ ZombieSOAM2 ☑ ZombieDAMP1 ☑ ZombieDAMP2 Availal 3. Mark the PCA DA-MP and SBR server checkboxess assigned to this place. 4. Repeat this step for all other DA-MP or SBR servers you want to assign to places. ***Note:*** All PCA DA-MPs, SS7MPs, and SBR MPs must be added to the site place that corresponds to the physical location of the server. See section 1.3 Terminology for more information on sites.

Procedure 31. Configure DAMP Server Groups and Profiles

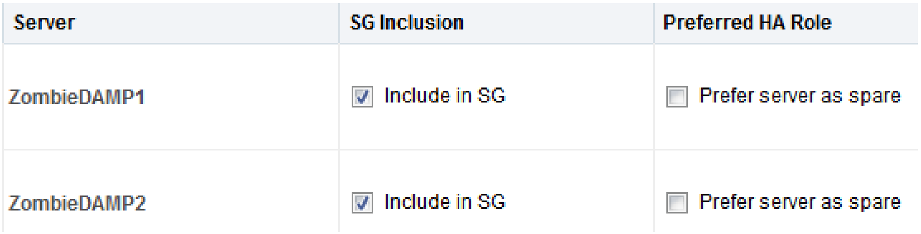
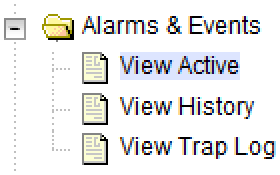
This procedure configures MP server groups as DAMPs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Primary NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of: `https://<NOAM_XMI_VIP_IP_Address>` 2. Login as the **guiadmin** user.  ORACLE 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
2. ☐	**NOAM VIP GUI**: Enter MP server group data	1. Navigate to **Configuration > Server Groups**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Click **Insert**. Insert Edit Delete Report 3. Enter these values: **Server Group Name**: <Server Group Name> **Level**: C **Parent**: SOAM server group that is parent to this MP **Function**: DSR (multi-active cluster) 4. Click **OK**.

Procedure 31. Configure DAMP Server Groups and Profiles

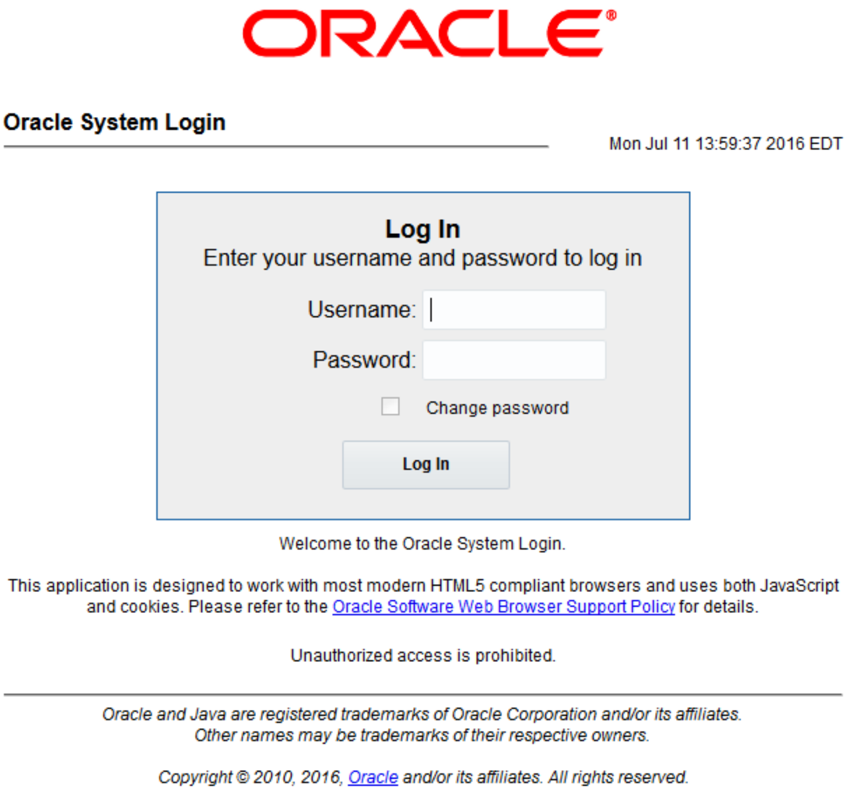
<table>
<tr>
<td>3.
☐</td>
<td>**NOAM VIP GUI**: Edit the MP server groups to include MPs</td>
<td>
1. Navigate to **Configuration > Server Groups**.

Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Select the server group you just created and click **Edit**.

Insert
Edit
Delete
Report

3. Select the network element that represents the MP server group.
4. Mark the **Include in SG** checkbox for the MP server.
5. Leave other checkboxes blank.

<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<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>
</table>
Each MP server should be included in the server group one at a time. Do not include multiple MPs at a time in the server group.
6. Click **OK**.
</td>
</tr>
<tr>
<td>4.
☐</td>
<td>**NOAM VIP GUI**: Wait for remote database alarm to clear</td>
<td>
Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding.
Monitor progress by navigating to **Alarms & Events > View Active**.

Alarms & Events
View Active
View History
View Trap Log
</td>
</tr>
</table>

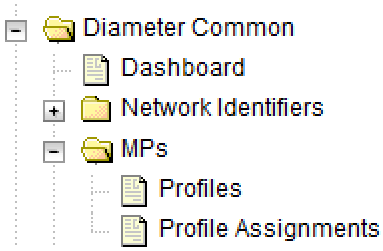
Procedure 31. Configure DAMP Server Groups and Profiles

5. ☐	**SOAM VIP GUI**: Login	1. 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>` 2. Login as the **guiadmin** user.  ORACLE® 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.*

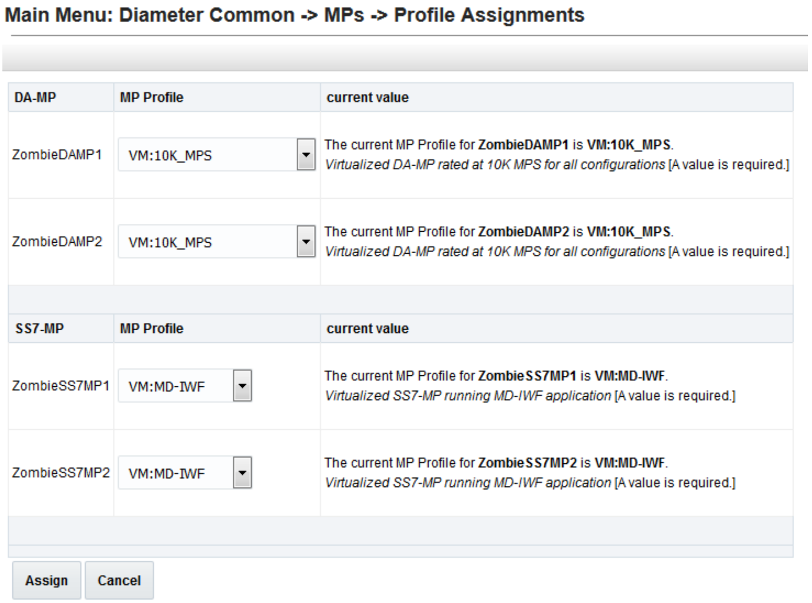
Procedure 31. Configure DAMP Server Groups and Profiles

6. ☐ **SOAM VIP GUI**: Assign profiles to DA-MPs from SOAM GUI

1. Navigate to **Diameter Common > MPs > Profiles Assignments**.



If the site has both DSR and MAP-IWF server groups, both DA-MP and SS7-MP sections display.

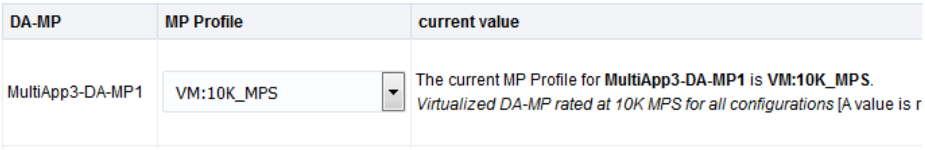

Main Menu: Diameter Common -> MPs -> Profile Assignments

DA-MP	MP Profile	current value
ZombieDAMP1	VM:10K_MPS	The current MP Profile for **ZombieDAMP1** is **VM:10K_MPS**. *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.]

2. For each MP, select the proper profile assignment based on the function of each MP.

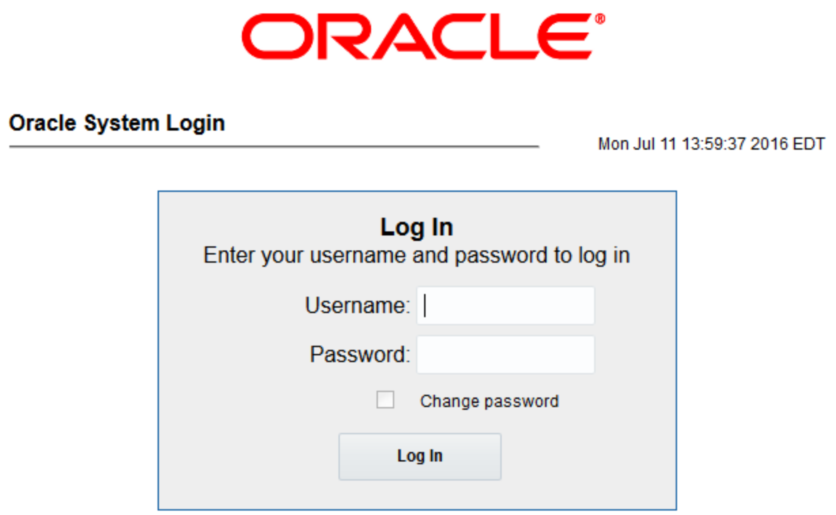
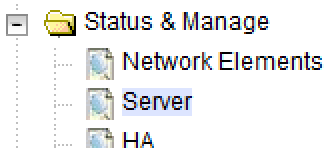
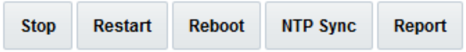
Profile Name	Description
VM:10K_MPS	Virtualized DA-MP rated at 10K MPS for all configurations
VM:Relay	Virtualized DA-MP Guest running the relay application
VM:Database	Virtualized DA-MP Guest running relay and database applications



DA-MP	MP Profile	current value
MultiApp3-DA-MP1	VM:10K_MPS	The current MP Profile for **MultiApp3-DA-MP1** is **VM:10K_MPS**. *Virtualized DA-MP rated at 10K MPS for all configurations* [A value is r

3. Click **Assign**.

Procedure 31. Configure DAMP Server Groups and Profiles

7. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. ORACLE 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
8. ☐	**NOAM VIP GUI**: Restart all MP servers	1. Navigate to **Status & Manage > Server**.  2. For each MP server, select the MP server and click **Restart**.  3. Click **OK** to confirm. Wait for the restart successful message. ***Note:*** **Policy and Charging DRA Installations/DCA Installations**: You may see alarms related to ComAgent until the PCA/DCA installation is complete.

Procedure 32. Configure IPFE Server Groups

This procedure configures MP server groups as IPFEs.

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

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

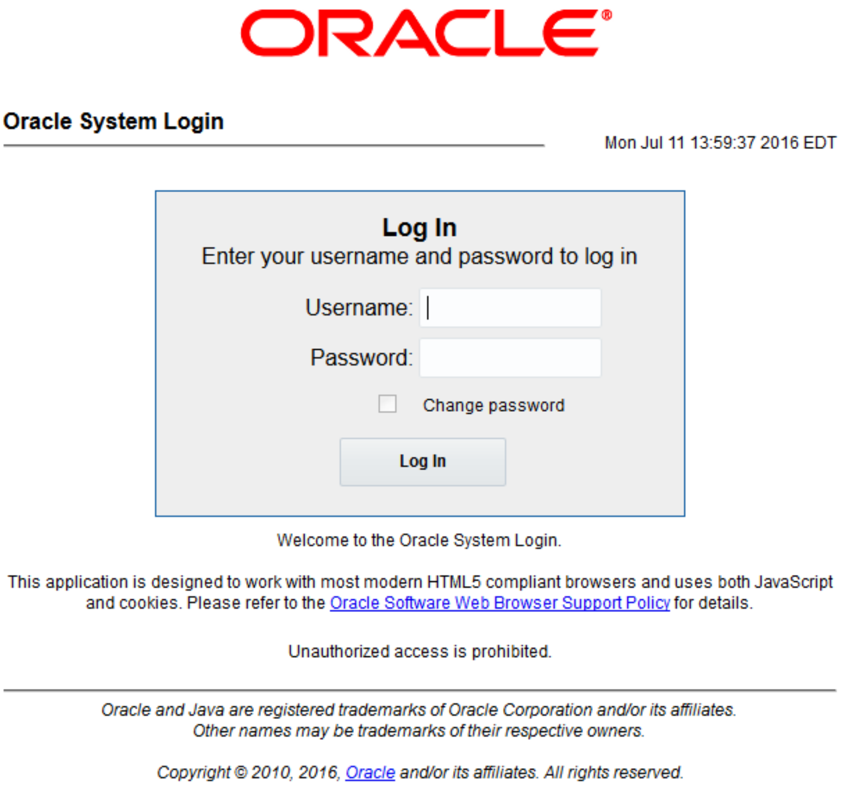
Procedure 32. Configure IPFE Server Groups

<table>
<tr>
<td>1.
☐</td>
<td>NOAM VIP GUI: Login</td>
<td>

1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:

```
https://<Primary_NOAM_VIP_IP_Address>
```

2. Login as the **guiadmin** user.



Oracle System Login

Mon Jul 11 13:59:37 2016 EDT

Log In

Enter your username and password to log in

Username:

Password:

☐ Change password

Log In

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

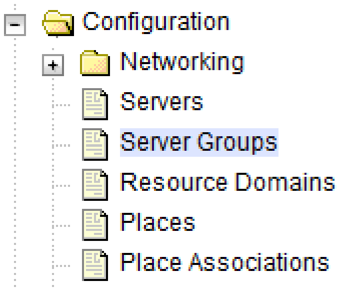
Unauthorized access is prohibited.

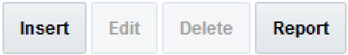
Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

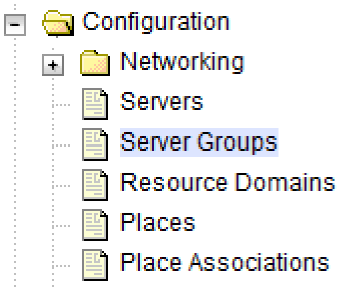
Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.

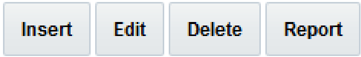
</td>
</tr>
</table>

Procedure 32. Configure IPFE Server Groups

<table>
<tr>
<td>2.
☐</td>
<td>NOAM VIP GUI: Enter MP server group data</td>
<td>
1. Navigate to Configuration > Server Groups.

Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

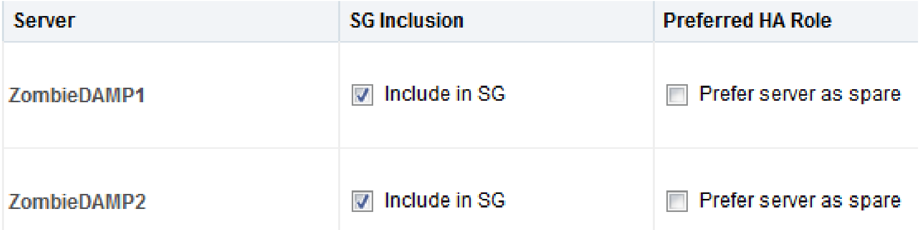
2. Click Insert.

Insert
Edit
Delete
Report

3. Enter these values:
<table>
<tr><td>Server Group Name:</td><td><Server Group Name></td></tr>
<tr><td>Level:</td><td>C</td></tr>
<tr><td>Parent:</td><td>SOAM server group that is parent to this MP</td></tr>
<tr><td>Function:</td><td>IP Front End</td></tr>
</table>
4. Click OK.
</td>
</tr>
<tr>
<td>3.
☐</td>
<td>NOAM VIP GUI: Edit the MP server groups to include MPs</td>
<td>
1. Navigate to Configuration > Server Groups.

Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Select the server group you just created and click Edit.

Insert
Edit
Delete
Report

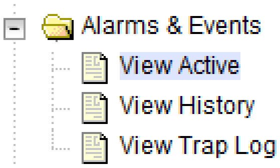
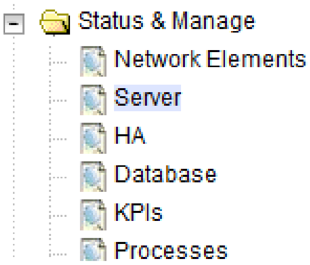
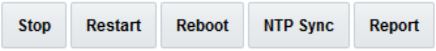
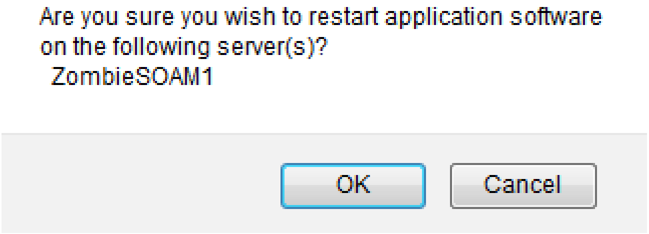
3. Select the network element that represents the MP server group.

4. Mark the Include in SG checkbox for the IPFE MP server.

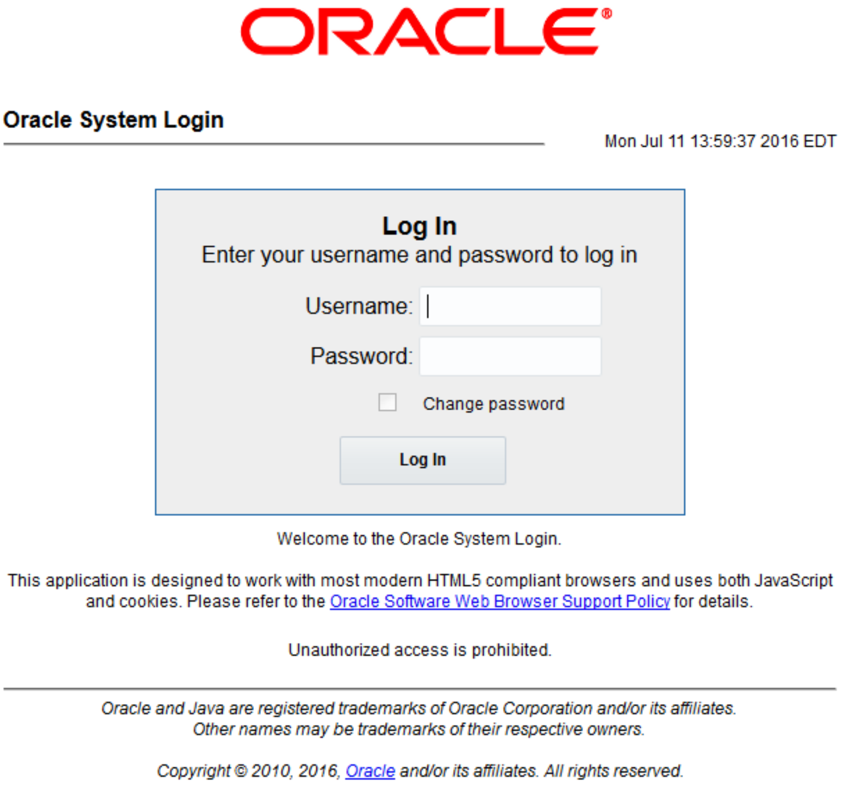
5. Leave other checkboxes blank.

<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<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>
</table>
IPFE MP server should have an individual server group of type IPFE.

6. Click OK.
</td>
</tr>
</table>

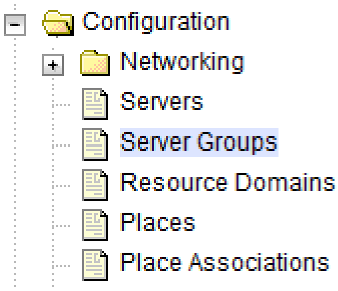
Procedure 32. Configure IPFE Server Groups

4. ☐	**NOAM VIP GUI**: Wait for remote database alarm to clear	Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding. Monitor progress by navigating to **Alarms & Events > View Active**.  Alarms & Events View Active View History View Trap Log
5. ☐	**NOAM GUI**: Restart MP server	1. Navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the MP server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm. Are you sure you wish to restart application software on the following server(s)? ZombieSOAM1

Procedure 33. Configure SS7-MP Server Groups and Profiles

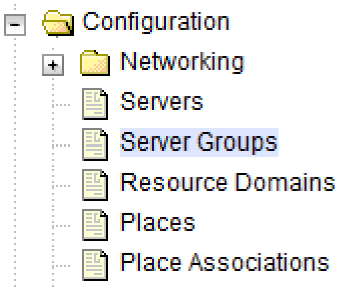
This procedure configures MP server groups as SS7-MPs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

Procedure 33. Configure SS7-MP Server Groups and Profiles

2. ☐	**NOAM VIP GUI**: Enter MP server group data	1. Navigate to **Configuration > Server Groups**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Click **Insert**. Insert Edit Delete Report 3. Enter these values: **Server Group Name**: <Server Group Name> **Level**: C **Parent**: SOAM server group that is parent to this MP **Function**: SS7-IWF 4. Click **OK**.

Procedure 33. Configure SS7-MP Server Groups and Profiles

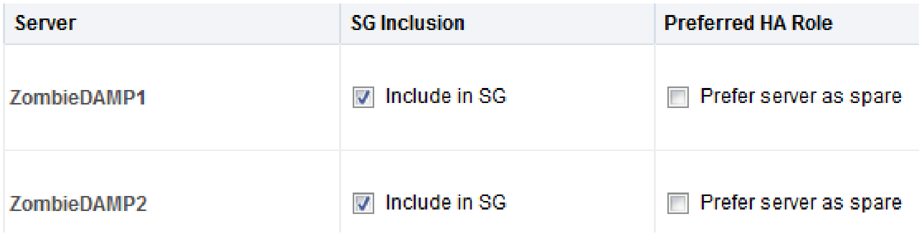
<table>
<tr>
<td>3.
☐</td>
<td>**NOAM VIP GUI**: Edit the MP server groups to include MPs</td>
<td>
1. Navigate to **Configuration > Server Groups**.


Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Select the server group you just created and click **Edit**.

Insert
Edit
Delete
Report

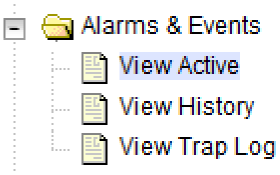
3. Select the network element that represents the MP server group.
4. Mark the **Include in SG** checkbox for the SS7-IWF MP server.
5. Leave other checkboxes blank.


Server | SG Inclusion | Preferred HA Role
ZombieDAMP1 | ☑ Include in SG | ☐ Prefer server as spare
ZombieDAMP2 | ☑ Include in SG | ☐ Prefer server as spare

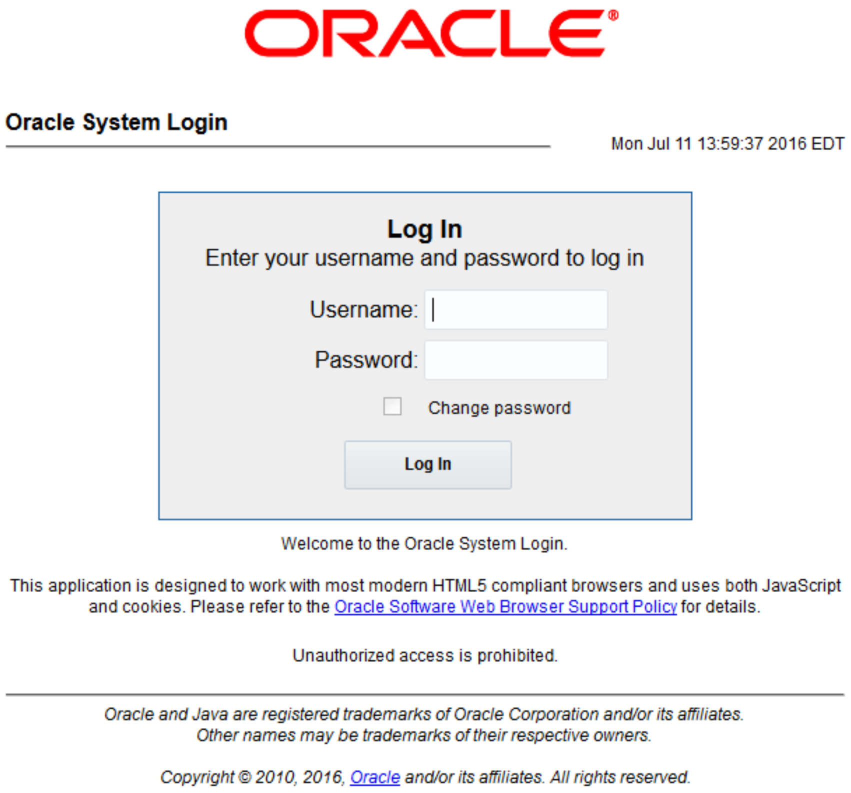
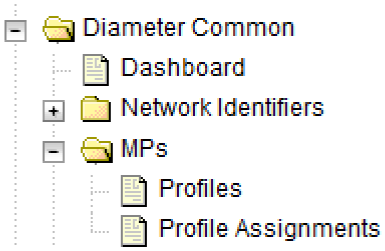
Each MP server should be included in the server group one at a time. Do not include multiple MPs at a time in the server group.

6. Click **OK**.
</td>
</tr>
<tr>
<td>4.
☐</td>
<td>**NOAM VIP GUI**: Wait for remote database alarm to clear</td>
<td>
Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding.

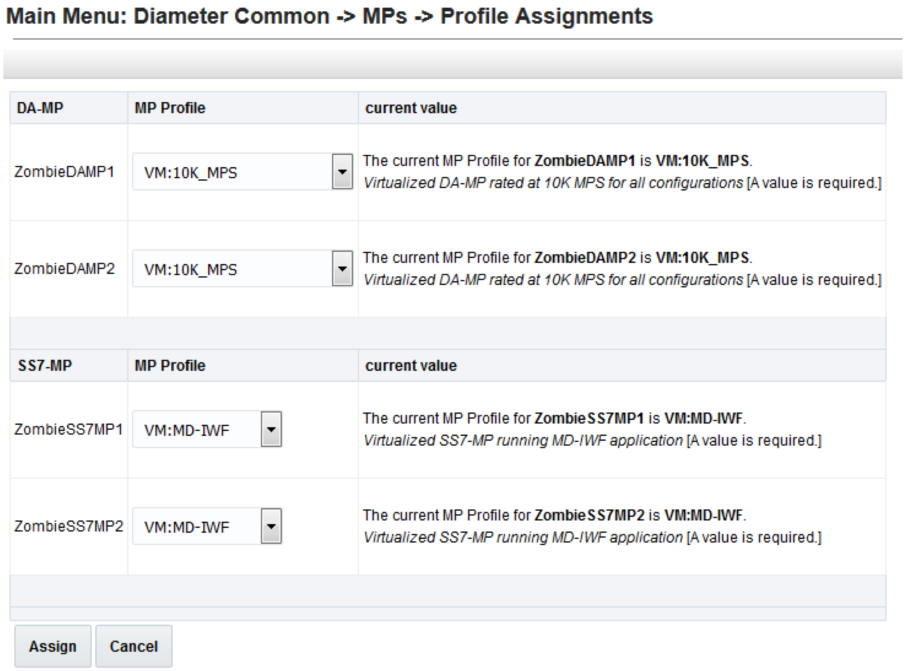
Monitor progress by navigating to **Alarms & Events > View Active**.


Alarms & Events
View Active
View History
View Trap Log
</td>
</tr>
</table>

Procedure 33. Configure SS7-MP Server Groups and Profiles

5. ☐	**SOAM VIP GUI**: Login	1. 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>` 2. Login as the **guiadmin** user.  **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*
6. ☐	**SOAM VIP GUI**: Assign profiles to DA-MPs from SOAM GUI	1. Navigate to **Diameter Common > MPs > Profiles Assignments**.  Diameter Common Dashboard Network Identifiers MPs Profiles Profile Assignments If the site has both DSR and MAP-IWF server groups, both DA-MP and SS7-MP sections display.

Procedure 33. Configure SS7-MP Server Groups and Profiles

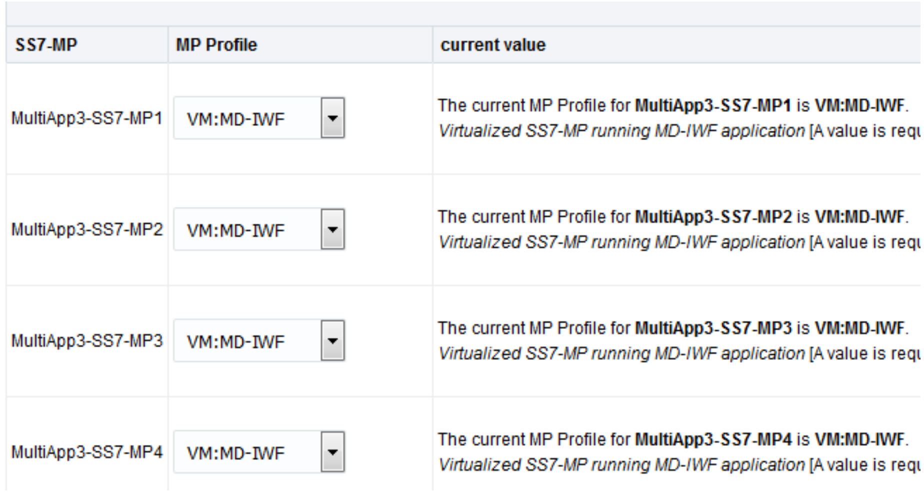

Main Menu: Diameter Common -> MPs -> Profile Assignments

DA-MP	MP Profile	current value
ZombieDAMP1	VM:10K_MPS	The current MP Profile for **ZombieDAMP1** is **VM:10K_MPS**. *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.]

2. For each SS7-MP, select the proper profile assignment based on the function of each MP.

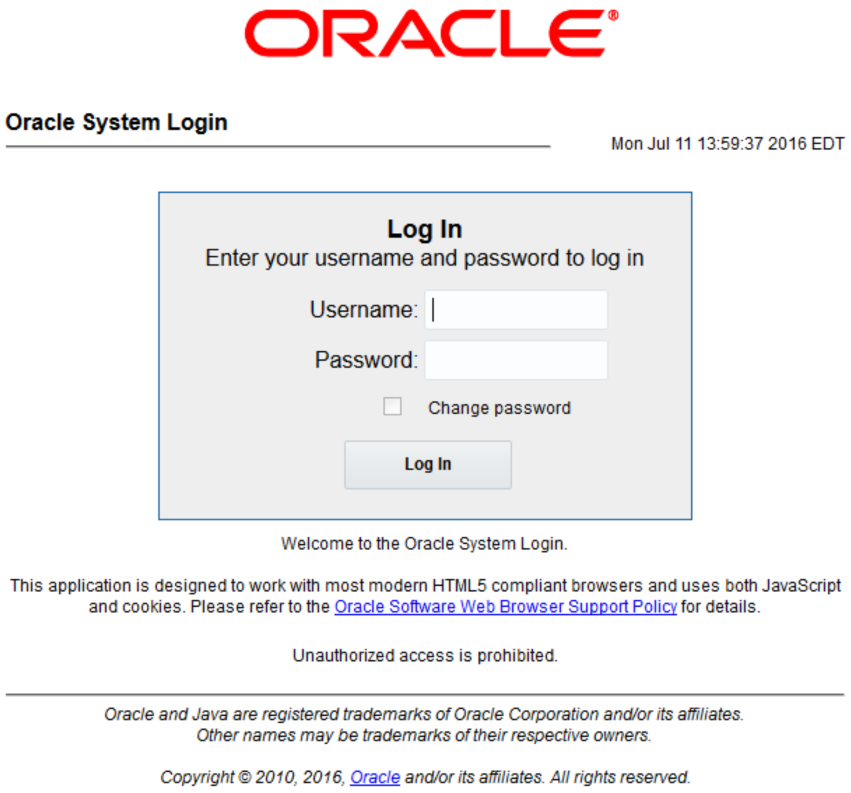
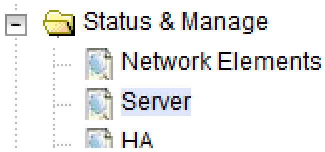
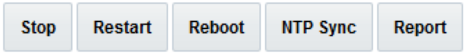
Profile Name	Description
VM:MD-IWF	Virtualized SS7-MP running MD-IWF application



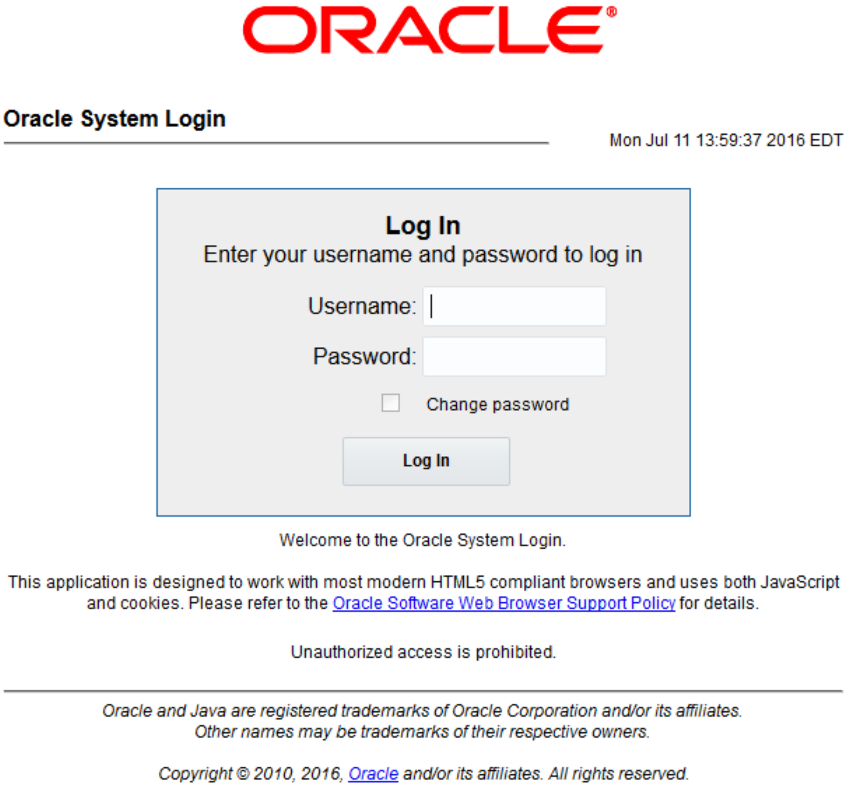
SS7-MP	MP Profile	current value
MultiApp3-SS7-MP1	VM:MD-IWF	The current MP Profile for **MultiApp3-SS7-MP1** is **VM:MD-IWF**. *Virtualized SS7-MP running MD-IWF application* [A value is requ
MultiApp3-SS7-MP2	VM:MD-IWF	The current MP Profile for **MultiApp3-SS7-MP2** is **VM:MD-IWF**. *Virtualized SS7-MP running MD-IWF application* [A value is requ
MultiApp3-SS7-MP3	VM:MD-IWF	The current MP Profile for **MultiApp3-SS7-MP3** is **VM:MD-IWF**. *Virtualized SS7-MP running MD-IWF application* [A value is requ
MultiApp3-SS7-MP4	VM:MD-IWF	The current MP Profile for **MultiApp3-SS7-MP4** is **VM:MD-IWF**. *Virtualized SS7-MP running MD-IWF application* [A value is requ

3. Click **Assign**.

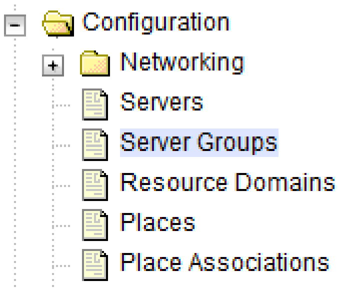
Procedure 33. Configure SS7-MP Server Groups and Profiles

7. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  Oracle System Login Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*
8. ☐	**NOAM VIP GUI**: Restart all MP servers	1. Navigate to **Status & Manage > Server**.  2. For each MP server, select the MP server and click **Restart**.  3. Click **OK** to confirm. Wait for the restart successful message.

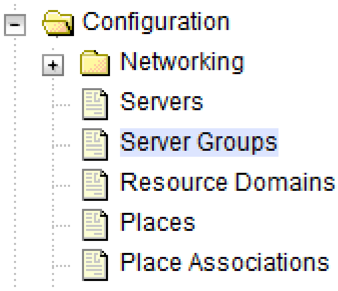
Procedure 34. Configure Session SBR Server Groups

<table>
<tr><td colspan="3">This procedure configures MP server groups as session SBRs.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>**NOAM VIP GUI**: Login</td><td>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:
`https://<Primary_NOAM_VIP_IP_Address>`
2. Login as the **guiadmin** user.

Oracle System Login
Mon Jul 11 13:59:37 2016 EDT
Log In
Enter your username and password to log in
Username:
Password:
☐ Change password
Log In
Welcome to the Oracle System Login.
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.
Unauthorized access is prohibited.
Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.</td></tr>
</table>

Procedure 34. Configure Session SBR Server Groups

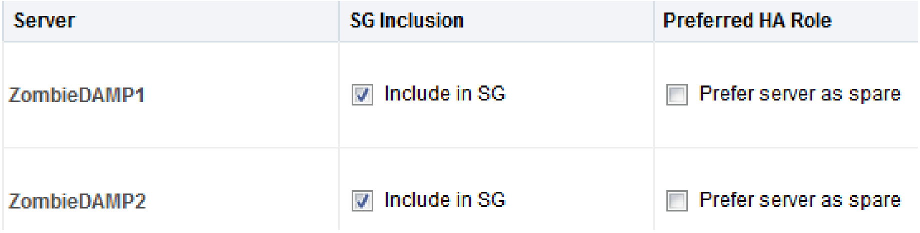
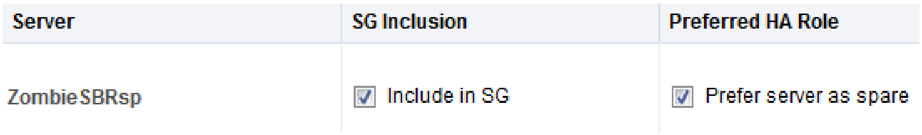
2. ☐	**NOAM VIP GUI**: Enter MP server group data	1. Navigate to **Configuration > Server Groups**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Click **Insert**. Insert Edit Delete Report 3. Enter these values: **Server Group Name**: <Server Group Name> **Level**: C **Parent**: SOAM server group that is parent to this MP **Function**: SBR **WAN Replication Connection Count**: 8 4. Click **OK**.

Procedure 34. Configure Session SBR Server Groups

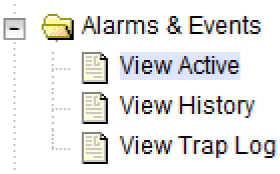
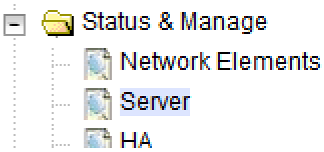
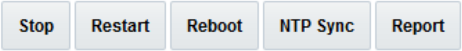
<table>
<tr>
<td>3.
☐</td>
<td>NOAM VIP GUI: Edit the MP server groups to include MPs</td>
<td>
1. Navigate to Configuration > Server Groups.


2. Select the server group you just created and click Edit.

Insert
Edit
Delete
Report

3. Select the network element that represents the MP server group.
4. Mark the Include in SG checkbox for the Session SBR MP server.
5. Leave other checkboxes blank.

<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<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>
</table>
Each MP server should be included in the server group one at a time. Do not include multiple MPs at a time in the server group.
6. Click OK.
</td>
</tr>
<tr>
<td>4.
☐</td>
<td>NOAM VIP GUI: Edit the MP server group and add preferred spares for site redundancy (optional)
PCA/DCA Only</td>
<td>
If Two Site Redundancy feature for the Policy and Charging SBR server group OR Session Binding Repository is wanted, add an MP server that is physically located in a separate site (location) to the server group by marking the Include in SG checkbox. Also, mark the Preferred Spare checkbox.

<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<tr><td>ZombieSBRsp</td><td>☑ Include in SG</td><td>☑ Prefer server as spare</td></tr>
</table>
If Three Site Redundancy feature for the SBR MP server group is wanted, add two SBR MP servers that are both physically located in separate sites (location) to the server group by marking the Include in SG checkbox. Also, mark the Preferred Spare checkbox for both servers.
<i>Note:</i> 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).
For more information about site redundancy for Policy and Charging SBR server groups/session binding repository server groups, see section 1.3 Terminology.
Click OK to save.
</td>
</tr>
</table>

Procedure 34. Configure Session SBR Server Groups

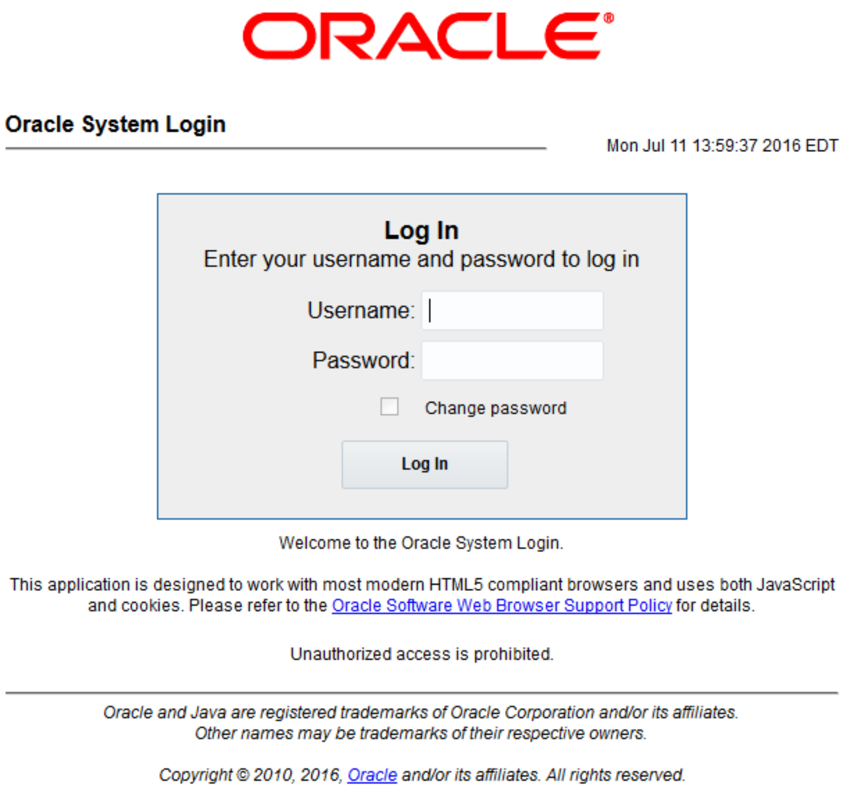
5. ☐	**NOAM VIP GUI**: Wait for remote database alarm to clear	Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding. Monitor progress by navigating to **Alarms & Events > View Active**.  Alarms & Events View Active View History View Trap Log
6. ☐	**NOAM VIP GUI**: Restart all MP servers	1. Navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA 2. For each MP server, select the MP server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm. Wait for the restart successful message.

Procedure 35. Configure Binding SBR Server Groups

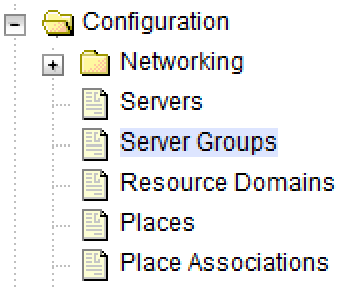
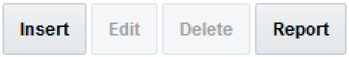
This procedure configures MP server groups as binding SBRs.

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

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

1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

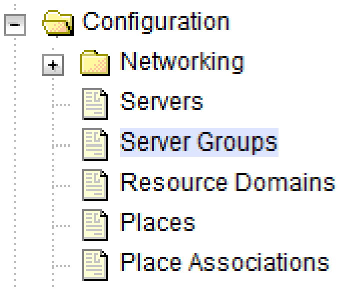
Procedure 35. Configure Binding SBR Server Groups

2. ☐	**NOAM VIP GUI**: Enter MP server group data	1. Navigate to **Configuration > Server Groups**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Click **Insert**.  Insert Edit Delete Report 3. Enter these values: **Server Group Name**: <Server Group Name> **Level**: C **Parent**: SOAM server group that is parent to this MP **Function**: SBR **WAN Replication Connection Count**: 8 4. Click **OK**.

Procedure 35. Configure Binding SBR Server Groups

3. ☐ **NOAM VIP GUI**: Edit the MP server groups to include MPs

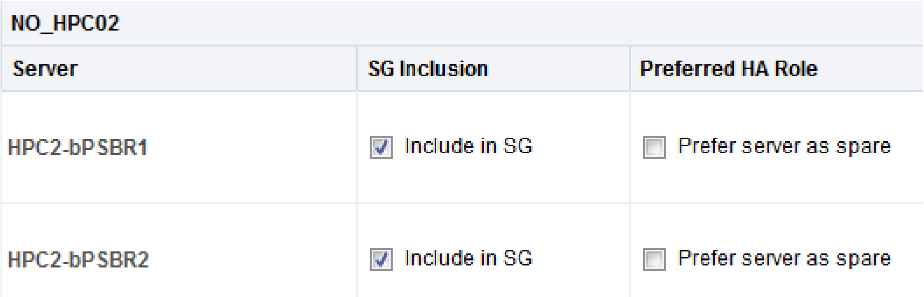
1. Navigate to **Configuration > Server Groups**.


Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Select the server group you just created and click **Edit**.

Insert
Edit
Delete
Report

3. Select the network element that represents the MP server group.
4. Mark the **Include in SG** checkbox for the MP server.
5. Leave other checkboxes blank.



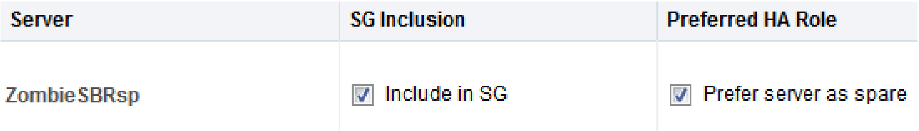
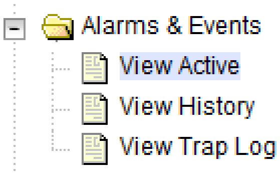
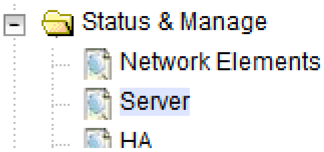
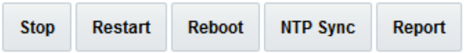
NO_HPC02

Server	SG Inclusion	Preferred HA Role
HPC2-bPSBR1	☑ Include in SG	☐ Prefer server as spare
HPC2-bPSBR2	☑ Include in SG	☐ Prefer server as spare

Each MP server should be included in the server group one at a time. Do not include multiple MPs at a time in the server group.

6. Click **OK**.

Procedure 35. Configure Binding SBR Server Groups

4. ☐	**NOAM VIP GUI**: Edit the MP server group and add preferred spares for site redundancy (optional) PCA/DCA Only	If Two Site Redundancy feature for the Policy and Charging SBR server group OR Session Binding Repository is wanted, add an MP server that is physically located in a separate site (location) to the server group by marking the **Include in SG** checkbox. Also, mark the **Preferred Spare** checkbox.  Server | SG Inclusion | Preferred HA Role ZombieSBRsp | ☑ Include in SG | ☑ Prefer server as spare If Three Site Redundancy feature for the SBR MP server group is wanted, add two SBR MP servers that are both physically located in separate sites (location) to the server group by marking the **Include in SG** checkbox. Also, mark 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). For more information about site redundancy for Policy and Charging SBR server groups/session binding repository server groups, see section 1.3 Terminology. Click **OK** to save.
5. ☐	**NOAM VIP GUI**: Wait for remote database alarm to clear	Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding. Monitor progress by navigating to **Alarms & Events > View Active**.  Alarms & Events View Active View History View Trap Log
6. ☐	**NOAM VIP GUI**: Restart all MP servers	1. Navigate to **Status & Manage > Server**.  2. For each MP server, select the MP server and click **Restart**.  3. Click **OK** to confirm. Wait for the restart successful message.

3.14.8 Signaling Network Configuration

To configure signaling network routes on MP-type servers (DA-MP, IPFE, and so on), refer to the procedure Configure the Signaling Network Routes in the C-Class Software Installation and Configuration Procedure 2/2.

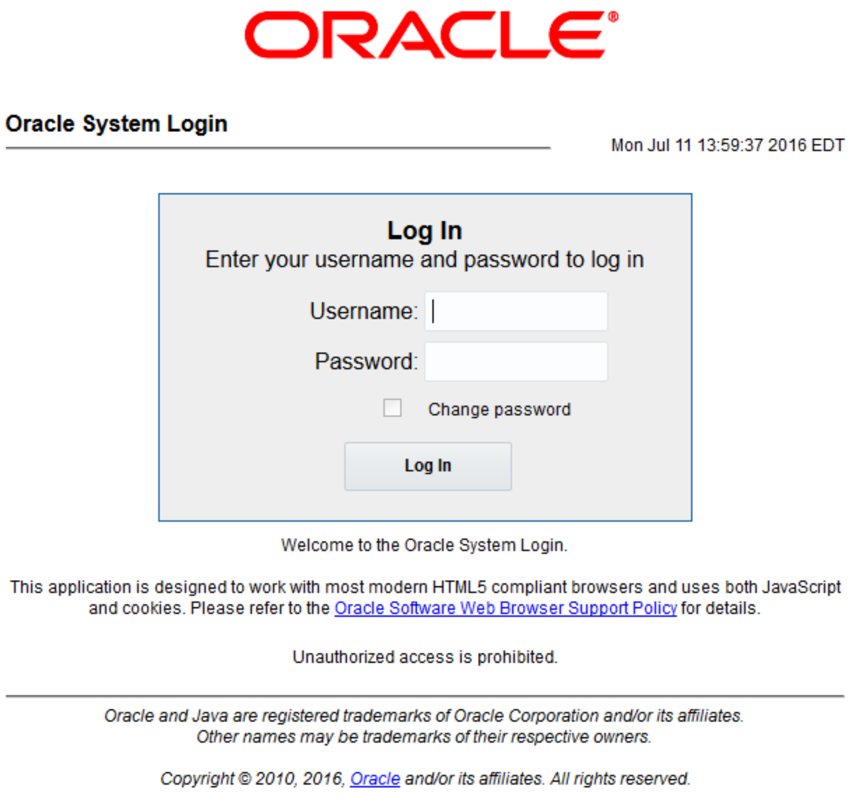
3.14.9 DSCP Configuration (Optional)

Procedure 36. Configure DSCP Values for Outgoing Traffic (Optional)

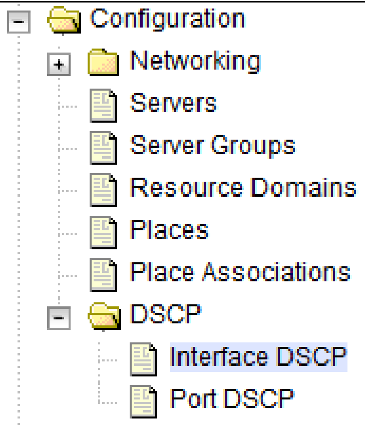
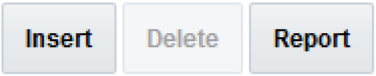
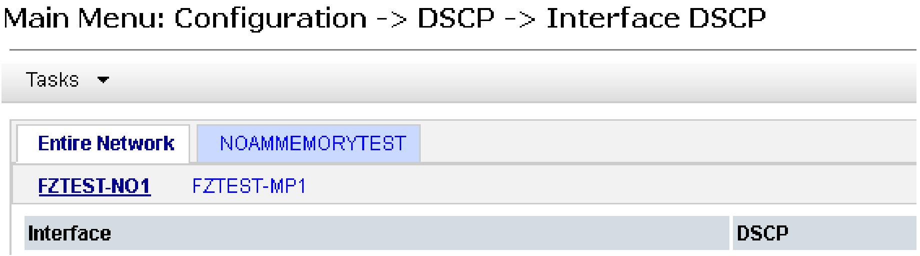
This procedure configures the DSCP values for outgoing packets on servers. DSCP values can be applied to an outbound interface as a whole, or to all outbound traffic using a specific TCP or SCTP source port. This step is optional and should only be executed if your network uses packet DSCP markings for quality-of-service.

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

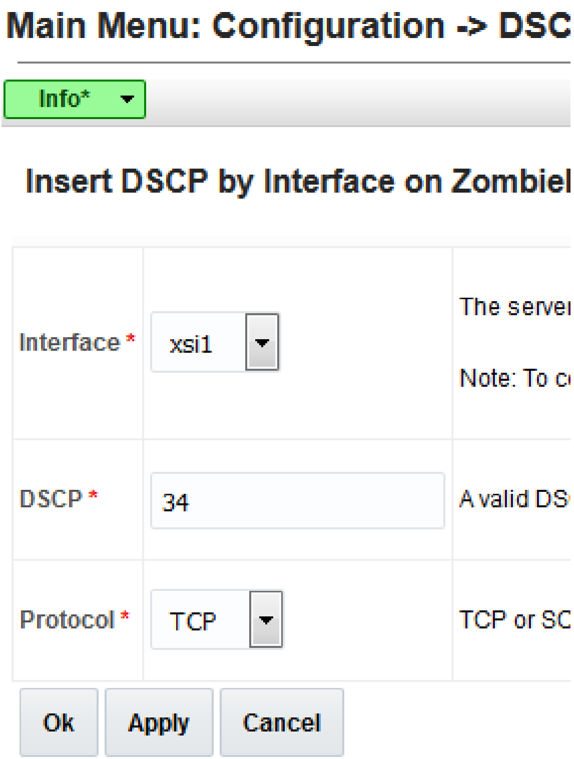
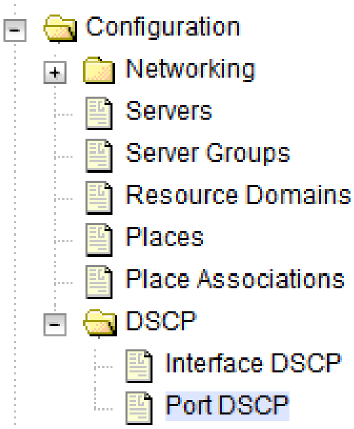
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**Primary NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of: `https://<NOAM_XMI_VIP_IP_Address>` 2. Login as the **guiadmin** user.  **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*
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 vary. 3. Navigate to **Configuration > DSCP > Interface DSCP**.

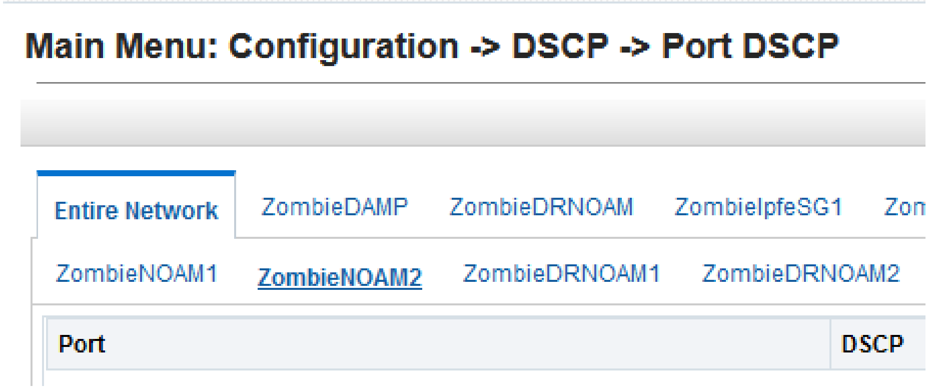
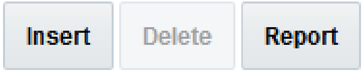
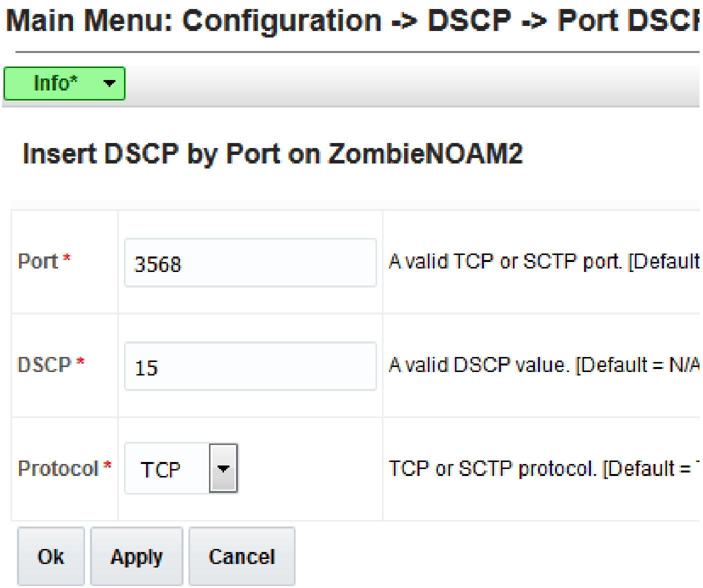
Procedure 36. Configure DSCP Values for Outgoing Traffic (Optional)

		 Configuration Networking Servers Server Groups Resource Domains Places Place Associations DSCP Interface DSCP Port DSCP 4. Select the server you want to configure from the list of servers on the second line. You can view all servers with **Entire Network** selected; or limit yourself to a specific server group by clicking on that server group name's tab. 5. Click **Insert**.  Insert Delete Report  Main Menu: Configuration -> DSCP -> Interface DSCP Tasks Entire Network NOAMMEMORYTEST FZTEST-NO1 FZTEST-MP1 Interface DSCP 6. Select the network **Interface**, type the **DSCP** value to apply to packets leaving this interface, and select the transport **Protocol**.

Procedure 36. Configure DSCP Values for Outgoing Traffic (Optional)

		 Main Menu: Configuration -> DSC Insert DSCP by Interface on Zombiel Interface * xsi1 The serve Note: To c DSCP * 34 A valid DS Protocol * TCP TCP or SC Info* Ok Apply Cancel 7. Click **OK** if there are no more interfaces on this server to configure, or click **Apply** to finish this interface and continue with more interfaces by selecting them from the drop down and entering their DSCP values.
3. ☐	**NOAM VIP GUI**: Option 2 — Configure port DSCP	***Note:*** The exact DSCP values for your site vary. 1. Navigate to **Configuration > DSCP > Port DSCP**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations DSCP Interface DSCP Port DSCP 2. Select the server you want to configure from the list of servers on the second line. You can view all servers with **Entire Network** selected; or limit yourself to a specific server group by clicking on that server group name's tab.

Procedure 36. Configure DSCP Values for Outgoing Traffic (Optional)

		 Main Menu: Configuration -> DSCP -> Port DSCP Entire Network ZombieDAMP ZombieDRNOAM ZombieIpfeSG1 Zon ZombieNOAM1 ZombieNOAM2 ZombieDRNOAM1 ZombieDRNOAM2 Port DSCP 3. Click **Insert**.  Insert Delete Report 4. Enter the source **Port**, **DSCP** value, and select the transport **Protocol**.  Main Menu: Configuration -> DSCP -> Port DSCI Info* Insert DSCP by Port on ZombieNOAM2 Port * 3568 A valid TCP or SCTP port. [Default DSCP * 15 A valid DSCP value. [Default = N/A Protocol * TCP TCP or SCTP protocol. [Default = Ok Apply Cancel 5. 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 DSCP mappings.
4. ☐	**NOAM VIP GUI**: Repeat for additional servers	Repeat this procedure for all remaining servers.

3.14.10 SNMP Configuration

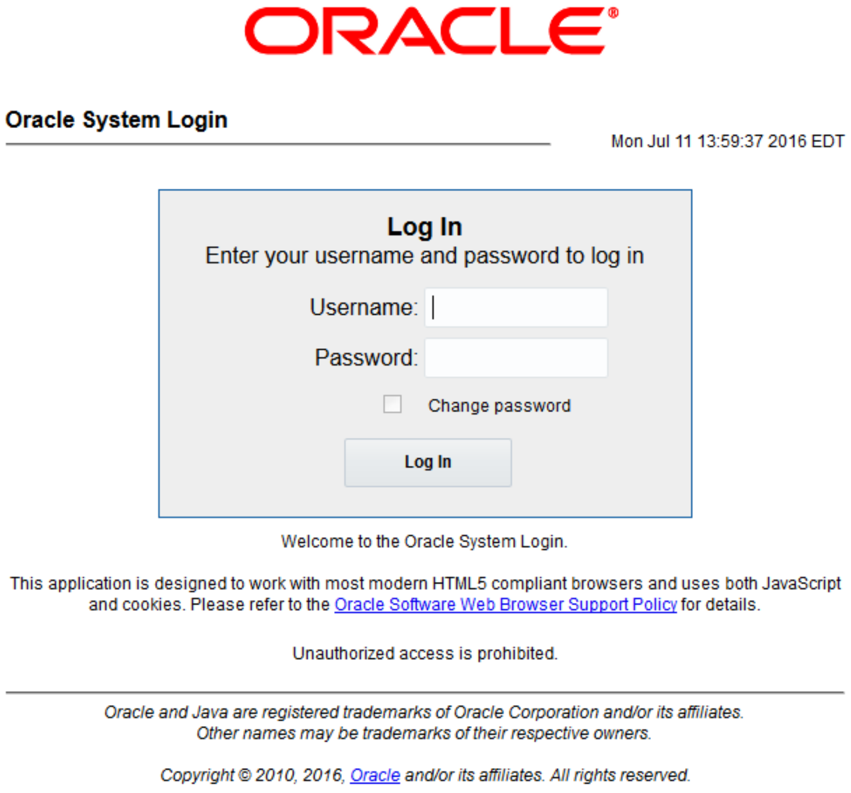
Procedure 37. Configure SNMP Trap Receivers

This procedure configures forwarding of SNMP traps from each individual server.

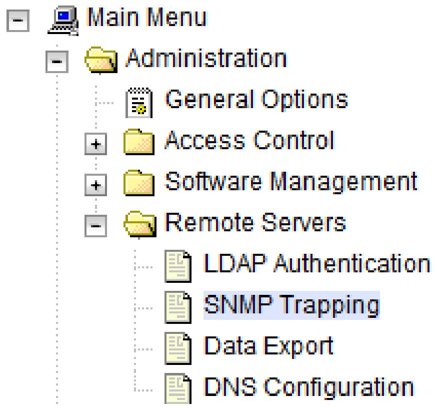
Note: If SNMP configuration is not required, skip to step 4.

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

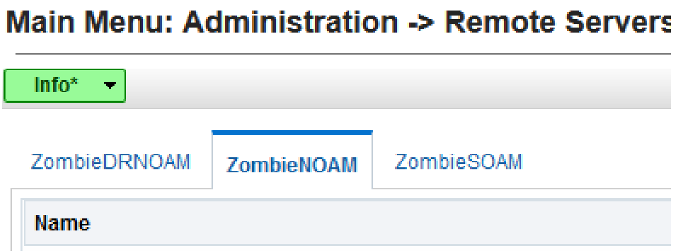
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**Primary NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of: `https://<NOAM_XMI_VIP_IP_Address>` 2. Login as the **guiadmin** user.  ORACLE Log In Username: Password: ☐ Change password Log In **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT Enter your username and password to 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.*
2. ☐	**NOAM VIP GUI**: Configure system-wide SNMP trap receiver(s)	1. Navigate to **Administration > Remote Servers > SNMP Trapping**.

Procedure 37. Configure SNMP Trap Receivers

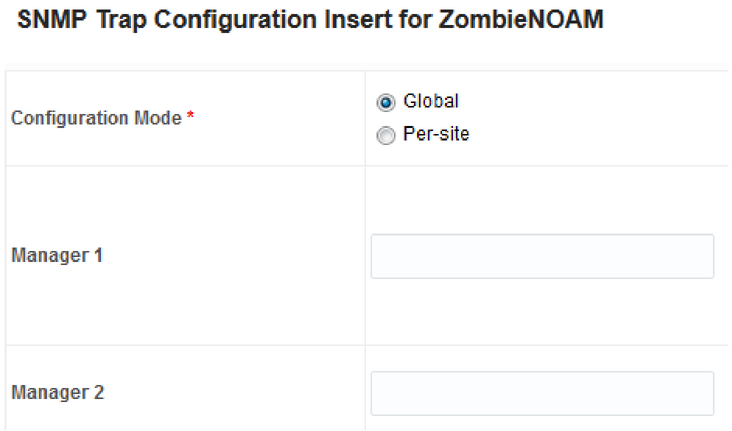

Main Menu
Administration
General Options
Access Control
Software Management
Remote Servers
LDAP Authentication
SNMP Trapping
Data Export
DNS Configuration

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


Main Menu: Administration -> Remote Servers
Info*
ZombieDRNOAM
ZombieNOAM
ZombieSOAM
Name

3. Type the **IP address** or **Hostname** of the Network Management Station (NMS) to forward traps to. This IP should be reachable from the NOAMP's XMI network.

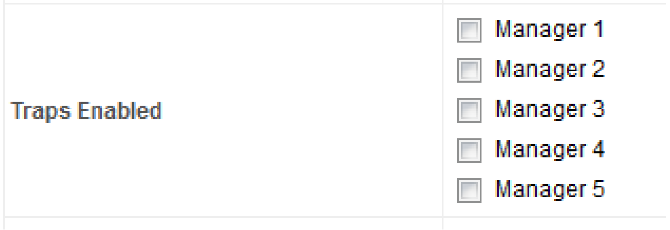
4. Add additional secondary, tertiary, etc., **Manager IPs** in the corresponding slots, if desired.



SNMP Trap Configuration Insert for ZombieNOAM

Configuration Mode *	● Global ○ Per-site
Manager 1	
Manager 2	

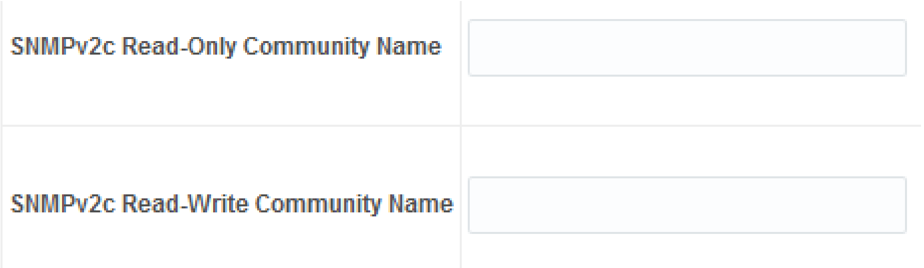
5. Mark the **Traps Enabled** checkboxes for the manager servers being configured:



Traps Enabled	☐ Manager 1 ☐ Manager 2 ☐ Manager 3 ☐ Manager 4 ☐ Manager 5

Procedure 37. Configure SNMP Trap Receivers

<table>
<tr>
<td></td>
<td></td>
<td>
6. Type the SNMP Community Name.

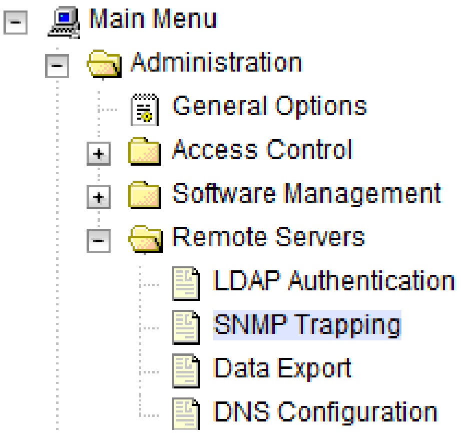

SNMPv2c Read-Only Community Name
SNMPv2c Read-Write Community Name

7. Leave all other fields at their default values.

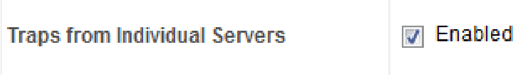
8. Click OK.
</td>
</tr>
<tr>
<td>3.
☐</td>
<td>NOAMP VIP: Enable traps from individual servers (optional)</td>
<td>
<i>Note:</i> By default, SNMP traps from DPs are aggregated and displayed at the active NOAMP. If instead, you want every server to send its own traps directly to the NMS, then execute this procedure.

This procedure requires all servers, including DPs, have an XMI interface on which the customer SNMP target server (NMS) is reachable.

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


Main Menu
Administration
General Options
Access Control
Software Management
Remote Servers
LDAP Authentication
SNMP Trapping
Data Export
DNS Configuration

2. Make sure the checkbox next to Enabled is checked, if not, check it.



Traps from Individual Servers ☑ Enabled

3. Click Apply and verify the data is committed.
</td>
</tr>
</table>

Procedure 37. Configure SNMP Trap Receivers

4. ☐ **PMAC GUI**: Update the TVOE host SNMP community string

1. Establish an SSH session to the PMAC and Login as **admusr**.
2. Update the community string.

```
$ sudo pmaccli setCommStr --accessType=rw --
commStr=<site specific value>
```

Note: When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest on the PMAC control network are updated. All servers that match the existing site specific community string are not updated again until the string name is changed.

3. Restart the server.

```
$ sudo sentry restart
```

5. ☐ **NOAM VIP GUI**: Login

Note: This workaround step should be performed only in these cases:

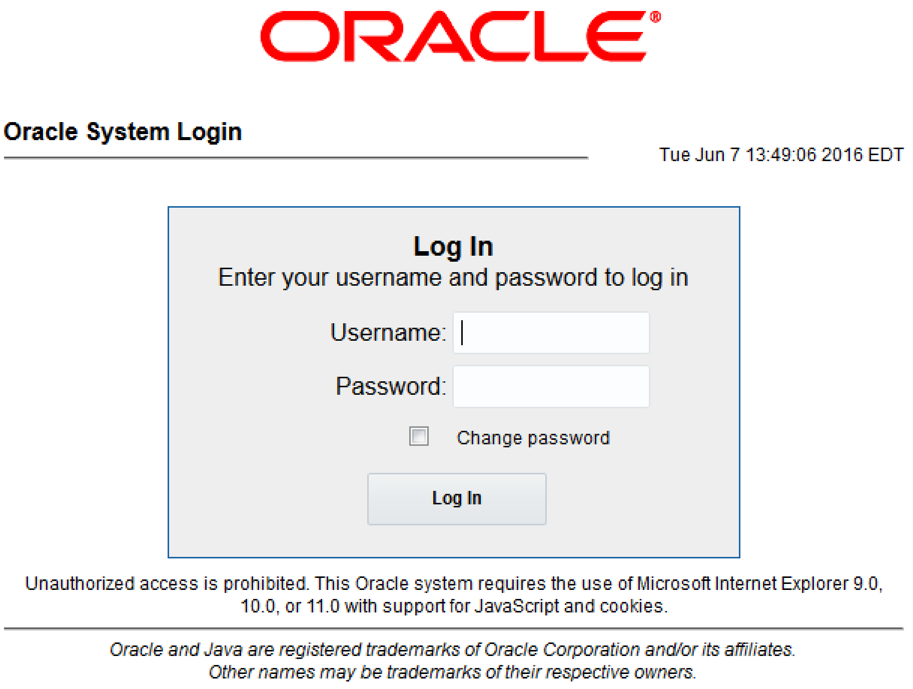
- If SNMP is not configured.
- If SNMP is already configured and SNMPv3 is selected as enabled version.

Note: This is a workaround step to configure SNMP with 'SNMPv2c and SNMPv3' as the enabled versions for SNMP Traps configuration, since PMAC does not support SNMPv3.

1. Establish a GUI session on the NOAM server using the VIP IP address of the NOAM server.
2. Open the web browser and enter a URL of:

```
https://<Primary_NOAM_VIP_IP_Address>
```

3. Log into the NOAM GUI as the **guiadmin** user:



ORACLE

Oracle System Login

Tue Jun 7 13:49:06 2016 EDT

Log In

Enter your username and password to log in

Username:

Password:

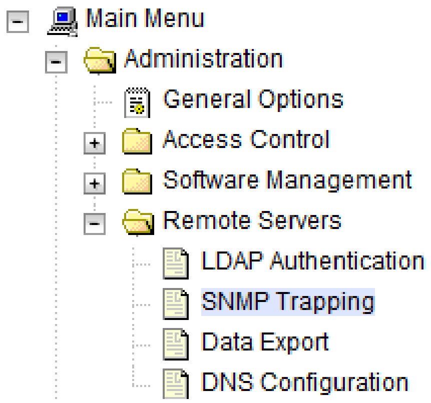
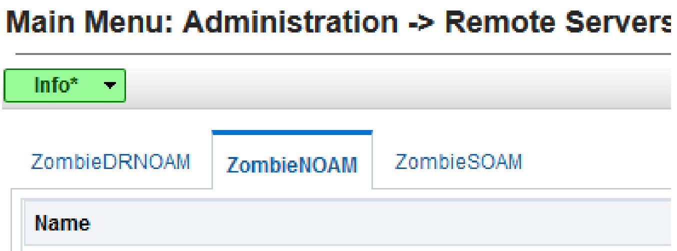
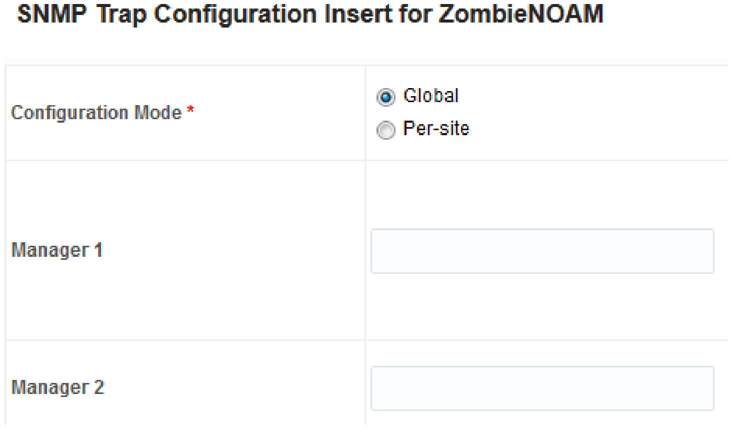
☐ Change password

Log In

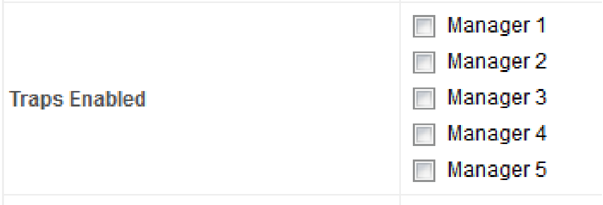
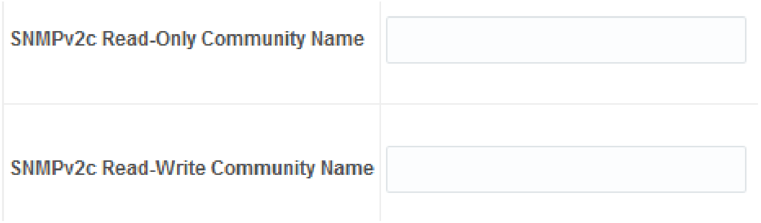
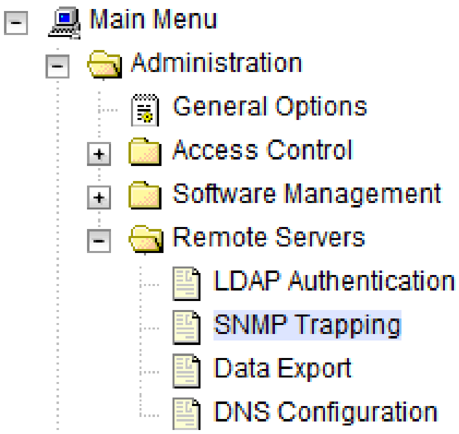
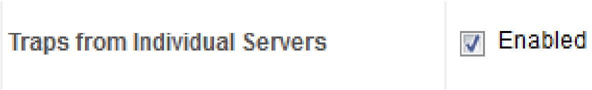
Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.

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

Procedure 37. Configure SNMP Trap Receivers

6. ☐	**NOAM VIP GUI**: Configure system-wide SNMP trap receiver(s)	1. Navigate to **Administration > Remote Servers > SNMP Trapping**.  Main Menu Administration General Options Access Control Software Management Remote Servers LDAP Authentication SNMP Trapping Data Export DNS Configuration 2. Select the Server Group tab for SNMP trap configuration.  Main Menu: Administration -> Remote Servers Info* ZombieDRNOAM ZombieNOAM ZombieSOAM Name 3. Type the **IP address** or **Hostname** of the Network Management Station (NMS) where you want to forward traps. This IP should be reachable from the NOAMP's XMI network. If already configured SNMP with **SNMPv3** as enabled version, another server needs to be configured here. 4. Add additional secondary, tertiary, etc., **Manager IPs** in the corresponding slots, if desired.  SNMP Trap Configuration Insert for ZombieNOAM Configuration Mode * ● Global ○ Per-site Manager 1 Manager 2 5. Set the Enabled Versions as **SNMPv2c and SNMPv3**. Enabled Versions: SNMPv2c and SNMPv3 6. Mark the **Traps Enabled** checkboxes for the manager servers being configured.

Procedure 37. Configure SNMP Trap Receivers

		 Traps Enabled ☐ Manager 1 ☐ Manager 2 ☐ Manager 3 ☐ Manager 4 ☐ Manager 5 7. Type the **SNMP Community Name**.  SNMPv2c Read-Only Community Name SNMPv2c Read-Write Community Name 8. Leave all other fields at their default values. 9. Click **OK**.
7. ☐	**NOAMP VIP**: Enable traps from individual servers (optional)	***Note:*** By default, SNMP traps from DPs are aggregated and displayed at the active NOAMP. If instead, you want every server to send its own traps directly to the NMS, then execute this procedure. This procedure requires all servers, including DPs, have an XMI interface on which the customer SNMP target server (NMS) is reachable. 1. Navigate to **Administration > Remote Servers > SNMP Trapping**.  Main Menu Administration General Options Access Control Software Management Remote Servers LDAP Authentication SNMP Trapping Data Export DNS Configuration 2. Make sure the checkbox next to **Enabled** is checked, if not, check it.  Traps from Individual Servers ☑ Enabled 3. Click **Apply** and verify the data is committed.

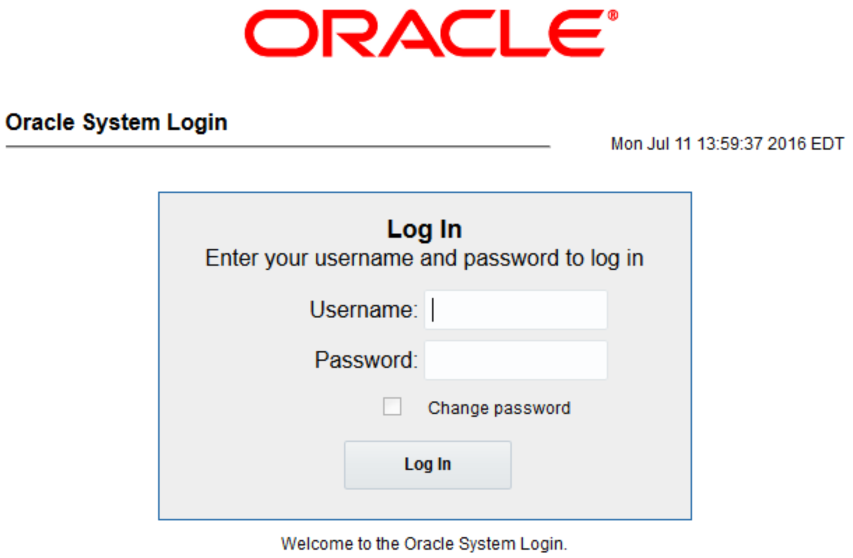
Procedure 37. Configure SNMP Trap Receivers

8.
☐
	PMAC GUI: Update the TVOE host SNMP community string	1. Establish an SSH session to the PMAC and Login as **admusr**.
		2. Update the community string.
		`$ sudo pmaccli setCommStr --accessType=rw --commStr=<site specific value>`
		Note: When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest on the PMAC control network are updated. All servers that match the existing site specific community string are not updated again until the string name is changed.
		3. Restart the server.
		`$ sudo sentry restart`

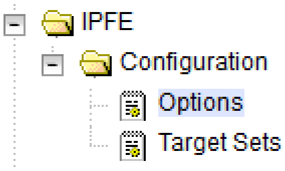
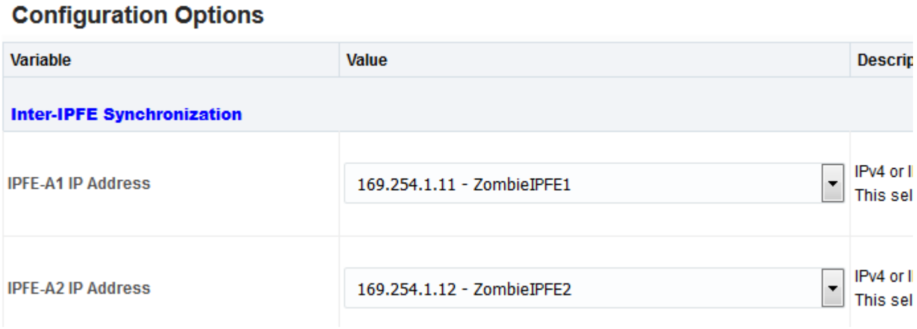
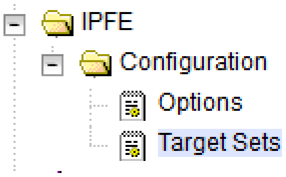
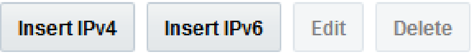
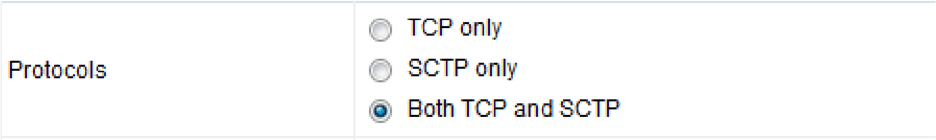
9. ☐	SNMPv3 (optional)	Refer to Appendix T Restore SNMP Configuration to SNMPv3 (Optional) to restore SNMPv3 after installation, if required.

3.14.11 IPFE Configuration (Optional)

Procedure 38. Configure IPFE (Optional)

This procedure configures IP front end (IPFE) and optimizes performance. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**SOAM VIP GUI**: Login	1. 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>` 2. Login as the **guiadmin** user.  Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login.

Procedure 38. Configure IPFE (Optional)

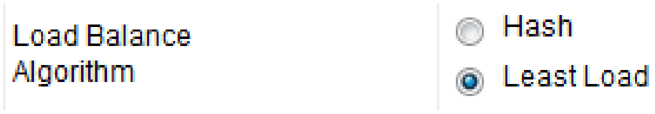
2. ☐	**SOAM VIP GUI**: Configure replication IPFE association data	1. Navigate to **IPFE > Configuration > Options**.  2. Type the IP address of the first IPFE as the **IPFE-A1 IP Address** and the IP address of the second IPFE as the **IPFE-A2 IP Address**. 3. If applicable, type the addresses of the third and fourth IPFE servers as the **IPFE-B1 IP Address** and **IPFE-B2 IP Address**.  **Configuration Options** Variable | Value | Descrip **Inter-IPFE Synchronization** IPFE-A1 IP Address | 169.254.1.11 - ZombieIPFE1 | IPv4 or I This sel IPFE-A2 IP Address | 169.254.1.12 - ZombieIPFE2 | IPv4 or I This sel ***Notes***: - The address should reside on the IMI (Internal Management Interface) network. - IPFE-A1 and IPFE-A2 must have connectivity between each other through these addresses. The same applies with IPFE-B1 and IPFE-B2. - Accept default configuration for remaining entries.
3. ☐	**SOAM VIP GUI**: Configure/Insert IPFE target sets	1. Navigate to **IPFE > Configuration > Target Sets**.  2. Click either **Insert IPv4** or **Insert IPv6**, depending on the IP version of the target set you plan to use.  **Protocols**: Protocols the target set supports.  Protocols ○ TCP only ○ SCTP only ● Both TCP and SCTP **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

Procedure 38. Configure IPFE (Optional)

Delete Age configuration are treated as a new connection and do not automatically go to the same application server.

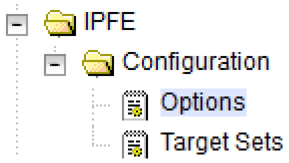
Delete Age * 600

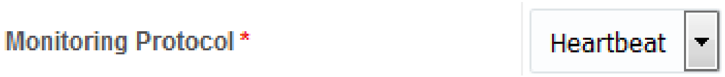
Load Balance Algorithm: Hash or Least Load options.



Load Balance Algorithm ○ Hash ● Least Load

Note: For the IPFE to provide Least Load distribution, navigate to **IPFE > Configuration > Options**. Monitoring protocol must be set to **Heartbeat** so the application servers can provide the load information the IPFE uses to select the **least-loaded** server for connections.





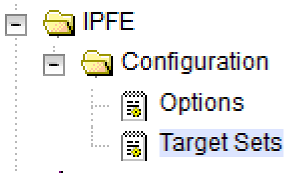
Monitoring Protocol * Heartbeat

Note: The **Least Load** option is default and recommended with exception of unique backward compatibility scenarios.

3. Execute the following command if Hash Load Balance Algorithm was selected above (advise cut and paste to prevent errors):
4. Establish an SSH session to the SOAM VIP and login as **admusr**.

```
$ sudo iset -fvalue="50" DpiOption where
"name='MpEngIngressMpsPercentile'"
=== changed 1 records ===
```

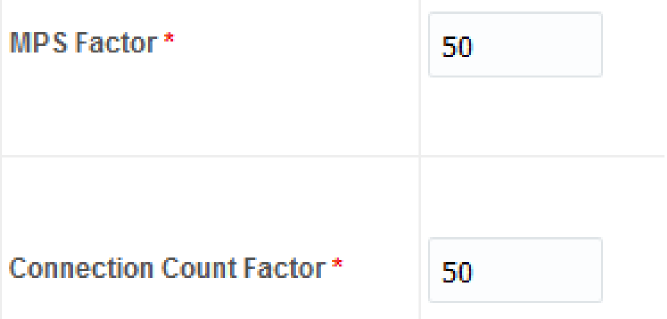
5. Navigate to **IPFE > Configuration > Target Sets**.



6. (Optional) If you have selected the **Least Load**, 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.

Procedure 38. Configure IPFE (Optional)



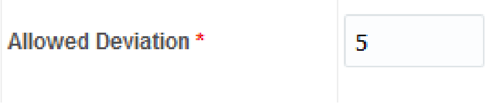
MPS Factor * 50

Connection Count Factor * 50

To configure Reserved Ingress MPS, navigate to **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**.

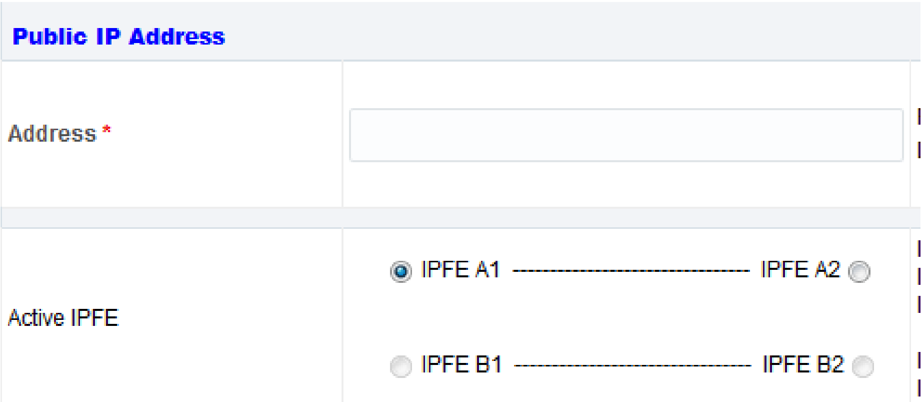
Connection Count Factor: This is the other component of the least load algorithm. This field allows you to set it from **0** (not used in load calculations) to **100** (the only component used for load calculations). Increase this setting if connection storms (the arrival of many connections at a very 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.



Allowed Deviation * 5

Primary Public IP Address: IP address for the target set.



Public IP Address

Address *

Active IPFE

● IPFE A1 ------------------------------ IPFE A2 ○

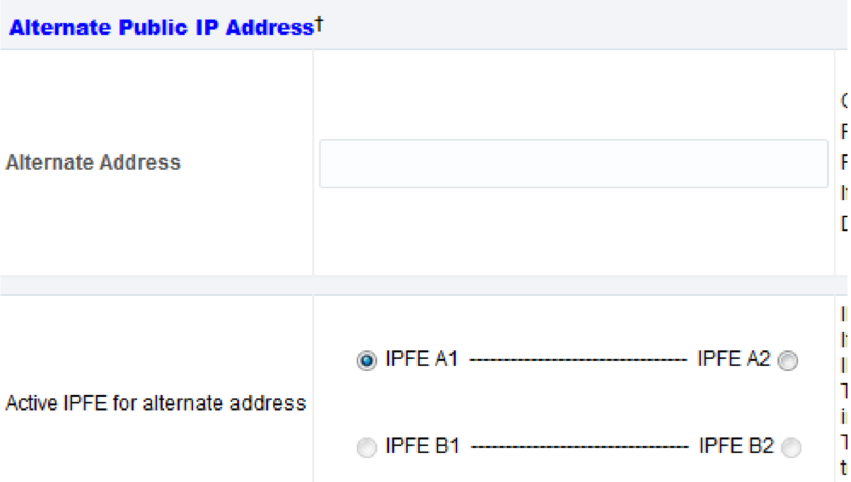
○ IPFE B1 ------------------------------ IPFE B2 ○

Note: This address must reside on the XSI (External Signaling Interface) network because it is 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.

Procedure 38. Configure IPFE (Optional)

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†

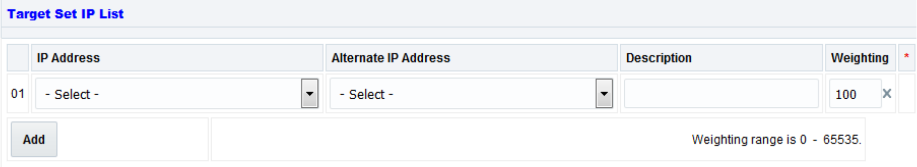
Alternate Address:

Active IPFE for alternate address:
● IPFE A1 ------------------------------ IPFE A2 ○
○ IPFE B1 ------------------------------ IPFE B2 ○

Notes:

- 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.
- 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

	IP Address	Alternate IP Address	Description	Weighting	*
01	- Select -	- Select -		100	×

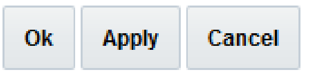
Add

Weighting range is 0 - 65535.

Notes:

- 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.
- If all application servers have an equal weight (for example, 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.

7. Click **Add** to add more application servers (up to 16).
8. Click **Apply**.



Procedure 38. Configure IPFE (Optional)

4. ☐	**SOAM VIP GUI**: Repeat for additional configuration of IPFE target sets	Repeat steps 3. for each target set (up to 16). At least one target set must be configured.

3.15 SDS Application Configuration

3.15.1 NOAM Configuration

Procedure 39. Configure First SDS NOAM NE and Server

This procedure configures the first SDS NOAM network element and 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 ach step number.

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

1.
☐

Save the NOAM network data to an XML file

1. Use a text editor to create a SDS NOAM network element file that describes the networking of the target install environment of your first SDS NOAM server.
2. 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**. For example, a SDS NOAM network element XML file would have a **SDS_NOAM_NetworkElement.xml** filename.

Alternatively, you can update the sample SDS network element file. It can be found on the management server at:

```
/usr/TKLC/smac/html/TPD/<DSR
Release>/upgrade/overlay/SAMPLE-NetworkElement.xml
```

A sample XML file can also be found in Appendix L Sample Network Element.

Note: These 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.

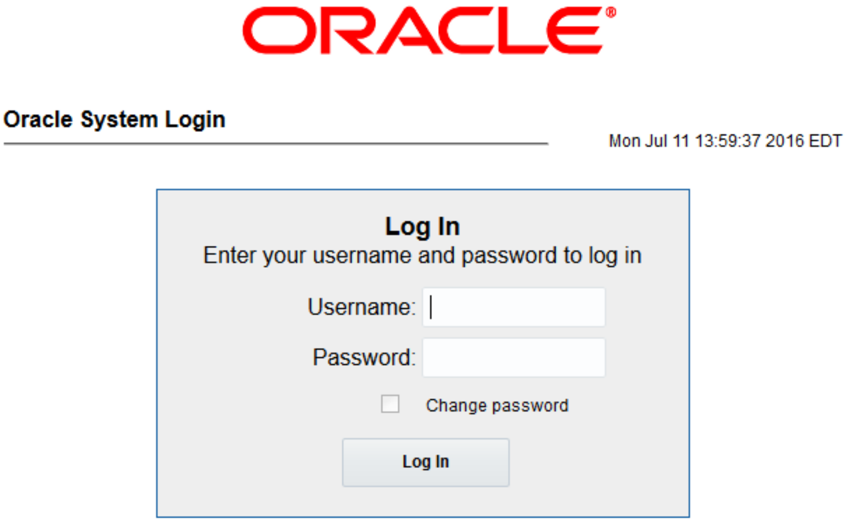
Procedure 39. Configure First SDS NOAM NE and Server

<table>
<tr><td>2.
☐</td><td>SDS NOAM VIP GUI: Login</td><td>

1. Establish a GUI session on the SDS NOAM server by using the VIP IP address of the NOAM server (defined and configured in the DSR fast deployment rms.cfg file). Open the web browser and enter a URL of:

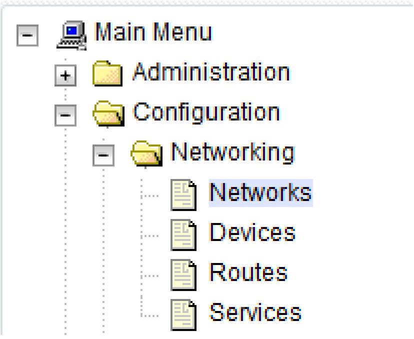
```
https://<Primary_SDS_NOAM_VIP_IP_Address>
```

2. Login as the **guiadmin** user.

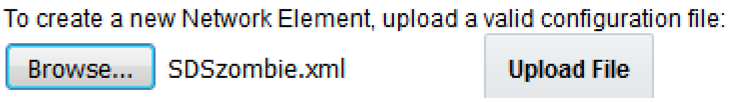

ORACLE
Oracle System Login
Mon Jul 11 13:59:37 2016 EDT
Log In
Enter your username and password to log in
Username:
Password:
Change password
Log In

</td></tr>
<tr><td>3.
☐</td><td>Primary SDS NOAM VIP GUI: Create the SDS NOAM network element using an XML file</td><td>

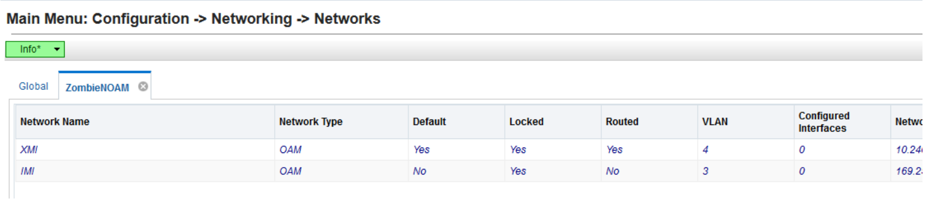
1. Navigate to **Configuration > Networking > Networks**.


Main Menu
Administration
Configuration
Networking
Networks
Devices
Routes
Services

2. Click **Browse** and enter the **Pathname** of the NOAM network XML file.
3. Click **Upload File**.


To create a new Network Element, upload a valid configuration file:
Browse...
Upload File
SDSzombie.xml

4. Click on the tab to display the configured network.


Main Menu: Configuration -> Networking -> Networks
Info*
Global
ZombieNOAM

<table>
<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>Netwo</th></tr>
<tr><td>XMI</td><td>OAM</td><td>Yes</td><td>Yes</td><td>Yes</td><td>4</td><td>0</td><td>10.24</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>169.2</td></tr>
</table>

</td></tr>
</table>

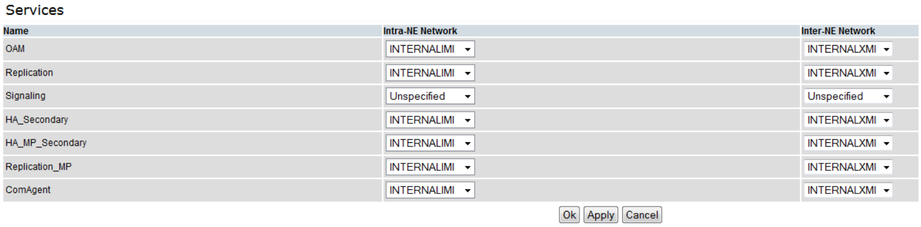
Procedure 39. Configure First SDS NOAM NE and Server

4. ☐ Map services to networks

1. Navigate to **Configuration > Services**.
2. Click **Edit** and set the services as shown in this table.

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 should configure to look like this:



Services

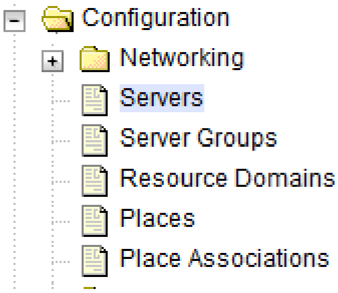
Name	Intra-NE Network	Inter-NE Network
OAM	INTERNALIMI	INTERNALXMI
Replication	INTERNALIMI	INTERNALXMI
Signaling	Unspecified	Unspecified
HA_Secondary	INTERNALIMI	INTERNALXMI
HA_MP_Secondary	INTERNALIMI	INTERNALXMI
Replication_MP	INTERNALIMI	INTERNALXMI
ComAgent	INTERNALIMI	INTERNALXMI

Ok
Apply
Cancel

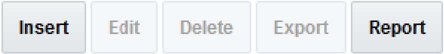
3. Click **OK** to apply the service-to-network selections.

5. ☐ **Primary SDS NOAM VIP GUI**: Insert the 1st SDS NOAM server

1. Navigate to **Configuration > Servers**.


Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

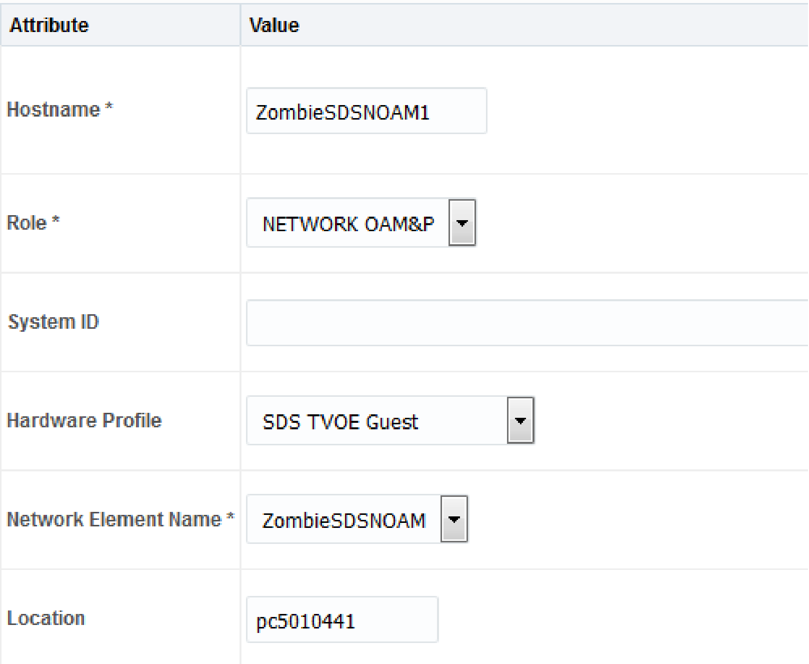
2. Click **Insert** to insert the new SDS NOAM server into the servers table.


Insert
Edit
Delete
Export
Report

3. Enter these values:

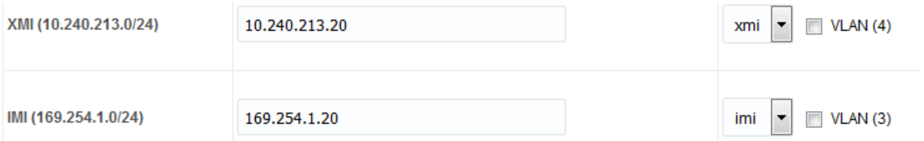
Hostname: <Hostname>
Role: Network OAM
System ID: <Site System ID>
Hardware Profile: SDS TVOE Guest
Network Element Name: [Select NE]
Location: <Enter an optional location description>

Procedure 39. Configure First SDS NOAM NE and Server



Attribute	Value
Hostname *	ZombieSDSNOAM1
Role *	NETWORK OAM&P
System ID	
Hardware Profile	SDS TVOE Guest
Network Element Name *	ZombieSDSNOAM
Location	pc5010441

4. For the **XMI** network, type the server XMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.
5. For the **IMI** network, type the server IMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.



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)

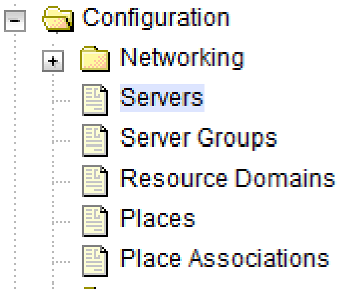
6. Add this NTP server.

NTP Server	Preferred?
<First-SDS-NOAM-TVOE-IP-Address>	Yes

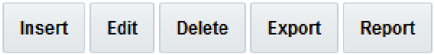
7. Click **OK**.

6. ☐ **SDS NOAM VIP GUI**: Export the initial configuration

1. Navigate to **Configuration > Servers**.


Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. From the GUI screen, select the SDS NOAM server and click **Export** to generate the initial configuration data for that server.


Insert
Edit
Delete
Export
Report

Procedure 39. Configure First SDS NOAM NE and Server

7. ☐	**SDS NOAM VIP GUI**: Copy the configuration file to the 2nd NOAM server	1. Obtain a terminal session to the first NOAM server console and login as **admusr**. 2. Copy the configuration file, created in the previous step, from the **/var/TKLC/db/filemgmt** directory on the first SDS NOAM to the **/var/tmp** directory. The configuration file has a filename like **TKLCConfigData.<hostname>.sh**.

```
$ sudo cp
/var/TKLC/db/filemgmt/TKLCConfigData.RMS01.sh
/var/tmp/TKLCConfigData.sh
```

		The automatic configuration daemon looks for the **TKLCConfigData.sh** file in the **/var/tmp** directory, implements the configuration in the file, and asks the user to reboot the server.
8. ☐	**SDS NOAM iLO**: Wait for configuration to complete	Wait to be prompted to reboot the server, but DO NOT reboot the server, it is rebooted later in this procedure. ***Note:*** Ignore the warning about removing the USB key, since no USB key is present.
9. ☐	**SDS NOAM iLO**: Set the time zone and reboot the server	***Note:*** Valid time zones can be found in Appendix J List of Frequently Used Time Zones. 1. Run:

```
$ sudo set_pmac_tz.pl <time zone>
```

Example:

```
$ sudo set_pmac_tz.pl America/New_York
```

2. Reboot the server.

```
$ sudo init 6
```

10. ☐	**MP Server**: Verify server health	Login as **admusr** to the first SDS NOAM server and make sure no errors are returned.

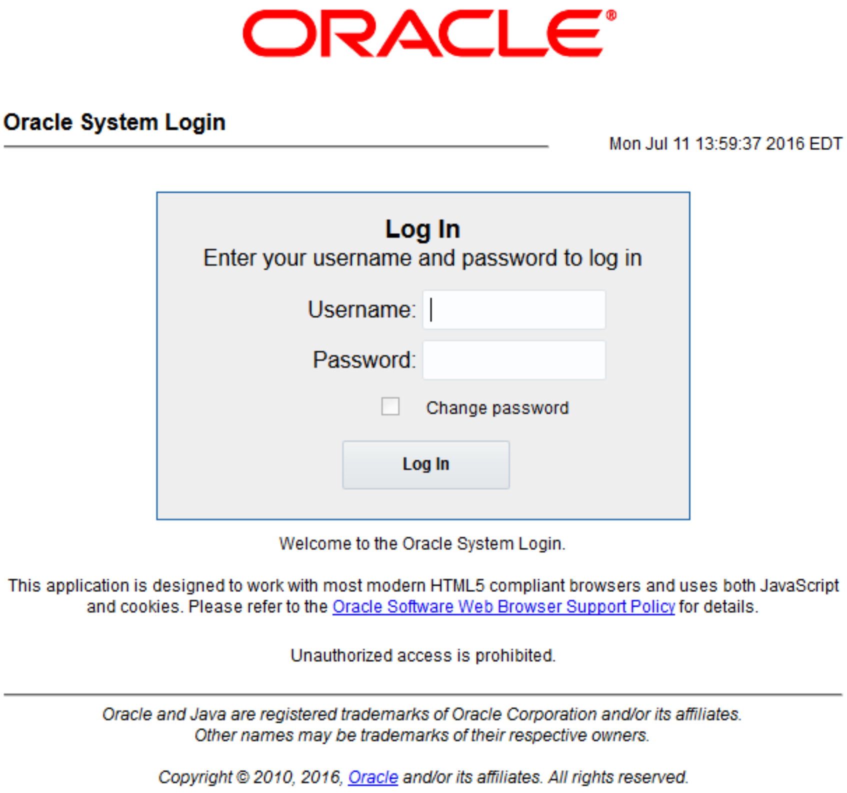
```
$ sudo syscheck
Running modules in class hardware…OK
Running modules in class disk…OK
Running modules in class net…OK
Running modules in class system…OK
Running modules in class proc…OK
LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

Procedure 40. Configure the SDS NOAM Server Group

This procedure configures the SDS NOAM server group.

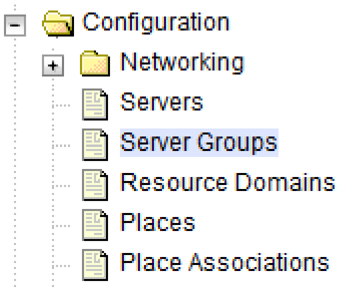
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.

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

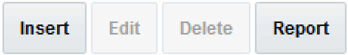
1. ☐	**SDS NOAM VIP GUI**: Login	1. Establish a GUI session on the first SDS NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_SDS_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

Procedure 40. Configure the SDS NOAM Server Group

<table>
<tr>
<td>2.
☐</td>
<td>SDS NOAM GUI: Enter the NOAM server group data</td>
<td>
1. Navigate to Configuration > Server Groups.

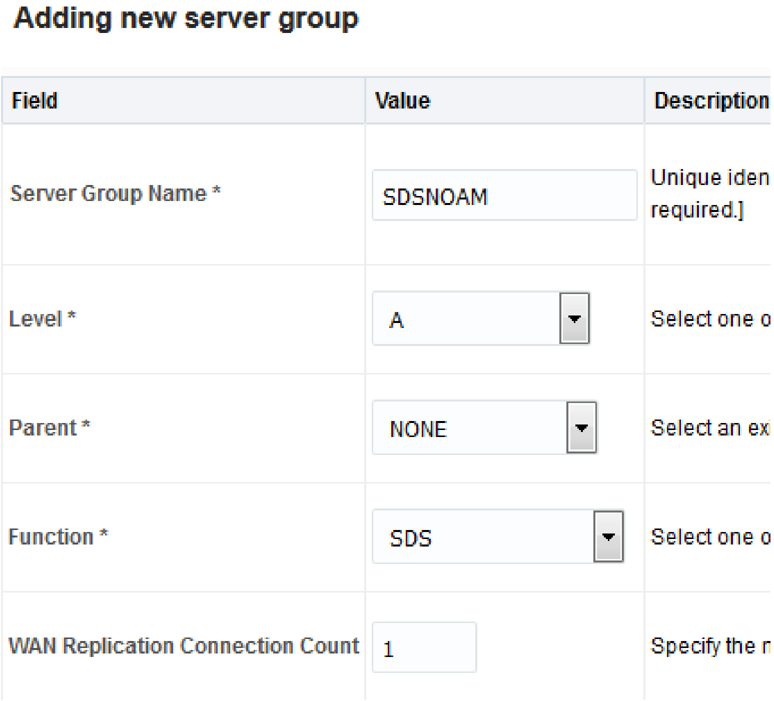

Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Click Insert.


Insert
Edit
Delete
Report

3. Enter these values:

Server Group Name: <Server Group Name>
Level: A
Parent: None
Function: SDS
WAN Replication Connection Count: Use Default Value

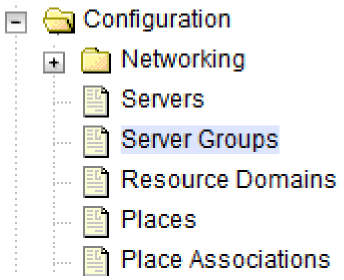
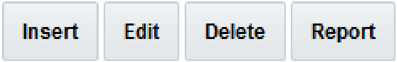
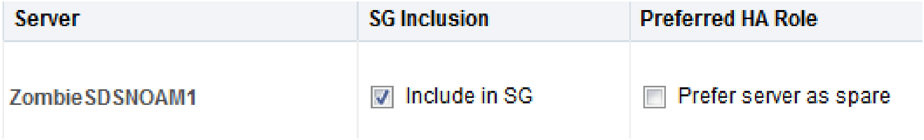
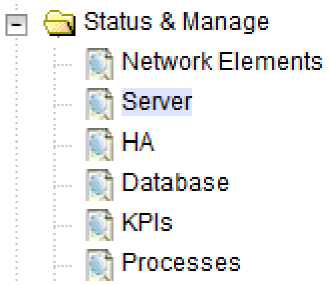
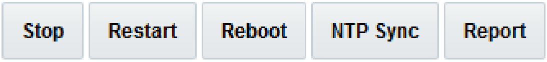
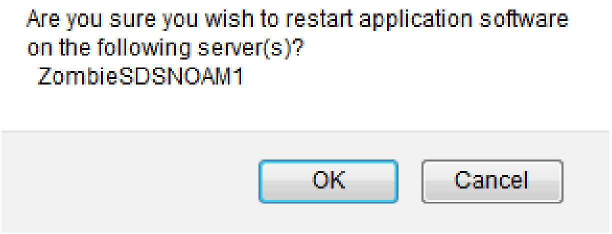


Adding new server group

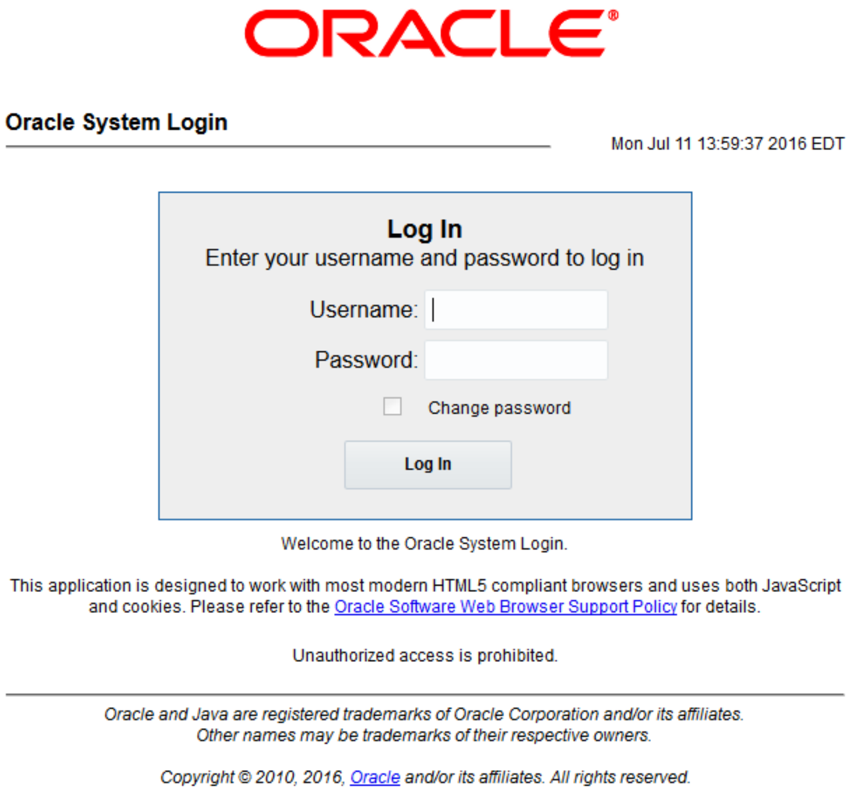
<table>
<tr><th>Field</th><th>Value</th><th>Description</th></tr>
<tr><td>Server Group Name *</td><td>SDSNOAM</td><td>Unique iden
required.]</td></tr>
<tr><td>Level *</td><td>A</td><td>Select one o</td></tr>
<tr><td>Parent *</td><td>NONE</td><td>Select an ex</td></tr>
<tr><td>Function *</td><td>SDS</td><td>Select one o</td></tr>
<tr><td>WAN Replication Connection Count</td><td>1</td><td>Specify the r</td></tr>
</table>

4. Click OK.
</td>
</tr>
</table>

Procedure 40. Configure the SDS NOAM Server Group

3. ☐	**SDS NOAM GUI**: Edit the SDS NOAM server group	1. Navigate to **Configuration > Server Groups**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Select the new server group and click **Edit**.  Insert Edit Delete Report 3. Select the network element that represents the SDS NOAM. 4. Mark the **Include in SG** checkbox for the SDS NOAM server. 5. Leave other checkboxes blank.  Server: ZombieSDSNOAM1 SG Inclusion: ☑ Include in SG Preferred HA Role: ☐ Prefer server as spare 6. Click **OK**.
4. ☐	**Primary SDS NOAM VIP GUI**: Restart the 1st SDS NOAM servers	1. From the SDS NOAM GUI, navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the first SDS NOAM server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm.  Are you sure you wish to restart application software on the following server(s)? ZombieSDSNOAM1 .

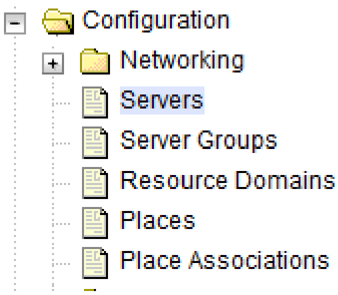
Procedure 41. Configure Second SDS NOAM Server

This procedure configures the second SDS NOAM server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**SDS NOAM VIP GUI**: Login	1. Establish a GUI session on the first 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>` 2. Login as the **guiadmin** user.  **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password 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.*

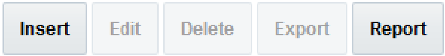
Procedure 41. Configure Second SDS NOAM Server

2. ☐ **SDS NOAM VIP GUI**: Insert the 2nd SDS NOAM server

1. Navigate to **Configuration > Servers**.

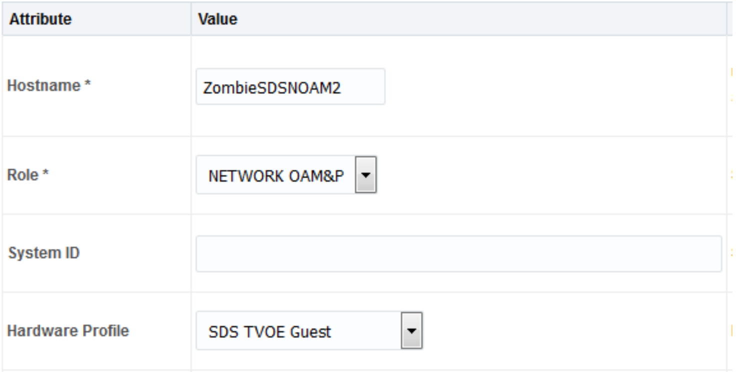

Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Click **Insert** to insert the second SDS NOAM server into the servers table.


Insert
Edit
Delete
Export
Report

3. Enter these values:

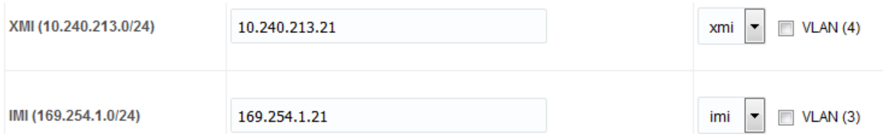
Hostname:	<Hostname>
Role:	Network OAM
System ID:	<Site System ID>
Hardware Profile:	SDS TVOE Guest
Network Element Name:	[Select NE]
Location:	<Enter an optional location description>



Attribute	Value
Hostname *	ZombieSDSNOAM2
Role *	NETWORK OAM&P
System ID	
Hardware Profile	SDS TVOE Guest

4. For the **XMI** network, type the server XMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.

5. For the **IMI** network, type the server IMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.



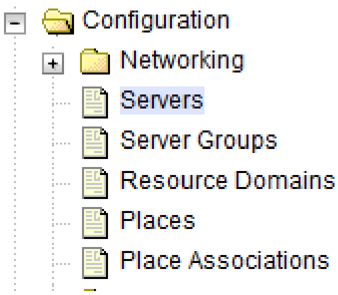
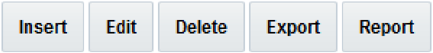
XMI (10.240.213.0/24)	10.240.213.21	xmi	☐ VLAN (4)
IMI (169.254.1.0/24)	169.254.1.21	imi	☐ VLAN (3)

6. Add this NTP server.

NTP Server	Preferred?
<Second-SDS NOAM-TVOE-IP-Address>	Yes

7. Click **OK**.

Procedure 41. Configure Second SDS NOAM Server

3. ☐	**SDS NOAM VIP GUI**: Export the initial configuration	1. Navigate to **Configuration > Servers**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. From the GUI screen, select the SDS NOAM server and click **Export** to generate the initial configuration data for that server. 
4. ☐	**1st SDS NOAM VIP GUI**: Copy the configuration file to the 2nd NOAM server	1. Obtain a terminal session to the first NOAM server console and login as **admusr**. 2. Configure the second NOAM server. `$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<NOAM2_Hostname>.sh admusr@<NOAM2_xmi_IP_address>:/var/tmp/TKLCConfigData.sh` The automatic configuration daemon looks for the **TKLCConfigData.sh** file in the **/var/tmp** directory, implements the configuration in the file, and asks the user to reboot the server.

5.
☐
	2nd SDS DR NOAM Server: Verify server configuration was called and reboot the configured server	1. Verify server configuration was called by checking the log file.
		`$ sudo cat /var/TKLC/appw/logs/Process/install.log`
		Verify this message displays:
		`[SUCCESS] script completed successfully!`
		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.
		2. Reboot the server.
		`$ sudo init 6`
		3. Proceed to the next step once the server finishes rebooting. The server is done rebooting once the login prompt displays.

Procedure 41. Configure Second SDS NOAM Server

6. ☐	**2nd SDS NOAM Server**: Verify server health	Login as **admusr** to the second SDS NOAM server and make sure no errors are returned.

```
$ 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
```

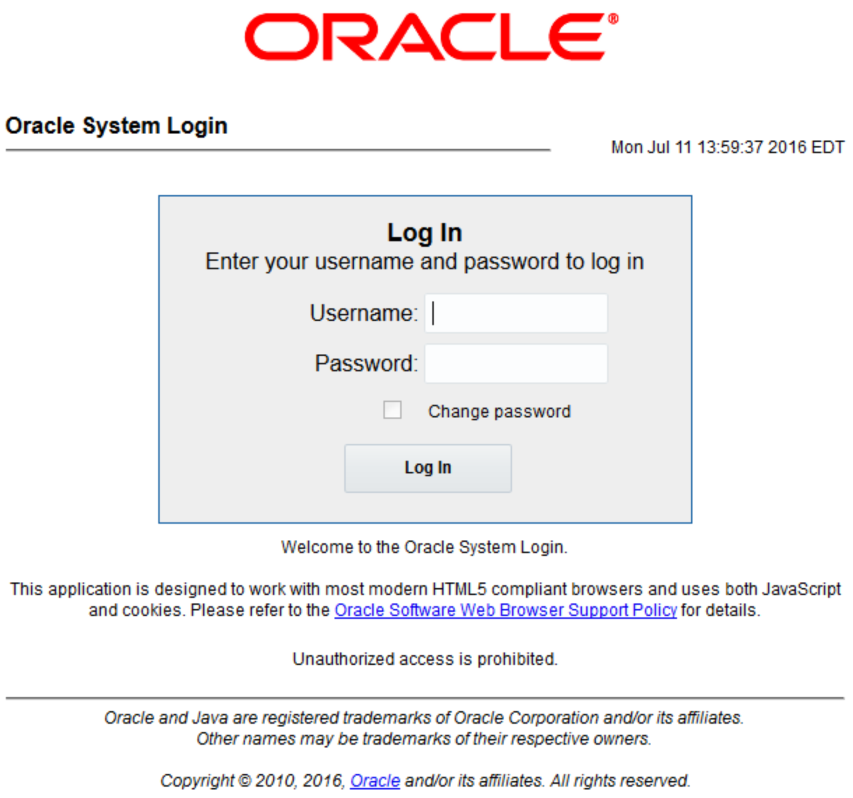
Procedure 42. Complete SDS NOAM Server Group Configuration

This procedure finishes configuration for the SDS NOAM server group.

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

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

1. ☐	**SDS NOAM VIP GUI**: Login	1. Establish a GUI session on the first 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>` 2. Login as the **guiadmin** user.



ORACLE®

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.

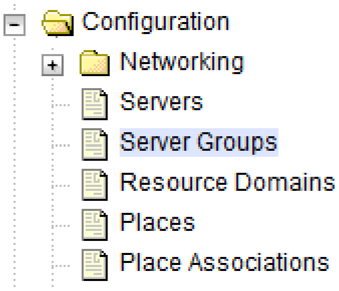
Unauthorized access is prohibited.

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 42. Complete SDS NOAM Server Group Configuration

<table>
<tr>
<td>2.
☐</td>
<td>**SDS NOAM VIP GUI**: Edit server group and VIP</td>
<td>
1. Navigate to **Configuration > Server Groups**.

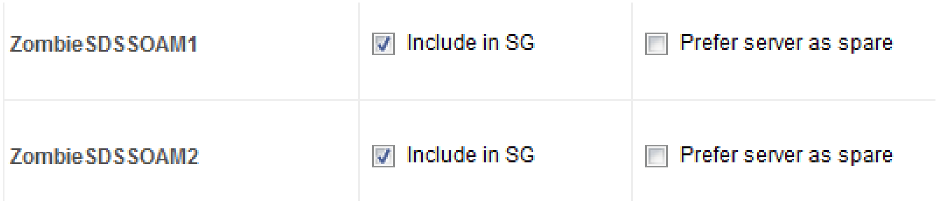

Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Select the server group you just created and click **Edit**.

Insert
Edit
Delete
Report

3. Add the second SDS NOAM server to the server group by marking the **Include in SG** checkbox for the second SDS NOAM server.

Do **not** mark any of the **Preferred Spare** checkboxes.



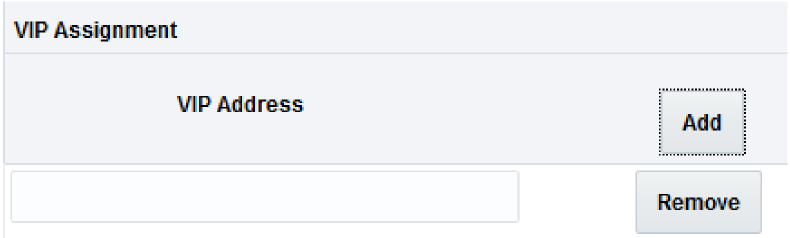
ZombieSDSSOAM1 ☑ Include in SG ☐ Prefer server as spare

ZombieSDSSOAM2 ☑ Include in SG ☐ Prefer server as spare

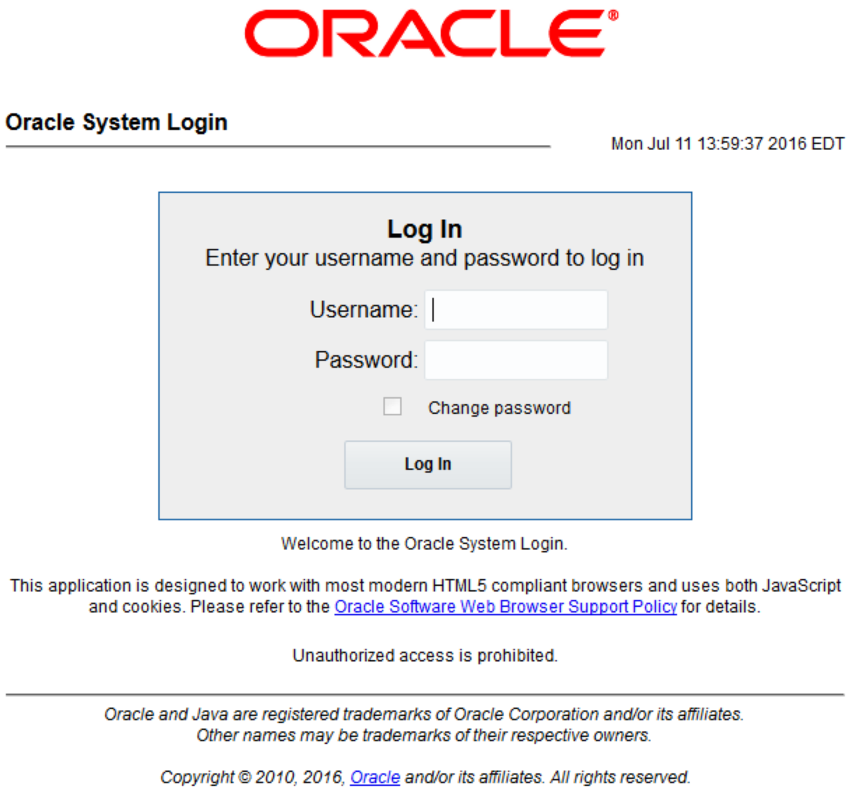
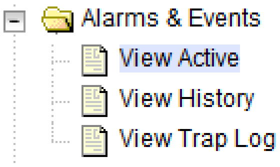
4. Click **Apply**.

5. Click **Add**.

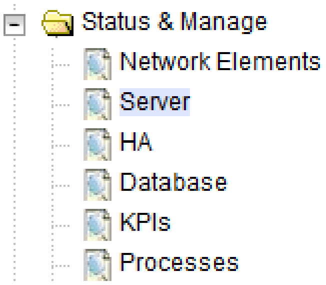
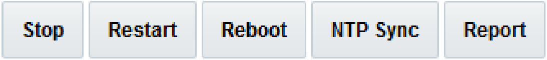
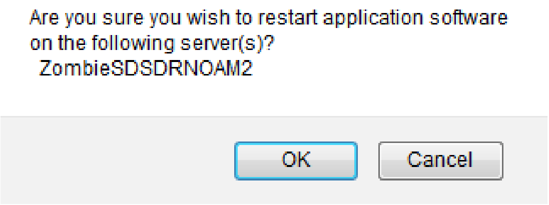
6. Type the **VIP Address** and click **OK**.


VIP Assignment
VIP Address
Add
Remove
</td>
</tr>
</table>

Procedure 42. Complete SDS NOAM Server Group Configuration

3. ☐	**SDS NOAM VIP GUI**: Login	1. Establish a GUI session on the first 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>` 2. Login as the **guiadmin** user.  Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.
4. ☐	**SDS NOAM VIP GUI**: Wait for remote database alarm to clear	Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding. Monitor progress by navigating to **Alarms & Events > View Active**.  Alarms & Events View Active View History View Trap Log

Procedure 42. Complete SDS NOAM Server Group Configuration

5. ☐	**SDS NOAM VIP GUI**: Restart the 2nd SDS NOAM server	1. From the SDS NOAM GUI, navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the second SDS NOAM server and click **Restart**.  3. Click **OK** to confirm.  Are you sure you wish to restart application software on the following server(s)? ZombieSDSDRNOAM2

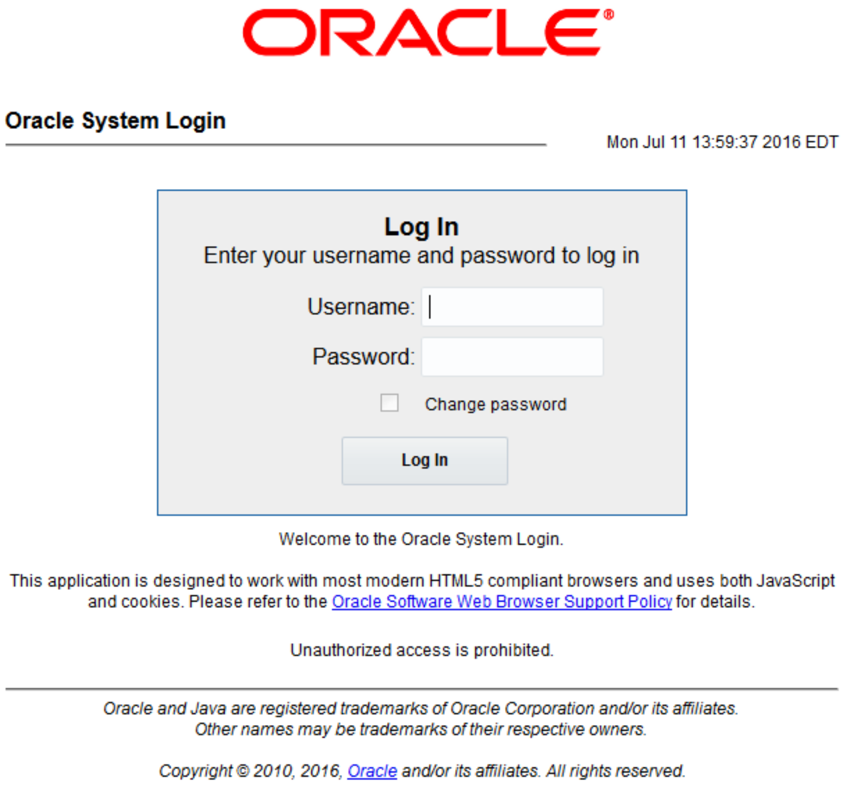
3.15.2 NetBackup Client Installation (Optional)

Procedure 43. Install NetBackup Client (Optional)

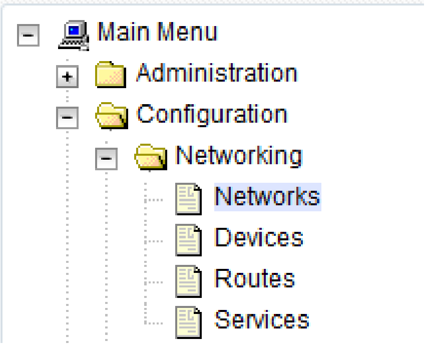
This procedure downloads and installs the NetBackup client software on the server Location of the bpstart_notify and bpend_notify scripts is required for the execution of this procedure. For Appworks-based applications, the scripts are located as follows: • /usr/TKLC/appworks/sbin/bpstart_notify • /usr/TKLC/appworks/sbin/bpend_notify Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact 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 using TPD tools (push configuration), then use Appendix I.2 Install NetBackup Client Using NBAutoInstall. ***Note:*** This is not common. If the answer to the previous question is not known, then use Appendix I.1 Install NetBackup Client Using platcfg.
2. ☐	Install NetBackup Client Software	Choose the same method used in step 1. to install NetBackup on the 2nd NOAM.

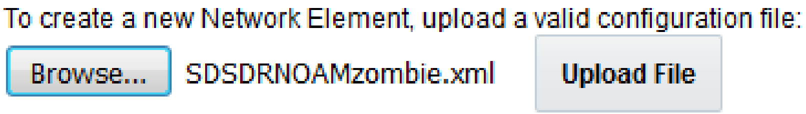
3.15.3 Disaster Recovery NOAM (Optional)

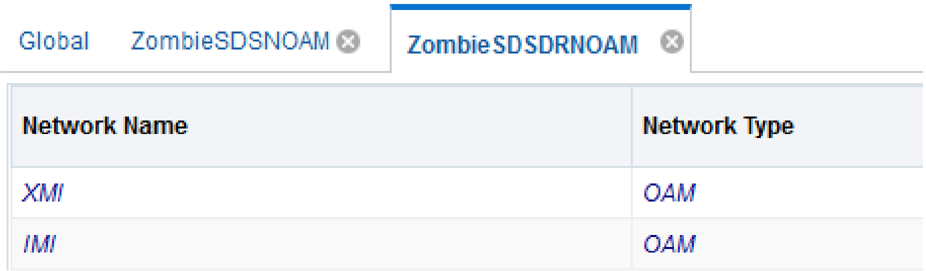
Procedure 44. Configure SDS NOAM for DR Site (Optional)

<table>
<tr><td colspan="3">This procedure configures the first DR NOAM server.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>Primary SDS NOAM VIP GUI: Login</td><td>1. Establish a GUI session on the first 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>
2. Login as the guiadmin user.

Oracle System Login
Mon Jul 11 13:59:37 2016 EDT
Log In
Enter your username and password to log in
Username:
Password:
☐ Change password
Log In
Welcome to the Oracle System Login.
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.
Unauthorized access is prohibited.
<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></td></tr>
</table>

Procedure 44. Configure SDS NOAM for DR Site (Optional)

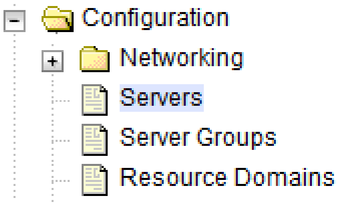
<table>
<tr>
<td>2.
☐</td>
<td>Primary SDS NOAM VIP GUI: Create the SDS DR NOAM network element using an XML file</td>
<td>
1. Navigate to Configuration > Networking > Networks.

Main Menu
Administration
Configuration
Networking
Networks
Devices
Routes
Services

2. Click Browse and enter the Pathname of the DR NOAM network XML file.
3. Click Upload File.

To create a new Network Element, upload a valid configuration file:
SDSDRNOAMzombie.xml
Browse...
Upload File

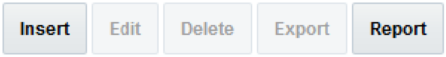
4. Click on the tab to display the configured network.

Global
ZombieSDSNOAM
ZombieSDSDRNOAM
<table>
<tr><th>Network Name</th><th>Network Type</th></tr>
<tr><td>XMI</td><td>OAM</td></tr>
<tr><td>IMI</td><td>OAM</td></tr>
</table>
</td>
</tr>
</table>

3. ☐ **Primary SDS NOAM VIP GUI**: Insert the 1st SDS DR NOAM server

1. Navigate to **Configuration > Servers**.

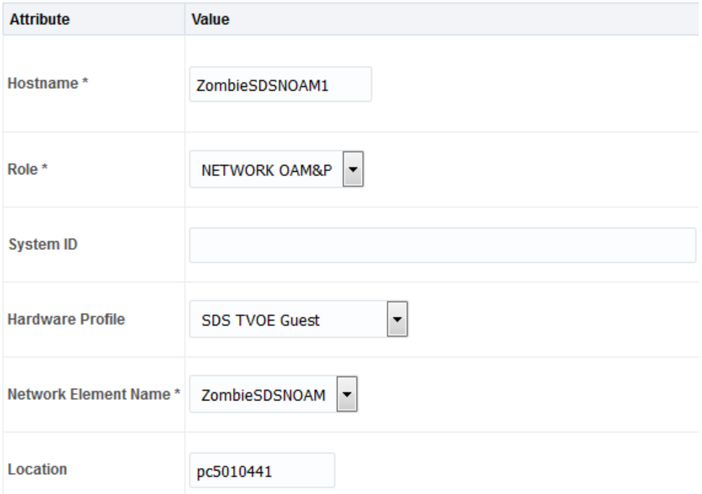

Configuration
Networking
Servers
Server Groups
Resource Domains

2. Click **Insert** to insert the first SDS DR NOAM server into the servers table.


Insert
Edit
Delete
Export
Report

3. Enter these values:

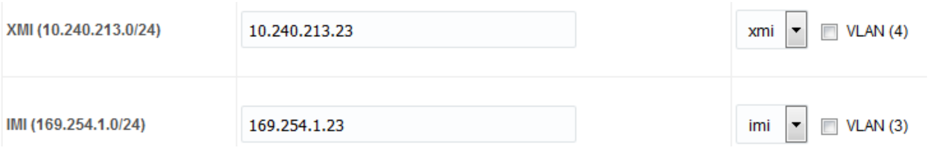
Hostname:	<Hostname>
Role:	Network OAM
System ID:	<Site System ID>
Hardware Profile:	SDS TVOE Guest
Network Element Name:	[Select NE]
Location:	<Enter an optional location description>



Attribute	Value
Hostname *	ZombieSDSNOAM1
Role *	NETWORK OAM&P
System ID	
Hardware Profile	SDS TVOE Guest
Network Element Name *	ZombieSDSNOAM
Location	pc5010441

4. For the **XMI** network, type the server XMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.

5. For the **IMI** network, type the server IMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.



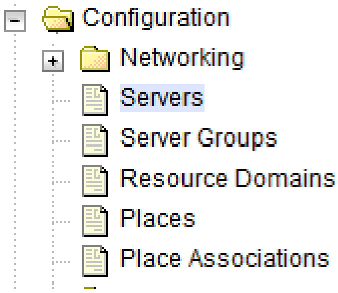
XMI (10.240.213.0/24) 10.240.213.23 xmi ☐ VLAN (4)
IMI (169.254.1.0/24) 169.254.1.23 imi ☐ VLAN (3)

6. Add this NTP server.

NTP Server	Preferred?
<First-SDS-DR NOAM-RMS-TVOE-IP-Address>	Yes

7. Click **OK**.

Procedure 44. Configure SDS NOAM for DR Site (Optional)

4. ☐	**Primary SDS NOAM VIP GUI**: Export the initial configuration	1. Navigate to **Configuration > Servers**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. From the GUI screen, select the SDS DR NOAM server and click **Export** to generate the initial configuration data for that server. Insert Edit Delete Export Report
5. ☐	**Primary SDS NOAM VIP GUI**: Copy the configuration file to the DR NOAM server	1. Obtain a terminal session to the primary NOAM server console and login as **admusr**. 2. Configure the first DR NOAM server. `$ sudo scp -r /var/TKLC/db/filemgmt/TKLCConfigData.<DRNOAM1_Hostname>.sh admusr@<DRNOAM1_xmi_IP_address>:/var/tmp/TKLCConfigData.sh` The automatic configuration daemon looks for the **TKLCConfigData.sh** file in the **/var/tmp** directory, implements the configuration in the file, and asks the user to reboot the server.

6.
☐
	1st **SDS DR NOAM Server**: Verify server configuration was called and reboot the configured server	1. Verify server configuration was called by checking the log file.
		`$ sudo cat /var/TKLC/appw/logs/Process/install.log`
		Verify this message displays:
		`[SUCCESS] script completed successfully!`
		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.
		2. Reboot the server.
		`$ sudo init 6`
		3. Proceed to the next step once the server finishes rebooting. The server is done rebooting once the login prompt displays.

Procedure 44. Configure SDS NOAM for DR Site (Optional)

7. ☐	1st **SDS DR NOAM Server**: Verify server health	Login as **admusr** to the first SDS DR NOAM server and make sure no errors are returned.

```
$ 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
```

8. ☐	Repeat for 2nd SDS DR NOAM server	Repeat steps 3. through 7. to configure second SDS DR NOAM server. When inserting the second SDS DR NOAM server, change the NTP server address to this:

NTP Server	Preferred?
<2nd SDS DR NOAM-RMS-TVOE-IP-Address>	Yes

Procedure 45. Pairing for SDS DR NOAM Site (Optional)

This procedure pairs the SDS DR NOAM site.

Prerequisite: The SDS DR NOAM site has been installed.

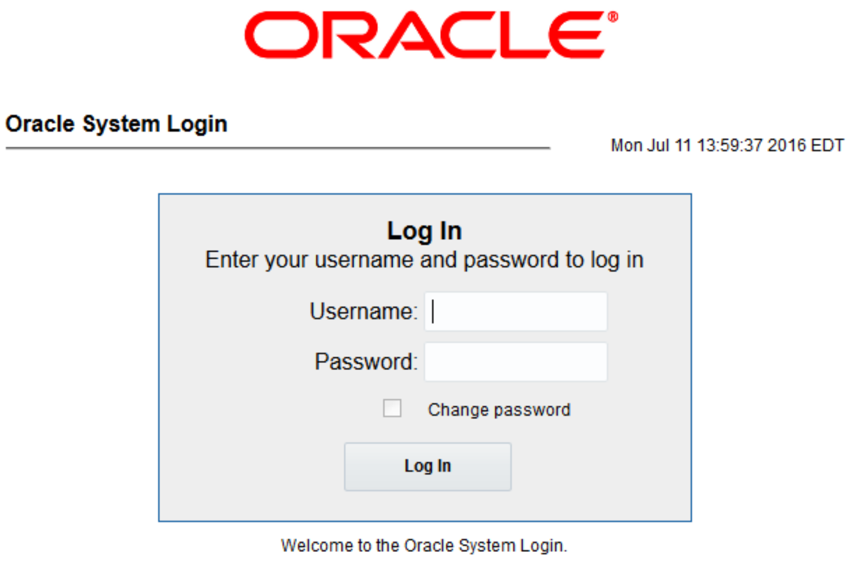
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.

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

1. ☐	**SDS NOAM VIP GUI**: Login	1. Establish a GUI session on the first 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>
```

2. Login as the **guiadmin** user.



Oracle System Login

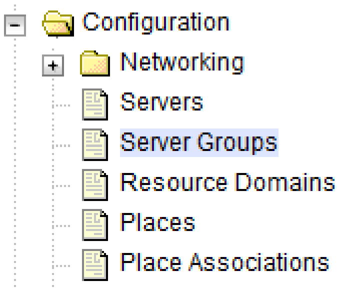
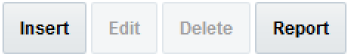
Mon Jul 11 13:59:37 2016 EDT

Log In

Enter your username and password to log in

Welcome to the Oracle System Login.

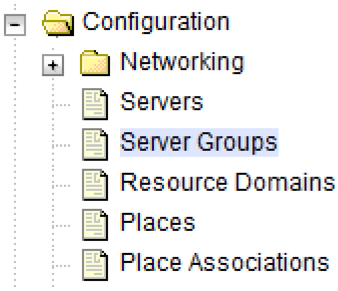
Procedure 45. Pairing for SDS DR NOAM Site (Optional)

2. ☐	**Primary SDS NOAM VIP GUI**: Enter SDS DR NOAM server group data	1. Navigate to **Configuration > Server Groups**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Click **Insert**.  Insert Edit Delete Report 3. Enter these values: **Server Group Name**: <Server Group Name> **Level**: A **Parent**: None **Function**: SDS **WAN Replication Connection Count**: Use Default Value 4. Click **OK**.

Procedure 45. Pairing for SDS DR NOAM Site (Optional)

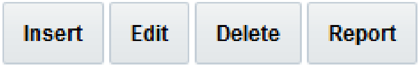
<table>
<tr>
<td>3.
☐</td>
<td>Primary SDS NOAM VIP GUI: Edit server group and VIP</td>
<td>

1. Navigate to **Configuration > Server Groups**.



Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

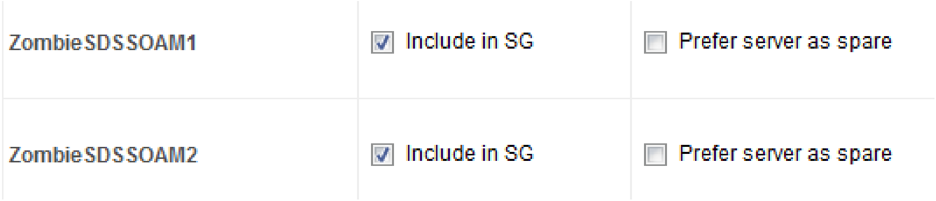
2. Select the server group you just created and click **Edit**.



Insert
Edit
Delete
Report

3. Add both SDS DR NOAM servers to the server group primary site by marking the **Include in SG** checkbox for each SDS DR server.

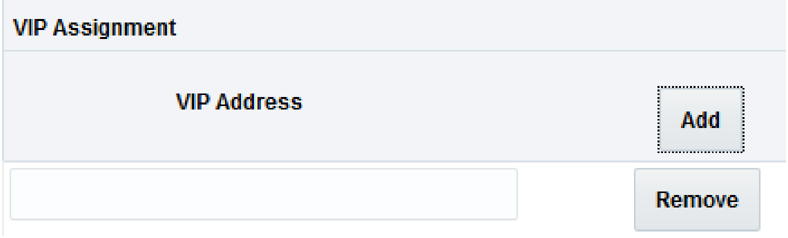
   Do **not** mark any of the **Preferred Spare** checkboxes.



ZombieSDSSOAM1 ☑ Include in SG ☐ Prefer server as spare

ZombieSDSSOAM2 ☑ Include in SG ☐ Prefer server as spare

4. Click **Apply**.
5. Click **Add**.
6. Type the **VIP Address** and click **OK**.

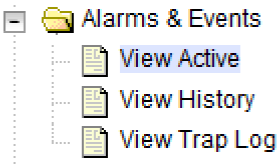


VIP Assignment
VIP Address
Add
Remove

</td>
</tr>
<tr>
<td>4.
☐</td>
<td>Primary SDS NOAM VIP GUI: Wait for remote database alarm to clear</td>
<td>

Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding.

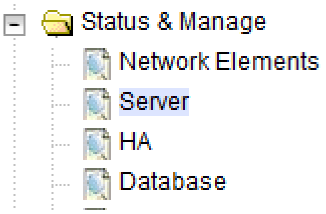
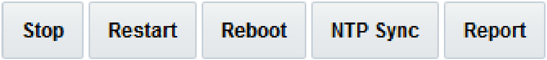
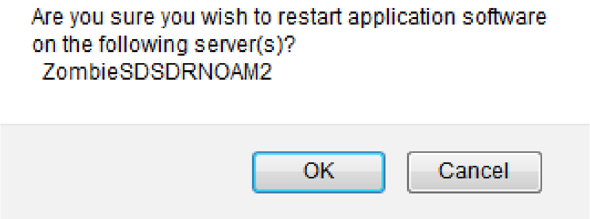
Monitor progress by navigating to **Alarms & Events > View Active**.



Alarms & Events
View Active
View History
View Trap Log

</td>
</tr>
</table>

Procedure 45. Pairing for SDS DR NOAM Site (Optional)

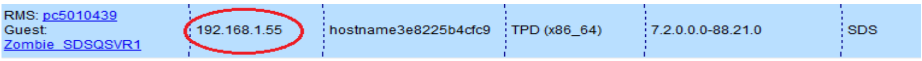
5. ☐	**Primary SDS NOAM VIP GUI**: Restart the SDS DR NOAM servers	1. From the SDS NOAM GUI, navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database 2. Select the first SDS DR NOAM server and click **Restart**.  3. Click **OK** to confirm.  Are you sure you wish to restart application software on the following server(s)? ZombieSDSDRNOAM2 4. Repeat this step selecting the second SDS DR NOAM server.

3.15.4 Query Server Configuration

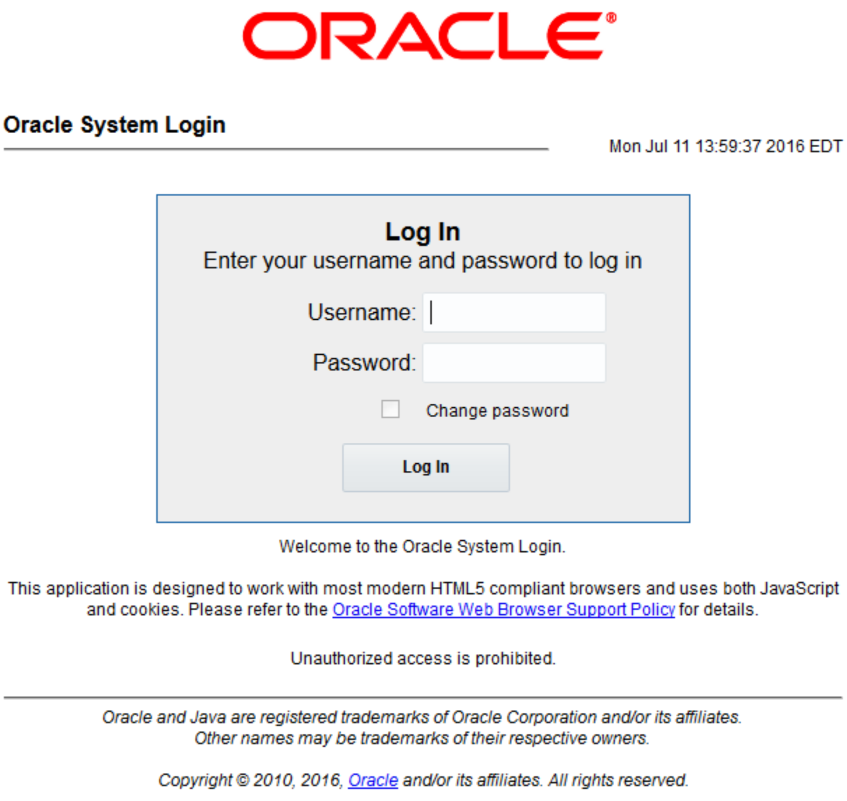
Various errors may display at different stages of this procedure. Ignore errors related to values other than the errors referenced in a specific step.

Procedure 46. Configure SDS Query Server

This procedure configures SDS query server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**PMAC**: Exchange SSH keys between SOAM site's local PMAC and the query server	1. 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 **Software > Software Inventory**.  RMS: pc5010439 Guest: Zombie_SDSQSVR1 | 192.168.1.55 | hostname3e8225b4cfc9 | TPD (x86_64) | 7.2.0.0.0-88.21.0 | SDS 2. Note the **IP address** for the query server. 3. Obtain a terminal session to PMAC and login as **admusr**. 4. Exchange SSH keys for admusr between the PMAC and the query server using the keyexchange utility and control network IP address for the query server. `$ keyexchange admusr@<Query_Server_Control_IP Address>` 5. Enter the password for the admusr user of the SOAM server.

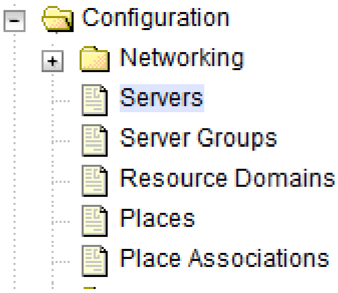
Procedure 46. Configure SDS Query Server

2. ☐	**SDS NOAM VIP GUI**: Login	1. Establish a GUI session on the first 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>` 2. Login as the **guiadmin** user.  Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in 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.*

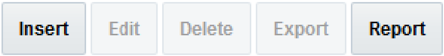
Procedure 46. Configure SDS Query Server

<table>
<tr>
<td>3.
☐</td>
<td>**SDS SOAM VIP GUI**: Insert the SDS DP SOAM server</td>
<td>

1. Navigate to **Configuration > Servers**.


Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Click **Insert** to insert the new SDS query server into the servers table.

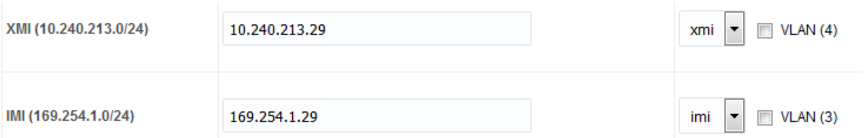

Insert
Edit
Delete
Export
Report

3. Enter these values:

Hostname:	<Hostname>
Role:	Query server
System ID:	<Site System ID>
Hardware Profile:	SDS TVOE Guest
Network Element Name:	[Select NE]

4. For the **XMI** network, type the server XMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.

5. For the **IMI** network, type the server IMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.



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)

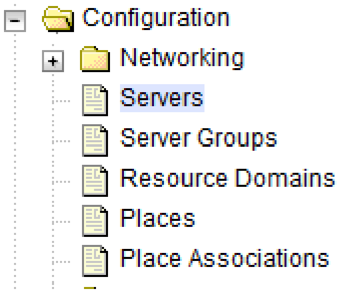
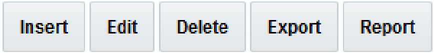
6. Add this NTP server.

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

7. Click **OK**.

</td>
</tr>
</table>

Procedure 46. Configure SDS Query Server

4. ☐	**SDS NOAM VIP GUI**: Export the initial configuration	1. Navigate to **Configuration > Servers**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. From the GUI screen, select the query server and click **Export** to generate the initial configuration data for that server.  Insert Edit Delete Export Report
5. ☐	**SDS NOAM VIP GUI**: Copy configuration file to 1st query server	1. Obtain a terminal session to the SDS NOAM VIP as the **admusr** user. 2. Use the **awpushcf**g utility to copy the configuration file, created in the previous step from the **/var/TKLC/db/filemgmt** directory on the SDS NOAM to the query server, using the control network IP address for the query server. The configuration file has a filename like **TKLCConfigData.<hostname>.sh**. `$ sudo awpushcfg` The awpushcfg utility is interactive, so the user is asked 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 46. Configure SDS Query Server

6.
☐
	Query Server: Verify awpushcfg was called and reboot the configured server	1. Obtain a terminal session to the query server console by establishing an ssh session from the SDS NOAM VIP terminal console.
		`$ ssh admusr@<Query_Server_Control_IP>`
		2. Login as **admusr**.
		The automatic configuration daemon looks for the **TKLCConfigData.sh** file in the **/var/tmp** directory, implements the configuration in the file, and asks the user to reboot the server.
		3. Verify awpushcfg was called by checking the log file.
		`$ sudo cat /var/TKLC/appw/logs/Process/install.log`
		Verify this message displays:
		`[SUCCESS] script completed successfully!`
		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.
		4. Reboot the server.
		`$ sudo init 6`
		5. Proceed to the next step once the server finishes rebooting. The server is done rebooting once the login prompt is displayed.

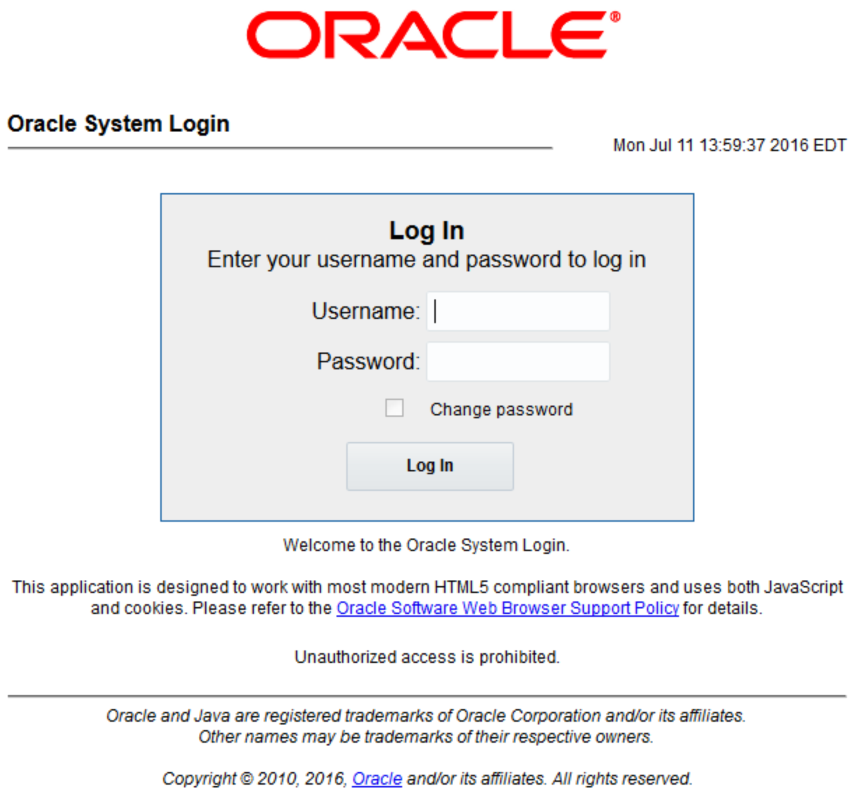
7.
☐
	Query Server: Verify server health	Login as **admusr** to the query server and make sure no errors are returned.
		`$ sudo syscheck`
		`Running modules in class hardware…OK`
		`Running modules in class disk…OK`
		`Running modules in class net…OK`
		`Running modules in class system…OK`
		`Running modules in class proc…OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

Procedure 47. Pair SDS Query Server with SDS NOAMs

This procedure pairs SDS query servers with SDS NOAMs.

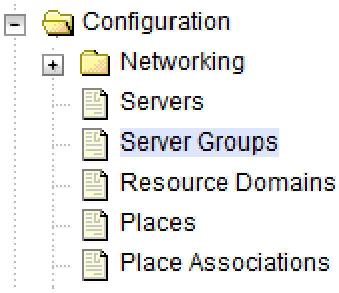
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.

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

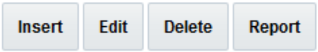
1. ☐	**SDS NOAM VIP GUI**: Login	1. Establish a GUI session on the first SDS NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_SDS_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  ORACLE® **Oracle System Login** Mon Jul 11 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 47. Pair SDS Query Server with SDS NOAMs

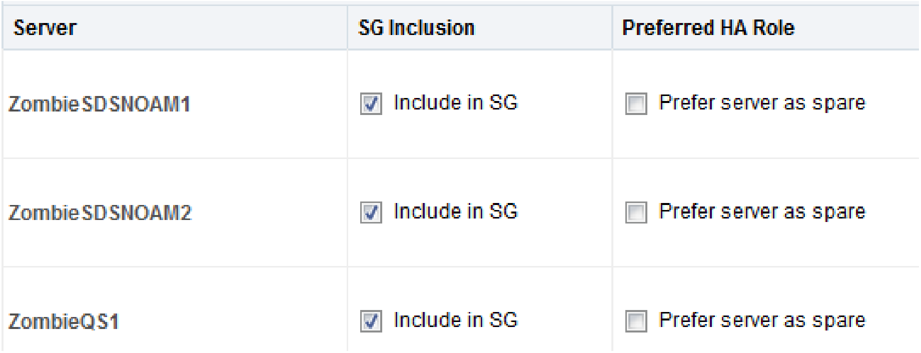
<table>
<tr>
<td>2.
☐</td>
<td>SDS NOAM VIP GUI: Edit the SDS NOAM server group data</td>
<td>
1. Navigate to Configuration > Server Groups.


Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Select the SDS NOAM server group and click Edit.


Insert
Edit
Delete
Report

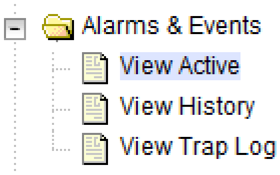
3. Mark the Include in SG checkbox for the query server to add it to the server group.



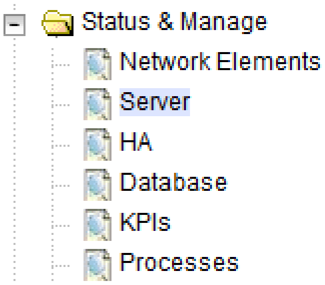
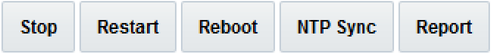
<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<tr><td>ZombieSDSNOAM1</td><td>☑ Include in SG</td><td>☐ Prefer server as spare</td></tr>
<tr><td>ZombieSDSNOAM2</td><td>☑ Include in SG</td><td>☐ Prefer server as spare</td></tr>
<tr><td>ZombieQS1</td><td>☑ Include in SG</td><td>☐ Prefer server as spare</td></tr>
</table>

4. Click OK.
</td>
</tr>
<tr>
<td>3.
☐</td>
<td>SDS NOAM VIP GUI: Wait for remote database alarm to clear</td>
<td>
Wait for the Remote Database re-initialization in progress alarm to clear before proceeding.

Monitor progress by navigating to Alarms & Events > View Active.


Alarms & Events
View Active
View History
View Trap Log
</td>
</tr>
</table>

Procedure 47. Pair SDS Query Server with SDS NOAMs

4. ☐	**SDS NOAM VIP GUI**: Restart query server	1. Navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the query server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm. Wait for the restart successful message.
5. ☐	Repeat for SDS DR NOAM	If SDS DR NOAMs have been configured, repeat this procedure at the site of the SDS DR NOAMs.

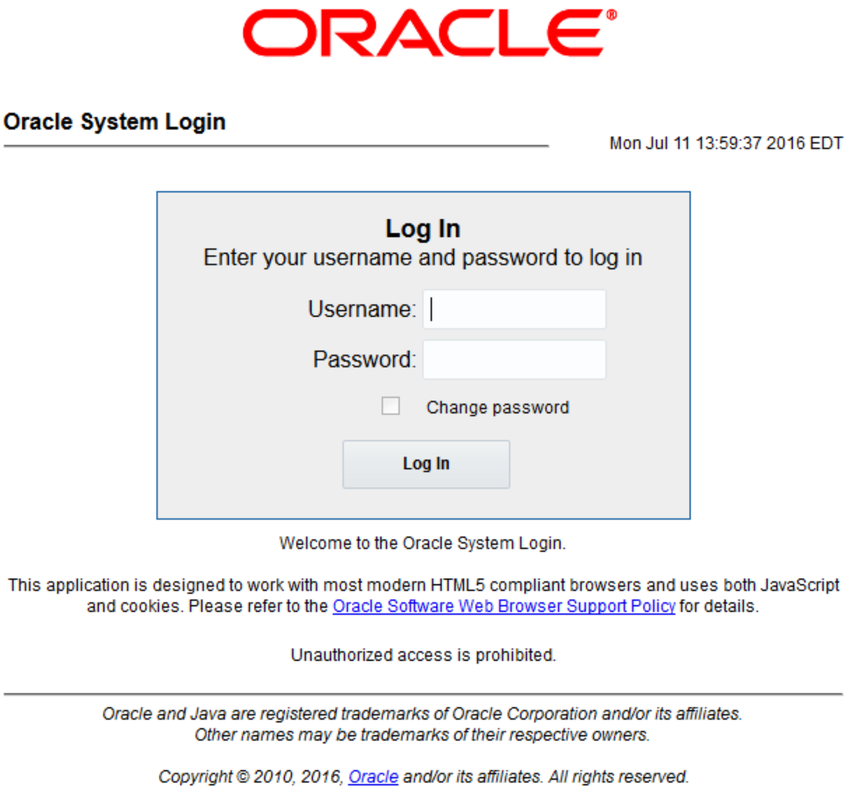
3.15.5 SOAM Configuration

Procedure 48. Configure SDS DP SOAM NE

This procedure configures the first SDS DP SOAM network element.

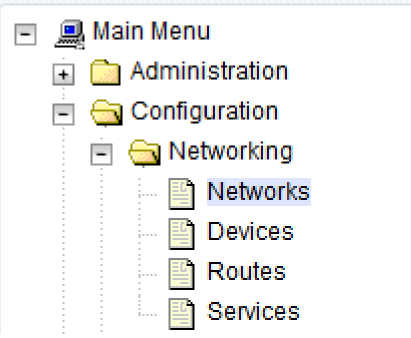
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.

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

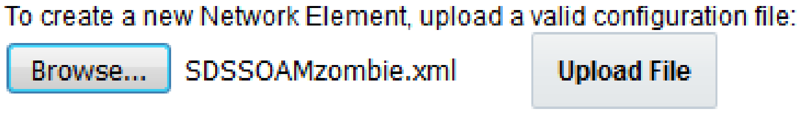
1. ☐	**SDS NOAM VIP GUI**: Login	1. Establish a GUI session on the first SDS NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_SDS_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

Procedure 48. Configure SDS DP SOAM NE

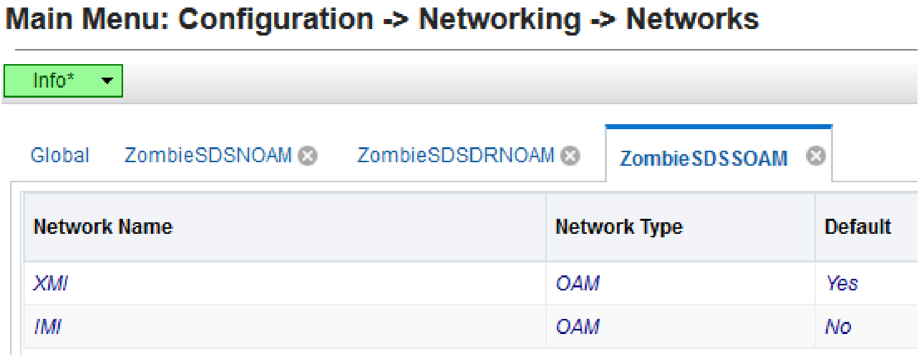
<table>
<tr>
<td>2.
☐</td>
<td>NOAM SDS VIP GUI: Create the SOAM network element using an XML file</td>
<td>
1. Navigate to Configuration > Networking > Networks.


Main Menu
Administration
Configuration
Networking
Networks
Devices
Routes
Services

2. Click Browse and enter the Pathname of the SOAM network XML file.
3. Click Upload File.


To create a new Network Element, upload a valid configuration file:
Browse...
SDSSOAMzombie.xml
Upload File

4. Click on the tab to display the configured network.


Main Menu: Configuration -> Networking -> Networks
Info*
Global
ZombieSDSNOAM
ZombieSDSDRNOAM
ZombieSDSSOAM

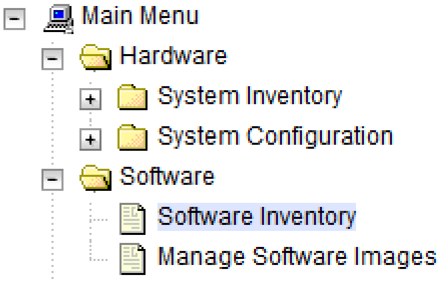
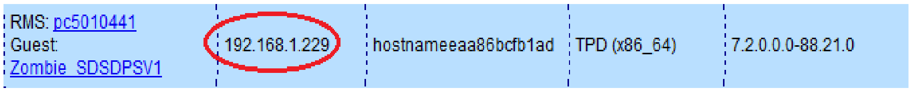
<table>
<tr><th>Network Name</th><th>Network Type</th><th>Default</th></tr>
<tr><td><i>XMI</i></td><td><i>OAM</i></td><td><i>Yes</i></td></tr>
<tr><td><i>IMI</i></td><td><i>OAM</i></td><td><i>No</i></td></tr>
</table>
</td>
</tr>
</table>

Procedure 49. Configure SDS DP SOAM Server

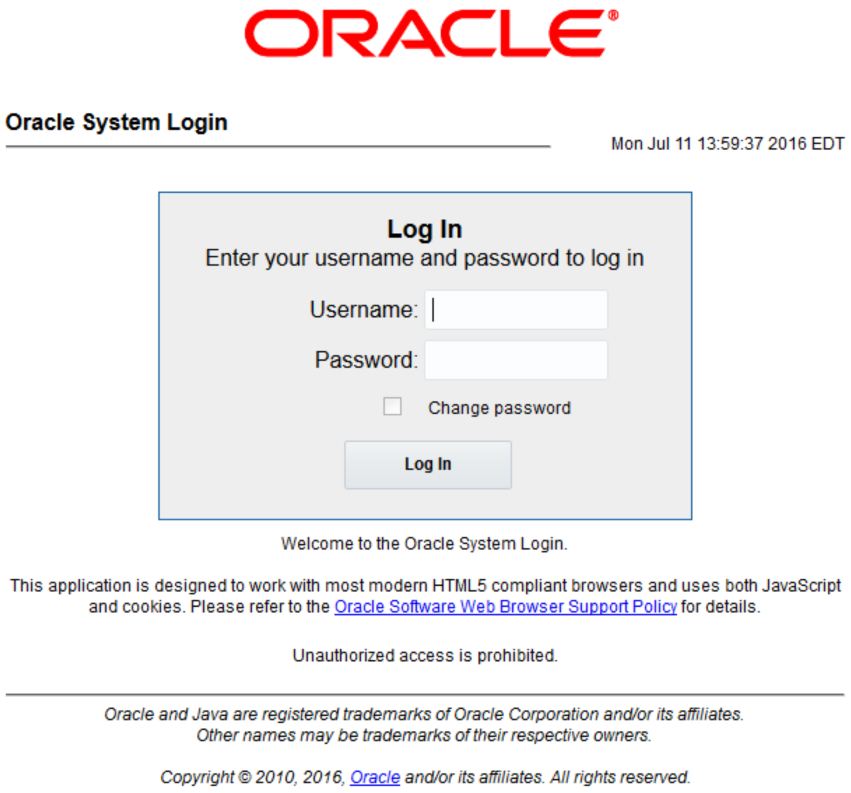
This procedure configures the SDS DP SOAM server.

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

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

1. ☐	**PMAC**: Exchange SSH keys between SDS DP SOAM site's local PMAC and the SOAM server	1. Use the PMAC GUI to determine the control network IP address of the server that is to be a SDS DP SOAM server. From the PMAC GUI, navigate to **Software > Software Inventory**.  Main Menu Hardware System Inventory System Configuration Software Software Inventory Manage Software Images 2. Note the **IP address** for a SDS DP SOAM server.  RMS: pc5010441 Guest: Zombie_SDSDPSV1 | 192.168.1.229 | hostnameeaa86bcfb1ad | TPD (x86_64) | 7.2.0.0.0-88.21.0 3. Obtain a terminal session to PMAC and login as **admusr**. 4. Exchange SSH keys for admusr between the PMAC and SDS DP SOAM server using the keyexchange utility and control network IP address for the SDS DP server. `$ keyexchange admusr@<SO1_Control_IP Address>` 5. Enter the password for the admusr user of the SDS DP SOAM server.
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 skip this step. 1. Obtain a terminal session to the SDS NOAM VIP and login as **admusr**. 2. Exchange SSH keys for admusr between the PMAC and the SDS NOAM for this SDS DP SOAM site using the keyexchange utility. `$ keyexchange admusr@<SO1_Site_PMAC_Mgmt_IP_Address>` 3. Enter the password for the admusr user of the PMAC server. 4. Repeat this step for the standby SDS DP SOAM server.

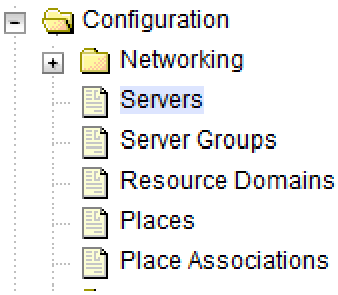
Procedure 49. Configure SDS DP SOAM Server

3. ☐	**SDS NOAM VIP GUI**: Login	1. Establish a GUI session on the first 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>` 2. Login as the **guiadmin** user.  ORACLE **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.*

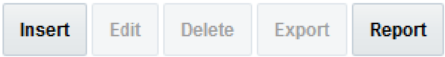
Procedure 49. Configure SDS DP SOAM Server

<table>
<tr>
<td>4.
☐</td>
<td>SDS SOAM VIP GUI: Insert the SDS DP SOAM server</td>
<td>

1. Navigate to **Configuration > Servers**.

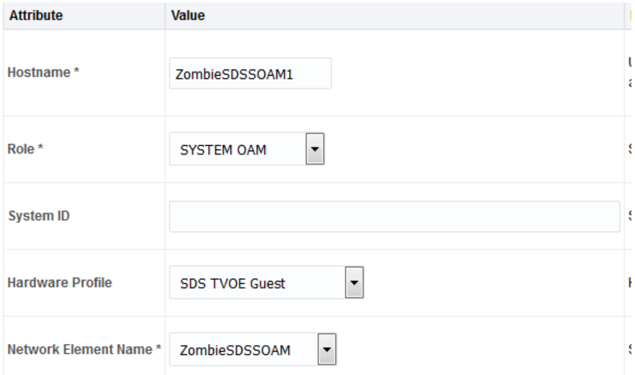

Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Click **Insert** to insert the first SDS DP SOAM server into the servers table.


Insert
Edit
Delete
Export
Report

3. Enter these values:

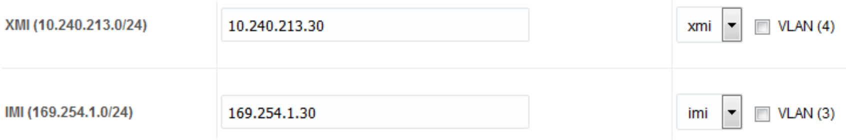
Hostname: <Hostname>
Role: System OAM
System ID: <Site System ID>
Hardware Profile: SDS TVOE Guest
Network Element Name: [Select NE]
Location: <Enter an optional location description>



Attribute | Value
Hostname * | ZombieSDSSOAM1
Role * | SYSTEM OAM
System ID |
Hardware Profile | SDS TVOE Guest
Network Element Name * | ZombieSDSSOAM

4. For the **XMI** network, type the SDS DP SOAM's XMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.

5. For the **IMI** network, type the SDS DP SOAM's IMI IP address. Select the **xmi** interface. Leave the **VLAN** checkbox unmarked.



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)

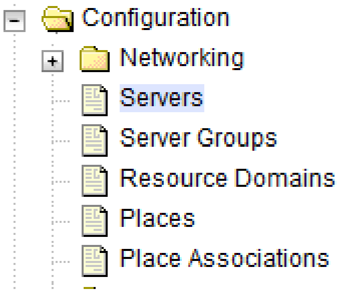
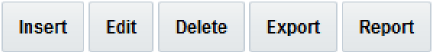
6. Add this NTP server.

<table>
<tr><th>NTP Server</th><th>Preferred?</th></tr>
<tr><td><First-SDS-SOAM-RMS-TVOE-IP-Address></td><td>Yes</td></tr>
</table>

7. Click **OK**.

</td>
</tr>
</table>

Procedure 49. Configure SDS DP SOAM Server

5. ☐	**SDS NOAM VIP GUI**: Export the initial configuration	1. Navigate to **Configuration > Servers**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. From the GUI screen, select the SDS DP SOAM server and click **Export** to generate the initial configuration data for that server.  Insert Edit Delete Export Report
6. ☐	**SDS NOAM VIP**: Copy configuration file to 1st SDS DP SOAM server	1. Obtain a terminal session to the SDS NOAM VIP as the **admusr** user. 2. Use the **awpushcfg** utility to copy the configuration file, created in the previous step, from the **/var/TKLC/db/filemgmt** directory on the SDS SOAM to the first SDS DP NOAM server, using the control network IP address for the first SDS DP SOAM server. The configuration file has a filename like **TKLCConfigData.<hostname>.sh**. `$ sudo awpushcfg` The awpushcfg utility is interactive, so the user is asked 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 first SDS DP SOAM server. • **Hostname of the target server**: Enter the server name configured in step 4.

Procedure 49. Configure SDS DP SOAM Server

7. ☐ **SDS NOAM VIP**: Verify awpushcfg was called and reboot the configured server

1. Obtain a terminal session to the first SDS DP SOAM server console by establishing an ssh session from the site PMAC terminal console.

```
$ ssh admusr@<SDS_SO1_Control_IP>
```

2. Login as **admusr**.

   The automatic configuration daemon looks for the **TKLCConfigData.sh** file in the **/var/tmp** directory, implements the configuration in the file, and asks the user to reboot the server.

3. Verify awpushcfg was called by checking the log file.

```
$ sudo cat /var/TKLC/appw/logs/Process/install.log
```

   Verify this message displays:

```
[SUCCESS] script completed successfully!
```

   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.

4. Reboot the server.

```
$ sudo init 6
```

5. Proceed to the next step once the server finishes rebooting. The server is done rebooting once the login prompt displays.

8. ☐ **SDS DP Server**: Verify server health

Login as **admusr** to the first SDS DP SOAM server and make sure no errors are returned.

```
$ 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
```

9. ☐ Insert and configure the 2nd SDS DP SOAM server

Repeat this procedure to insert and configure the second SDS DP SOAM server with the exception of the NTP server, which should be configured as:

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

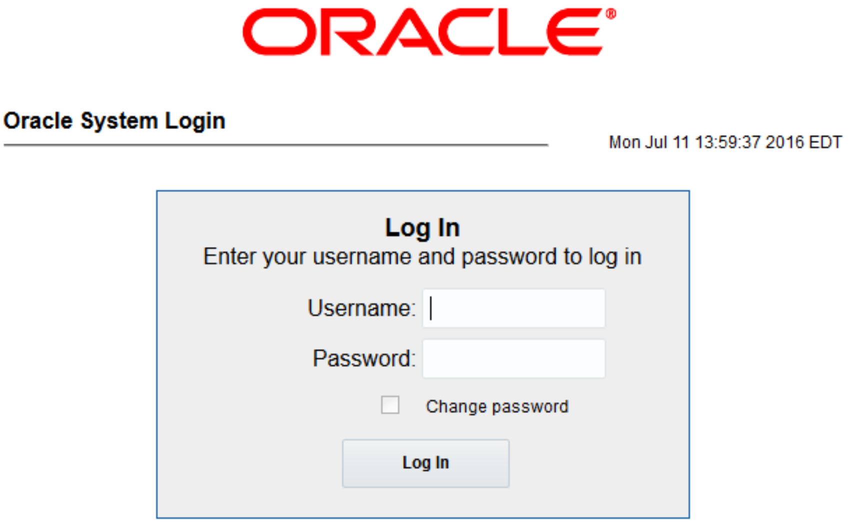
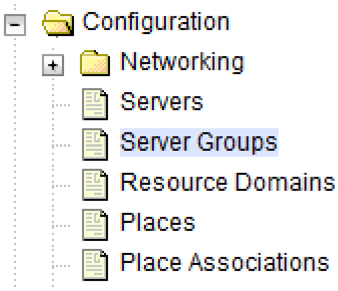
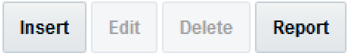
Instead of data for the first SDS DP SOAM server, insert the network data for the second SDS DP SOAM server, transfer the **TKLCConfigData** file to the second SDS DP SOAM server and reboot the second SDS DP SOAM server when prompted at a terminal window.

Procedure 50. Configure the SDS DP SOAM Server Group

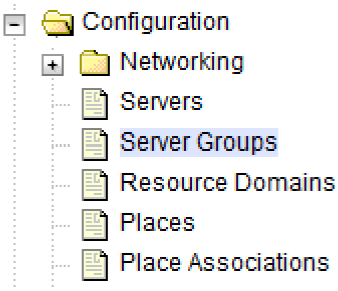
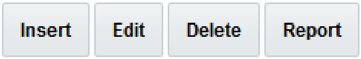
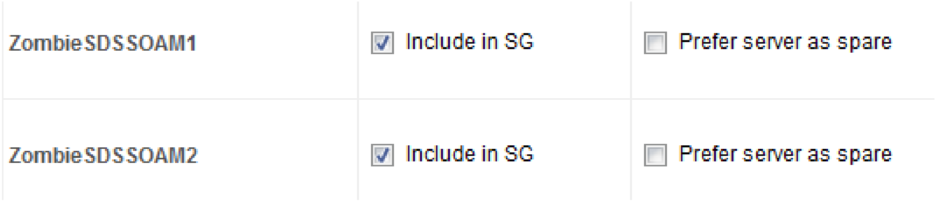
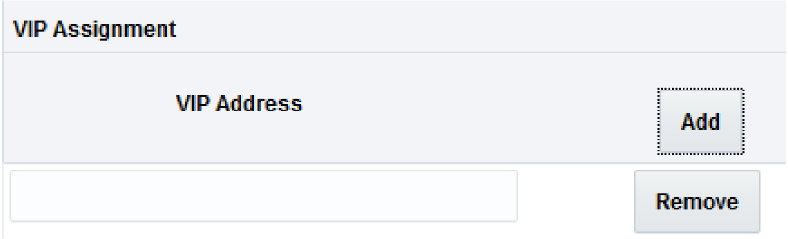
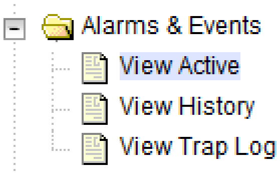
This procedure configures the SDS DP SOAM server group.

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

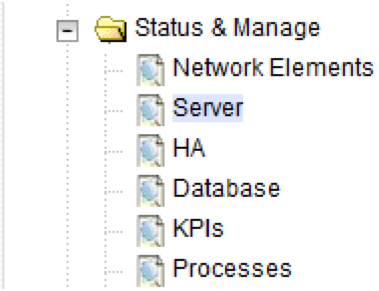
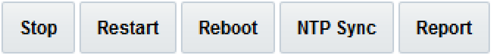
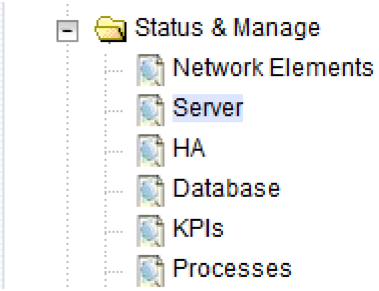
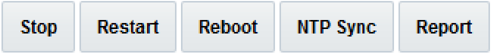
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**SDS NOAM VIP GUI**: Login	1. Establish a GUI session on the first 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>` 2. Login as the **guiadmin** user.  Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Username: Password: ☐ Change password Log In
2. ☐	**SDS NOAM VIP GUI**: Enter SDS DP SOAM server group data	1. Navigate to **Configuration > Server Groups**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Click **Insert**.  Insert Edit Delete Report 3. Enter these values: **Server Group Name**: <Server Group Name> **Level**: B **Parent**: Select the NOAM Server Group **Function**: SDS (Active/Standy Pair) **WAN Replication Connection Count**: Use default value 4. Click **OK**.

Procedure 50. Configure the SDS DP SOAM Server Group

3. ☐	**SDS NOAM VIP GUI**: Edit the SDS DP SOAM server groups and VIP	1. Navigate to **Configuration > Server Groups**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. Select the server group you just created and click **Edit**.  Insert Edit Delete Report 3. Add both SDS DP SOAM servers to the server group primary site by marking the **Include in SG** checkbox for each SDS DP server. Do **not** mark any of the **Preferred Spare** checkboxes.  ZombieSDSSOAM1 ☑ Include in SG ☐ Prefer server as spare ZombieSDSSOAM2 ☑ Include in SG ☐ Prefer server as spare 4. Click **Apply**. 5. Click **Add**. 6. Type the **VIP Address** and click **OK**.  VIP Assignment VIP Address Add Remove
4. ☐	**SDS NOAM VIP GUI**: Wait for remote database alarm to clear	Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding. Monitor progress by navigating to **Alarms & Events > View Active**.  Alarms & Events View Active View History View Trap Log

Procedure 50. Configure the SDS DP SOAM Server Group

5. ☐	**SDS NOAM VIP GUI**: Restart 1st SDS DP servers	1. Navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the first SDS DP server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm. Wait for the restart successful message.
6. ☐	**SDS NOAM VIP GUI**: Restart 2nd SDS DP servers	1. Navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the second SDS DP server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm. Wait for the restart successful message.

3.15.6 DP Configuration

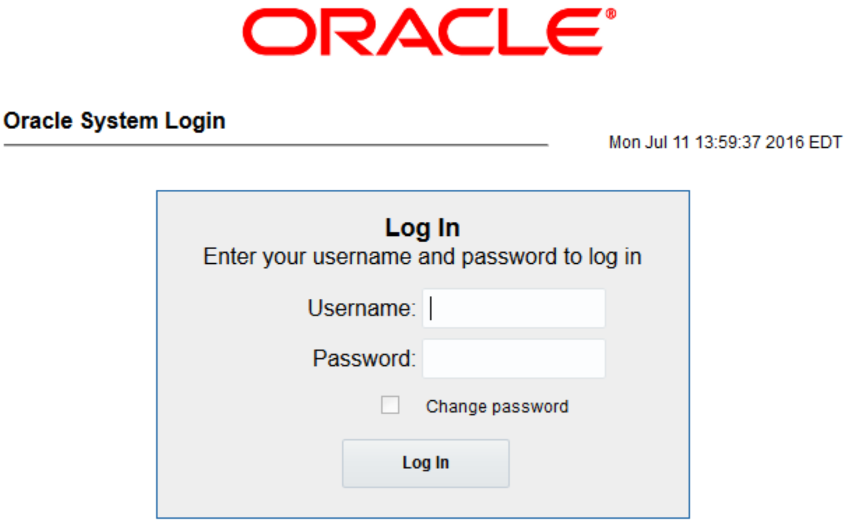
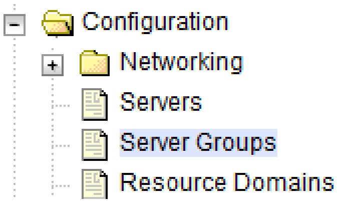
To install the Data Processor (DP) blade, refer to the procedure DP Installation (All SOAM sites) in the DSR Initial Installation and Configuration Guide.

Procedure 51. Configure the SDS DP Server Group

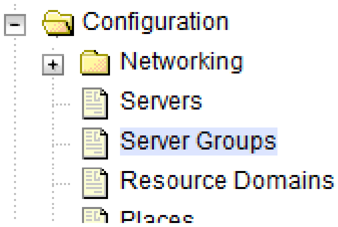
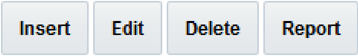
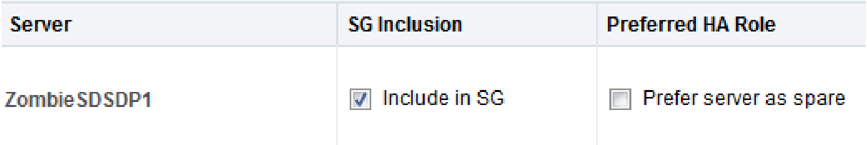
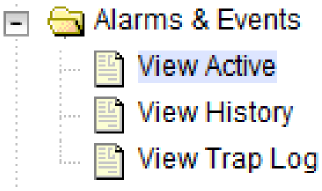
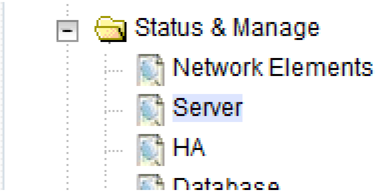
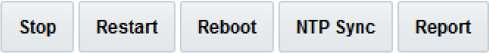
This procedure configures the SDS DP server group.

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

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

1. ☐	**SDS NOAM VIP GUI**: Login	1. Establish a GUI session on the first 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>` 2. Login as the **guiadmin** user.  ORACLE 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
2. ☐	**SDS NOAM VIP GUI**: Enter SDS DP server group data	1. Navigate to **Configuration > Server Groups**.  Configuration Networking Servers Server Groups Resource Domains 2. Click **Insert**. Insert Edit Delete Report 3. Enter these values: **Server Group Name**: <Server Group Name> **Level**: C **Parent**: SDS DP SOAM server group that is parent to this SDS DP **Function**: SDS 4. Click **OK**. 5. Repeat this step for any remaining SDS DP server groups.

Procedure 51. Configure the SDS DP Server Group

3. ☐	**SDS NOAM VIP GUI**: Edit the SDS DP server groups to include SDS DPs	1. Navigate to **Configuration > Server Groups**.  Configuration Networking Servers Server Groups Resource Domains Places 2. Select the server group you just created and click **Edit**.  Insert Edit Delete Report 3. Select the network element that represents the SDS DP server group. 4. Mark the **Include in SG** checkbox for the SDS DP server. 5. Leave other checkboxes blank.  Server | SG Inclusion | Preferred HA Role ZombieSDSDP1 | ☑ Include in SG | ☐ Prefer server as spare Each SDS DP server should be in its own server group. 6. Click **OK**. 7. Repeat this step for any remaining SDS DP server groups you need to edit.
4. ☐	**SDS NOAM VIP GUI**: Wait for remote database alarm to clear	Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding. Monitor progress by navigating to **Alarms & Events > View Active**.  Alarms & Events View Active View History View Trap Log
5. ☐	**SDS NOAM VIP GUI**: Restart SDS DP servers	1. Navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database 2. For each SDS DP server, select the SDS DP server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm. Wait for the restart successful message.

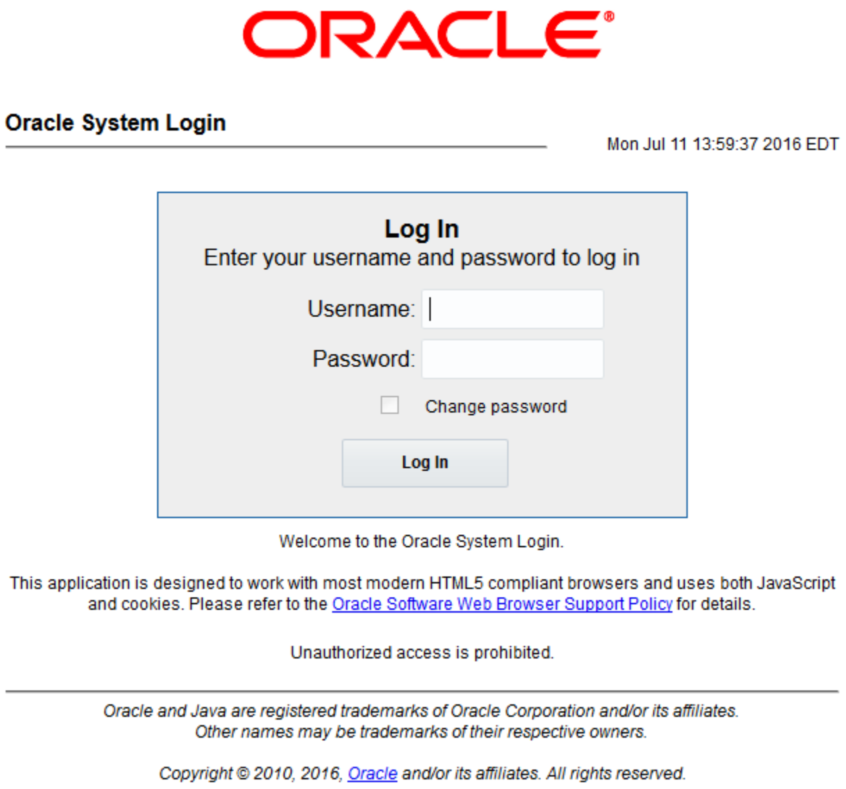
3.15.7 DSCP Configuration (Optional)

Procedure 52. Configure DSCP Values for Outgoing Traffic (Optional)

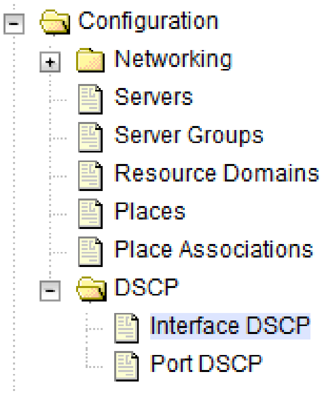
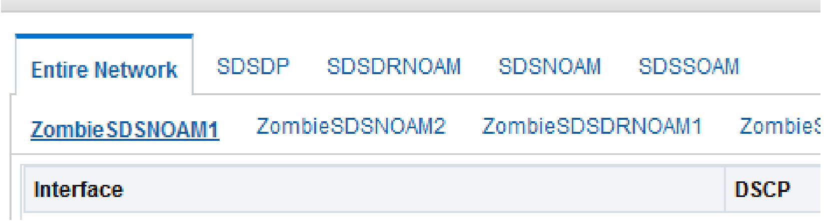
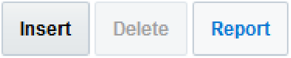
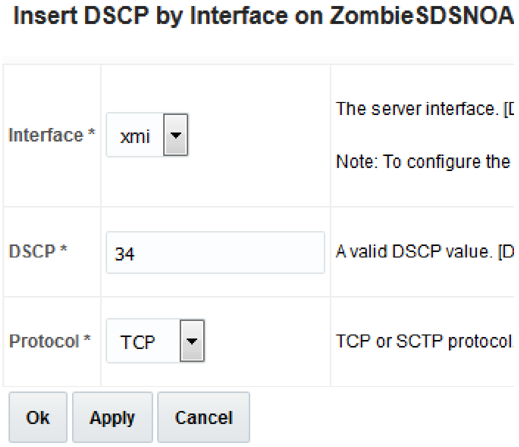
This procedure configures the DSCP values for outgoing packets on servers. DSCP values can be applied to an outbound interface as a whole, or to all outbound traffic using a specific TCP or SCTP source port. This step is optional and should only be executed if your network uses packet DSCP markings for quality-of-service.

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

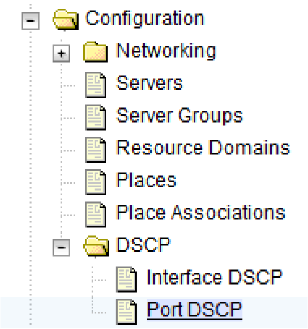
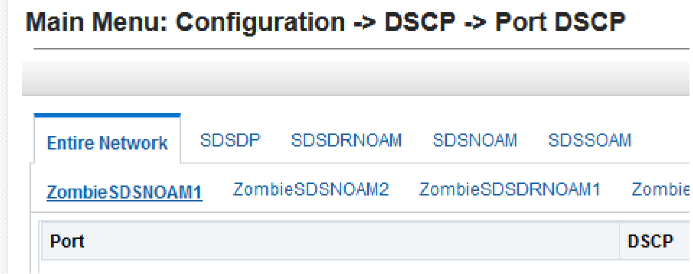
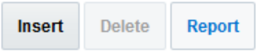
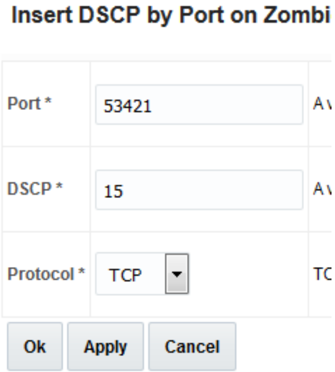
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**SDS NOAM VIP GUI**: Login	1. Establish a GUI session on the first 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>` 2. Login as the **guiadmin** user. Oracle System Login Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

Procedure 52. Configure DSCP Values for Outgoing Traffic (Optional)

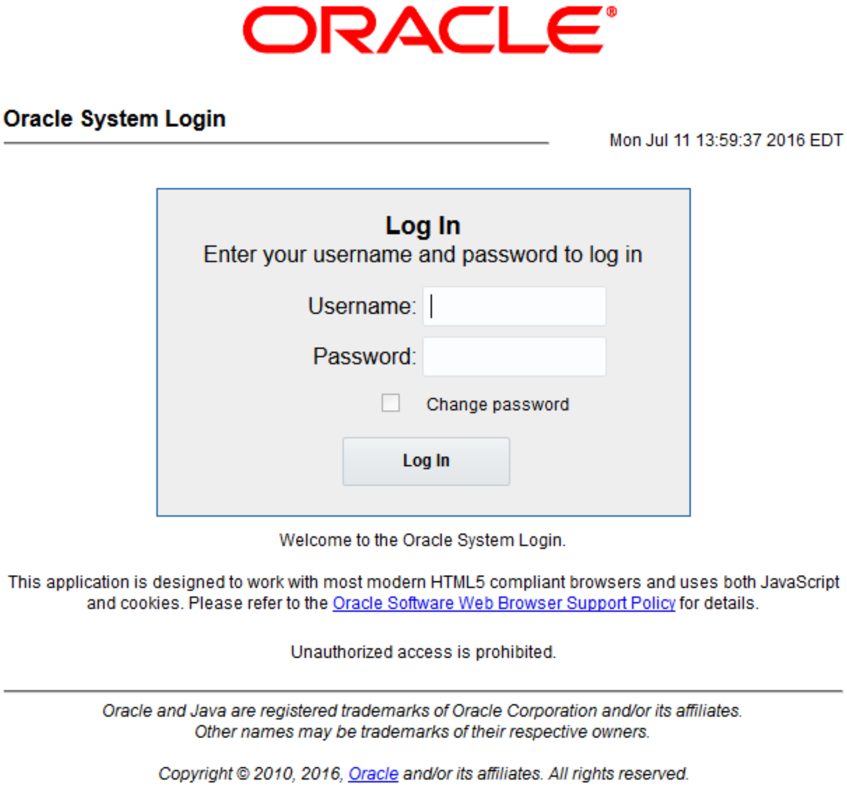
2. ☐	**NOAM VIP GUI**: Option 1 — Configure Interface DSCP	***Note:*** The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary. 1. Navigate to **Configuration > DSCP > Interface DSCP**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations DSCP Interface DSCP Port DSCP 2. Select the server to configure on the 2nd line. You can view all servers with **Entire Network** selected or limit it to a specific server group by clicking on that server group name's tab.  Entire Network SDSDP SDSDRNOAM SDSNOAM SDSSOAM ZombieSDSNOAM1 ZombieSDSNOAM2 ZombieSDSDRNOAM1 Interface DSCP 3. Click **Insert**.  Insert Delete Report 4. Select the network **Interface** option and type the **DSCP** value to apply to packets leaving this interface. Insert DSCP by Interface on ZombieSDSNOA Interface * xmi The server interface. [D Note: To configure the DSCP * 34 A valid DSCP value. [D Protocol * TCP TCP or SCTP protocol Ok Apply Cancel 5. Click **OK** if there are no more interfaces on this server to configure, or click **Apply** to finish this interface and continue entering more interfaces.

Procedure 52. Configure DSCP Values for Outgoing Traffic (Optional)

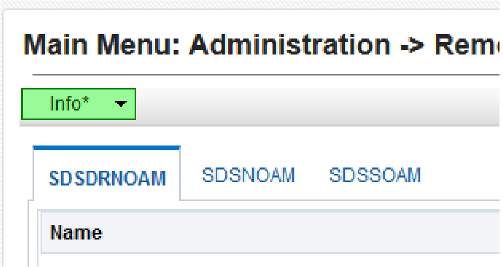
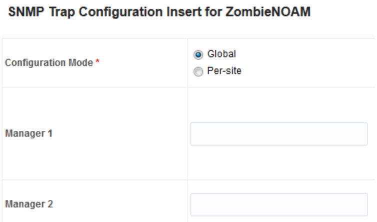
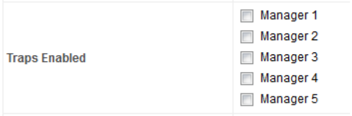
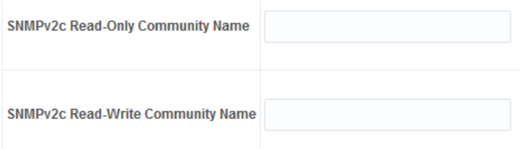
3. ☐	**NOAM VIP GUI**: Option 2 — Configure Port DSCP	***Note:*** The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary. 1. Navigate to **Configuration > DSCP > Port DSCP**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations DSCP Interface DSCP Port DSCP 2. Select the server to configure on the 2nd line. You can view all servers with **Entire Network** selected or limit it to a specific server group by clicking on that server group name's tab.  Main Menu: Configuration -> DSCP -> Port DSCP Entire Network SDSDP SDSDRNOAM SDSNOAM SDSSOAM ZombieSDSNOAM1 ZombieSDSNOAM2 ZombieSDSDRNOAM1 Zombie Port DSCP 3. Click **Insert**.  Insert Delete Report 4. Enter the source **Port**, **DSCP** value, and select the transport **Protocol**.  Insert DSCP by Port on Zombi Port * 53421 A DSCP * 15 A Protocol * TCP TC Ok Apply Cancel 5. Click **OK** if there are no more port DSCPs on this server to configure, or click **Apply** to finish this port entry and continue entering more port DSCP mappings.
4. ☐	**NOAM VIP GUI**: Repeat for additional servers	Repeat steps 2. through 3. for all remaining servers.

3.15.8 SNMP Configuration (Optional)

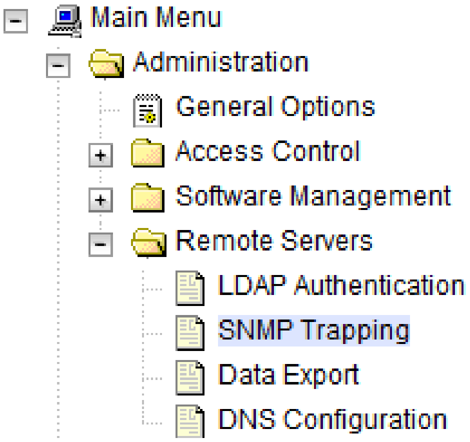
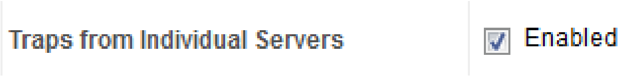
Procedure 53. Configure SNMP Trap Receivers (Optional)

<table>
<tr><td colspan="3">This procedure configures forwarding of SNMP traps from each individual server.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>SDS NOAM VIP GUI: Login</td><td>1. Establish a GUI session on the first 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>
2. Login as the guiadmin user.

Oracle System Login
Mon Jul 11 13:59:37 2016 EDT
Log In
Enter your username and password to log in
Username:
Password:
☐ Change password
Log In
Welcome to the Oracle System Login.
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.
Unauthorized access is prohibited.
<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></td></tr>
</table>

Procedure 53. Configure SNMP Trap Receivers (Optional)

2. ☐	**SDS NOAM VIP GUI**: Configure system-wide SNMP trap receiver(s)	1. Navigate to **Administration > Remote Servers > SNMP Trapping**. 2. Select the server group tab for SNMP trap configuration.  Main Menu: Administration -> Rem Info* SDSDRNOAM SDSNOAM SDSSOAM Name 3. Type the **IP address** or **hostname** of the network management station (NMS) to forward traps. This IP should be reachable from the NOAMP's XMI network. 4. Continue add additional secondary, tertiary, etc., manager IPs in the corresponding slots, if desired. SNMP Trap Configuration Insert for ZombieNOAM Configuration Mode * ● Global ○ Per-site Manager 1 Manager 2 5. Mark **Traps Enabled** checkboxes for the manager servers being configured. Traps Enabled ☐ Manager 1 ☐ Manager 2 ☐ Manager 3 ☐ Manager 4 ☐ Manager 5 6. Type the **SNMP Community Name**. SNMPv2c Read-Only Community Name SNMPv2c Read-Write Community Name 7. Leave all other fields at their default values. 8. Click **OK**.

Procedure 53. Configure SNMP Trap Receivers (Optional)

3. ☐	**SDS NOAM VIP GUI**: Enable Traps from Individual Servers (optional)	***Note:*** By default SNMP traps from DPs are aggregated and display on 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 all servers, including DPs, have an XMI interface on which the customer SNMP target server (NMS) is reachable. 1. Navigate to **Administration > Remote Servers > SNMP Trapping**.  Main Menu Administration General Options Access Control Software Management Remote Servers LDAP Authentication SNMP Trapping Data Export DNS Configuration 2. Make sure **Enabled** checkbox is marked. Traps from Individual Servers ☑ Enabled 3. Click **Apply** and verify that the data is committed.

3.16 IDIH Installation and Configuration (Optional)

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

Note: Refer to section 3.10 for IDIH VM placement information.

3.16.1 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 54 for IDIH installation.

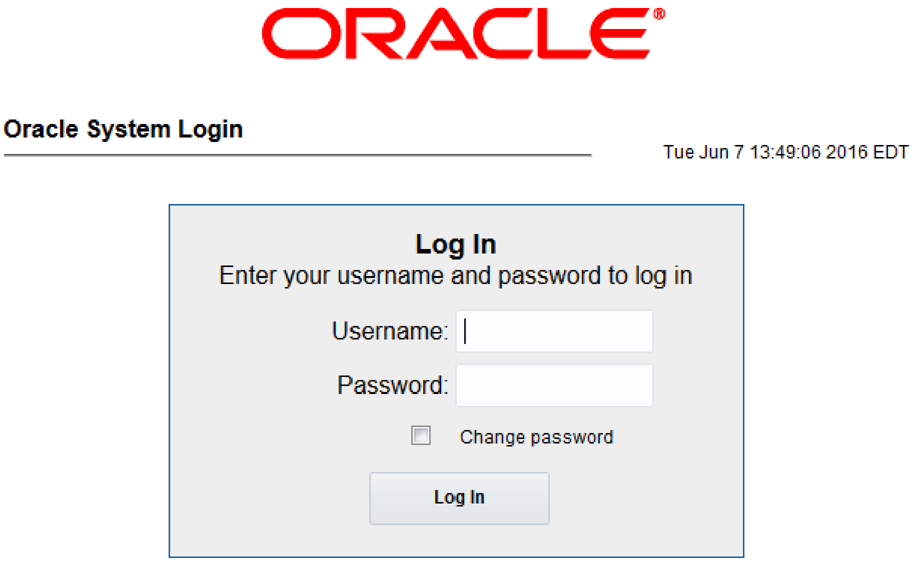
Procedure 54. IDIH Installation

This procedure installs IDIH.

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

If this procedure fails, it is recommended to contact 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. through 4.
		Use one of the following options add the application ISO images (mediation, application, and oracleGuest) to the PMAC:
		Option 1 — Insert the CD containing the IDIH media into the removable media drive.
		Option 2 — Attach the USB device containing the ISO image to a USB port.
		Option 3 — Copy the Application ISO file to the PMAC server into the **/var/TKLC/smac/image/isoimages/home/smacftpusr/** directory as **pmacftpusr** user:
		cd to the directory where your ISO image is located on the TVOE host (not on the PMAC server).
		Using sftp, connect to the PMAC server.
		`$ sftp pmacftpusr@<pmac_management_network_ip>`
		`$ put <image>.iso`
		After the image transfer is 100% complete, close the connection.
		`$ quit`

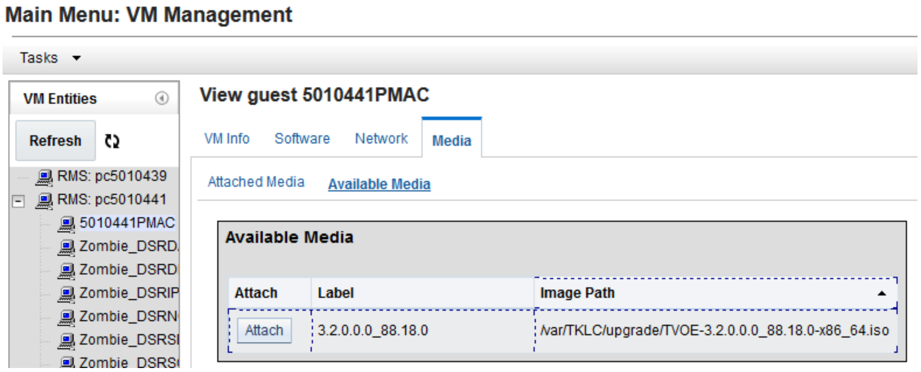
2. ☐	**PMAC GUI**: Login	1. Open the web browser and navigate to the PMAC GUI: `http://<PMAC_network_IP>` 2. Login as the **guiadmin** user:  Oracle System Login Tue Jun 7 13:49:06 2016 EDT Log In Enter your username and password to log in Username: Password: ☐ Change password Log In

Procedure 54. IDIH Installation

<table>
<tr>
<td>3.
☐</td>
<td>PMAC GUI: Attach the software Image to the PMAC guest</td>
<td>

If the ISO image was transferred directly to the PMAC guest using sftp, skip this step and continue with the next step.

1. From the PMAC GUI, navigate to **VM Management > PMAC guest > View VM Guest > Media tab**.
2. Locate the ISO image in the **Available Media** list and click its **Attach** button.

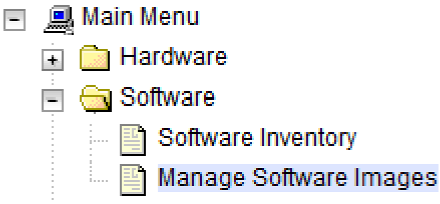
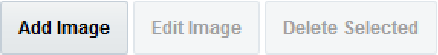
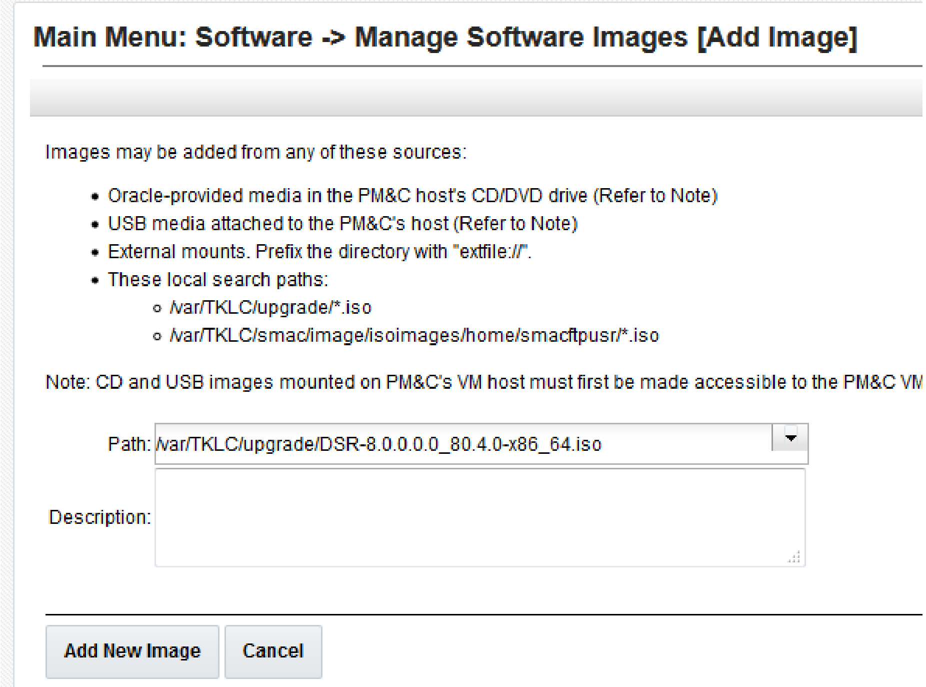


Main Menu: VM Management
Tasks
VM Entities
Refresh
RMS: pc5010439
RMS: pc5010441
5010441PMAC
Zombie_DSRD
Zombie_DSRD
Zombie_DSRIP
Zombie_DSRN
Zombie_DSRSI
Zombie_DSRS
View guest 5010441PMAC
VM Info
Software
Network
Media
Attached Media
Available Media
Available Media

Attach	Label	Image Path
Attach	3.2.0.0_88.18.0	/var/TKLC/upgrade/TVOE-3.2.0.0_88.18.0-x86_64.iso

</td>
</tr>
</table>

Procedure 54. IDIH Installation

4.
☐
	PMAC GUI: Add application image	1. Navigate to **Software > Manage Software Images**.
		 Main Menu
		Hardware
		Software
		Software Inventory
		Manage Software Images
		2. Click **Add Image**.
		3. Select the image from the options.
		
		If the image was supplied on a CD or a USB drive, it displays 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 on the second device, **device://dev/sr1**. If one or more CD or USB-based images was already on the management server before you started this procedure, select a correspondingly higher device number.
		If the image was transferred to PMAC using sftp, it displays in the list as a local file **/var/TKLC/...**.
		
		Main Menu: Software -> Manage Software Images [Add Image]
		Images may be added from any of these sources:
		• Oracle-provided media in the PM&C host's CD/DVD drive (Refer to Note)
		• USB media attached to the PM&C's host (Refer to Note)
		• External mounts. Prefix the directory with "extfile://".
		• These local search paths:
		  ○ /var/TKLC/upgrade/*.iso
		  ○ /var/TKLC/smac/image/isoimages/home/smacftpusr/*.iso
		Note: CD and USB images mounted on PM&C's VM host must first be made accessible to the PM&C VM
		Path: /var/TKLC/upgrade/DSR-8.0.0.0.0_80.4.0-x86_64.iso
		Description:
		
		4. Select the appropriate path and click **Add New Image**.
		5. Check the progress clicking the **Task Monitoring** link. Observe the green bar indicating success.
		6. Once complete, remove the TPD Media from the optical drive of the management server.

Procedure 54. IDIH Installation

5. ☐	**PMAC**: Establish terminal session	Establish an SSH session to the PMAC and login as **admusr**.

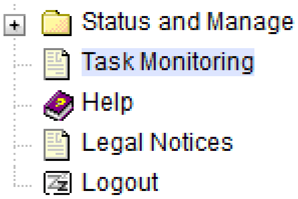
6.
☐
	PMAC: Reset create guest default timeout and other timeout parameters	1. Reset the create guest default timeout by executing these commands:
		`$ sudo sqlite3 /usr/TKLC/plat/etc/TKLCfd-config/db/fdcRepo.fdcdb ‘update params set value=3000 where name=”DEFAULT_CREATE_GUEST_TIMEOUT”’;`
		`$ sudo pmacadm setParam --paramName=defaultTpdProvdTimeout --paramValue=120`
		`$ sudo pmacadm setParam --paramName=guestDiskDeployTimeout --paramValue=50`
		2. Verify whether the above values are set correctly.
		`$ sudo sqlite3 /usr/TKLC/plat/etc/TKLCfd-config/db/fdcRepo.fdcdb 'select name, value from params where name like "%TIMEOUT%"';`
		`$ sudo pmacadm getParam --paramName=defaultTpdProvdTimeout`
		`$ sudo pmacadm getParam --paramName=guestDiskDeployTimeout`

7.
☐
	PMAC: Copy the fdc.cfg template XML file to the guest-dropin directory	3. Copy the vedsr_idih.xml.template XML file to the pmac guest-dropin directory.
		`$ sudo cp  /usr/TKLC/smac/html/TPD/mediation-8.4.0.0.0_x.x.x.x/vedsr_idih.xml.template /var/TKLC/smac/guest-dropin`
		`$ cd /var/TKLC/smac/guest-dropin/`
		`$ mv vedsr_idih.xml.template <idih_fdc_file_name>.xml`

8. ☐	**PMAC**: Configure the fdc.xml file	1. Configure the <idih_fdc_file_name>.xml file. See Appendix M Configure IDIH Fast Deployment for a breakdown of the parameters and a sample XML configuration file. 2. Update the software versions, hostnames, bond interfaces, network addresses, and network VLAN information for the TVOE host and IDIH guests that you are installing.

9.
☐
	PMAC: Run the fdconfig	`$ screen`
		`$ sudo fdconfig config --file=<idih_fdc_file_name>.xml`
		Example:
		`$ sudo fdconfig config --file=tvoe-ferbrms4_01-22-15.xml`
		Note: This is a long duration command (45-90 minutes). If the screen command was run before executing fdconfig, perform a **screen -dr** to resume the screen session in the event of a terminal timeout, etc.

Procedure 54. IDIH Installation

10. ☐	**PMAC GUI**: Monitor the configuration	1. If not already done so, establish a GUI session on the PMAC server. 2. Navigate to **Task Monitoring**.  Status and Manage Task Monitoring Help Legal Notices Logout 3. Monitor the IDIH configuration to completion.

3.16.2 IDIH Configuration

3.16.2.1 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 is 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 55. Configure DSR Reference Data Synchronization for IDIH

This procedure configures DSR reference data synchronization for IDIH. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**IDIH Application Server**: Login	1. Establish an SSH session to the IDIH application server login as **admusr**. 2. Login as tekelec user. `$ sudo su - tekelec`

2.
☐
	IDIH Application Server: Execute configuration script	`$ apps/trda-config.sh`
		Example output:
		`corsair-app:/usr/TKLC/xIH apps/trda-config.sh`
		`dos2unix: converting file /usr/TKLC/xIH/bea/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, 2018 Oracle.  All rights reserved.`

Procedure 55. Configure DSR Reference Data Synchronization for IDIH

```
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
```

Procedure 55. Configure DSR Reference Data Synchronization for IDIH

```
     [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
```

3. When asked to **enter DSR OAM server IP address**, type the **VIP of the DSR SOAM**, and press **Enter**.

   Note: If the address entered is unreachable, the script exits with an **Unable to connect to <ip-address>** error.

Procedure 55. Configure DSR Reference Data Synchronization for IDIH

3. ☐	**IDIH Application Server**: Monitor completion	1. Monitor the log file located at /var/TKLC/xIH/log/apps/weblogic/apps/application.log. 2. Examine the log file for entries containing text **Trace Reference Data Adapter**.
4. ☐	**IDIH Application Server** (optional): Switch iDIH from one DSR to another DSR in a different network	***Note:*** This is an optional step that 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 and login as the **tekelec** user. 2. Execute these commands.

```
cd /usr/TKLC/xIH/apps/trace-refdata-adapter
ant clean.data
cd /usr/TKLC/xIH/apps/xihoam
ant imp.init (flush comagent connection data)
cd /usr/TKLC/xIH/apps/trace-refdata-adapter
ant app.enable (Sync MOs from SOAM)
cd /usr/TKLC/xIH/apps
./trda-config.sh <DSR SOAM VIP in different network>
```

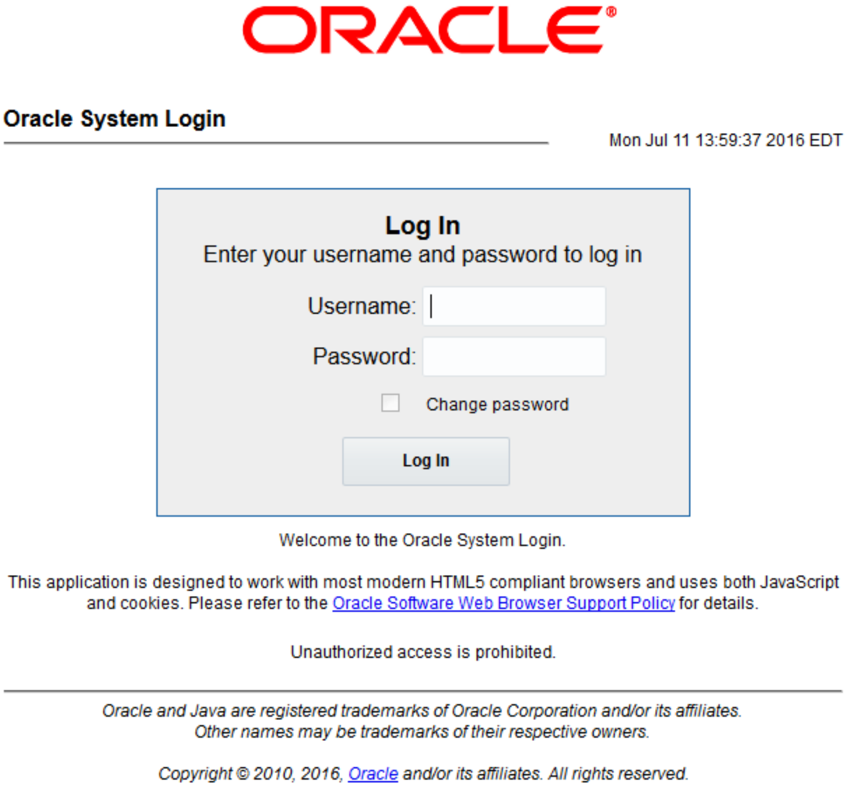
3.16.2.2 Configure the SSO Domain

Procedure 56. Configure the SSO Domain

This procedure configures the SSO domain for IDIH.

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

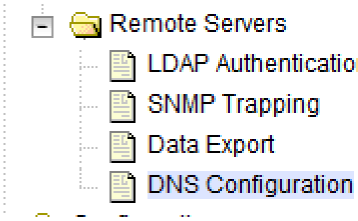
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Username: Password: ☐ Change password 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.*

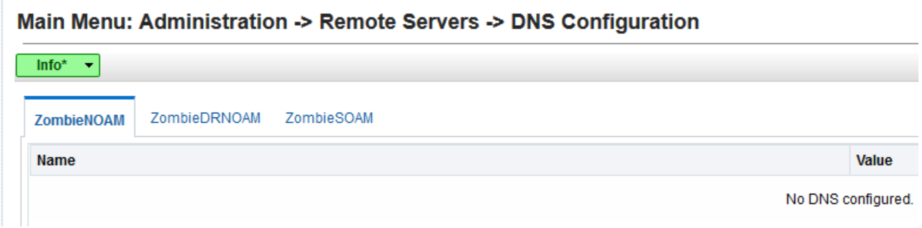
Procedure 56. Configure the SSO Domain

2. ☐ **NOAM VIP GUI**: Configure DNS

1. Navigate to **Administration > Remote Servers > DNS Configuration**.


Remote Servers
LDAP Authentication
SNMP Trapping
Data Export
DNS Configuration

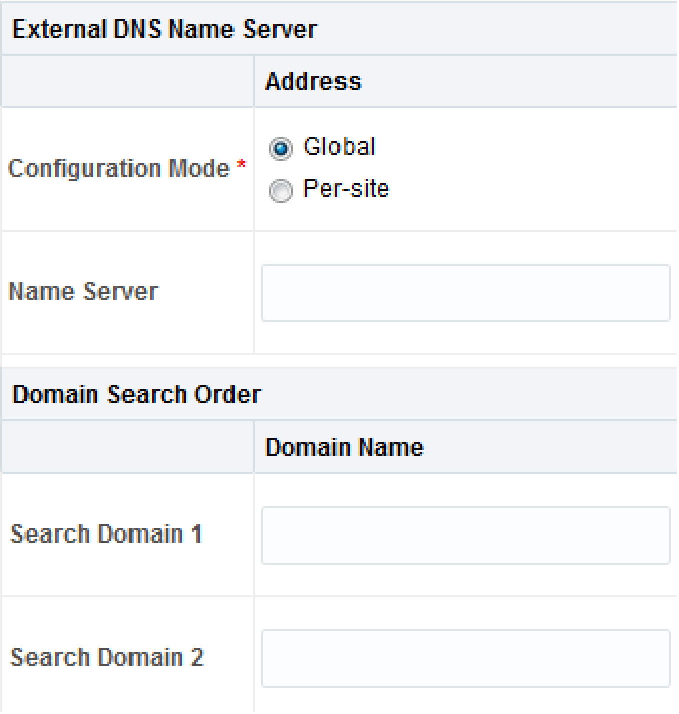
2. Select the NOAM tab.


Info*
ZombieNOAM
ZombieDRNOAM
ZombieSOAM

Main Menu: Administration -> Remote Servers -> DNS Configuration

Name	Value
	No DNS configured.

3. Configure values for the following fields:
   - Name Server
   - Domain Name
   - Search Domain 1



External DNS Name Server

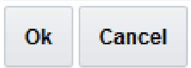
	Address
Configuration Mode *	● Global ○ Per-site
Name Server	

Domain Search Order

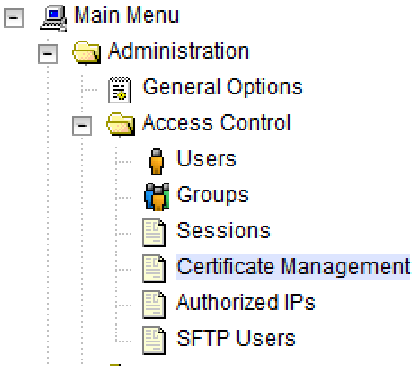
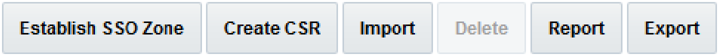
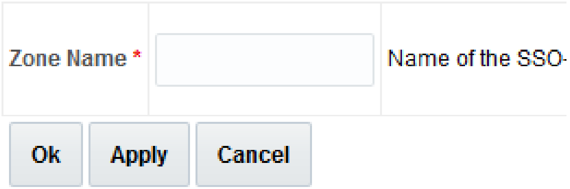
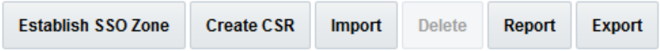
	Domain Name
Search Domain 1	
Search Domain 2	

If values have already been configured, click **Cancel**.

4. Click **OK**.

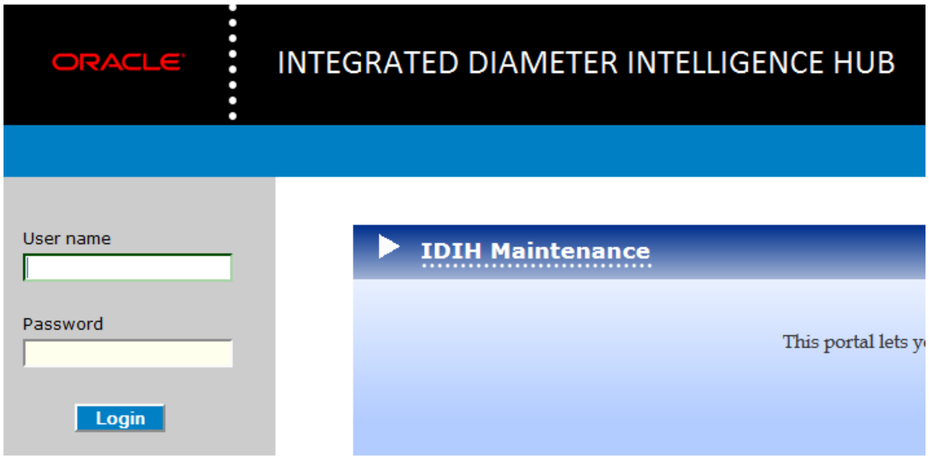
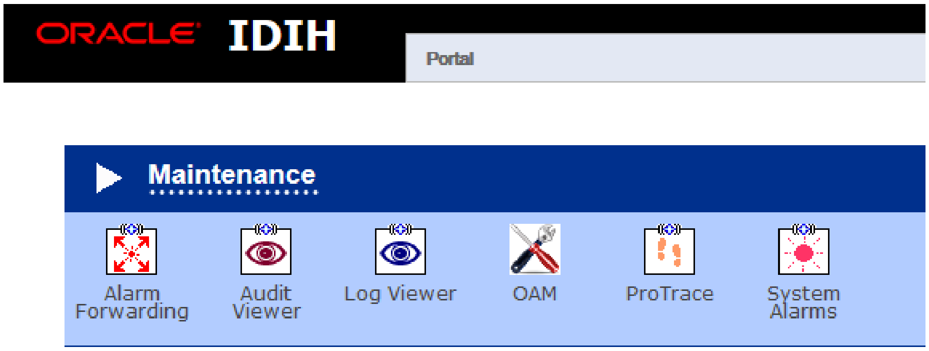


Procedure 56. Configure the SSO Domain

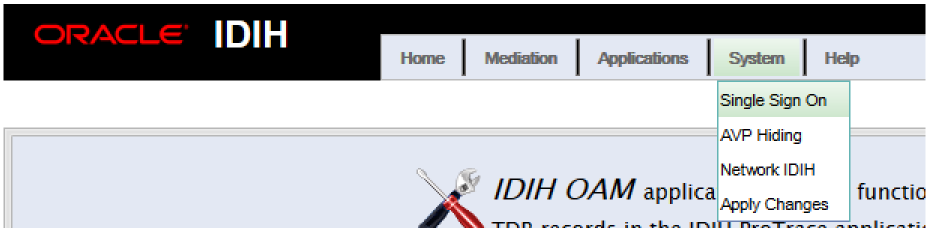
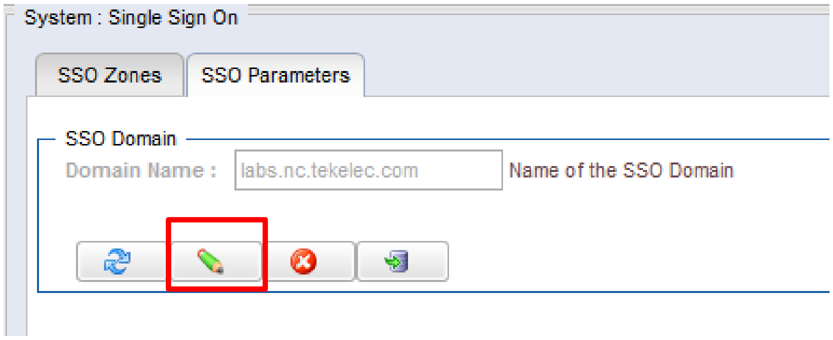
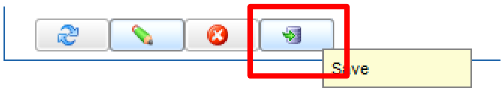
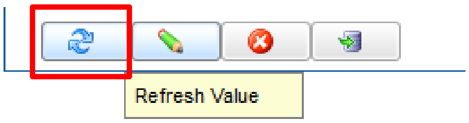
3. ☐	**NOAM VIP GUI**: Establish SSO local zone	1. Navigate to **Access Control > Certification Management**.  Main Menu Administration General Options Access Control Users Groups Sessions Certificate Management Authorized IPs SFTP Users 2. Click **Establish SSO Zone**.  Establish SSO Zone Create CSR Import Delete Report Export 3. Type a value for **Zone Name**. 4. Click **OK**.  Zone Name * Name of the SSO Ok Apply Cancel Information for the new Certificate type of SSO Local displays. 5. Click **Report**.  Establish SSO Zone Create CSR Import Delete Report Export 6. Select and copy the encoded certificate text to the clipboard for future access.

```
-----BEGIN CERTIFICATE-----
MIICKzCCAdWgAwIBAgIJAOVfSLNc3CeJMA0GCSqGSIb3DQEBCwUAMHExCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJOQzEQMA4GA1UEBwwHUmFsZWlnaDEPMA0GA1UECgwG
T3JhY2xlMQswCQYDVQQLDAJQVjEQMA4GA1UEAwwHTGliZXJ0eTETMBEGCSqGSIb3
DQEJARYEdGVzdDAeFw0xNTA1MDQxNDIzNTRaFw0xNjA1MDMxNDIzNTRaMHExCzAJ
BgNVBAYTAlVTMQswCQYDVQQIDAJOQzEQMA4GA1UEBwwHUmFsZWlnaDEPMA0GA1UE
CgwGT3JhY2xlMQswCQYDVQQLDAJQVjEQMA4GA1UEAwwHTGliZXJ0eTETMBEGCSqG
SIb3DQEJARYEdGVzdDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCZ/MpkhlvMP/iJ
s5xDO2MwxJm3jYim43H8gR9pfBTMNP6L9kluJYi+2T0hngJFQLpIn6SK6pXnuAGY
f/vDWfqPAgMBAAGjUDBOMB0GA1UdDgQWBBS6IzIOLP1gizQ6+BERr8Fo2XyDVDAf
BgNVHSMEGDAWgBS6IzIOLP1gizQ6+BERr8Fo2XyDVDAMBgNVHRMEBTADAQH/MA0G
CSqGSIb3DQEBCwUAA0EAOwIqBMEQyvfvt38r/yfgIx3w5dN8SBwHjHC5TpJrHV6U
zFlg5dfzoLz7ditjGOhWJ9l9VRw39LQ8lKFp7SMXwA==
-----END CERTIFICATE-----
```

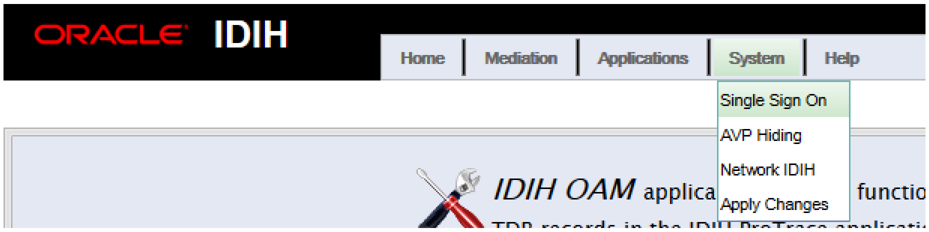
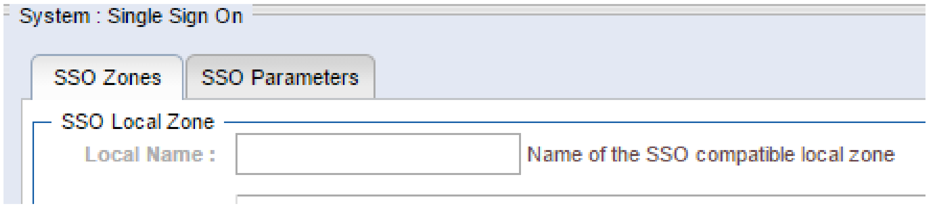
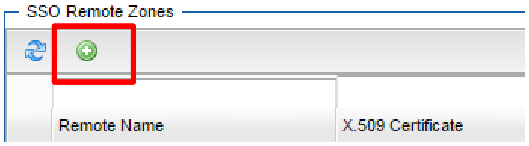
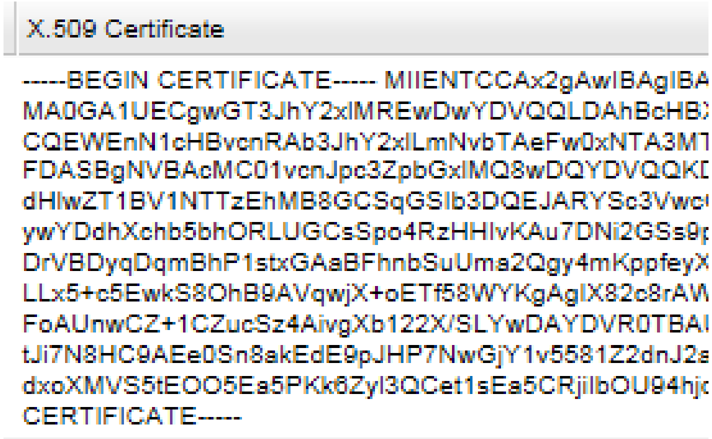
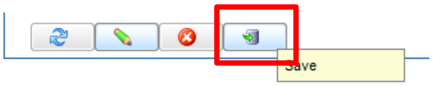
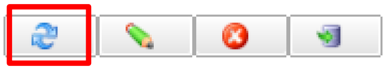
Procedure 56. Configure the SSO Domain

4. ☐	**IDIH Application Server GUI**: Login	1. Establish a GUI session on the IDIH app server <app server IP>. 2. Login as the **idihadmin** user.  ORACLE INTEGRATED DIAMETER INTELLIGENCE HUB User name Password Login IDIH Maintenance This portal lets y
5. ☐	**IDIH Application Server GUI**: Open the OAM portal	Select the **OAM** portal Icon to open the OAM web application.  ORACLE IDIH Portal Maintenance Alarm Forwarding Audit Viewer Log Viewer OAM ProTrace System Alarms

Procedure 56. Configure the SSO Domain

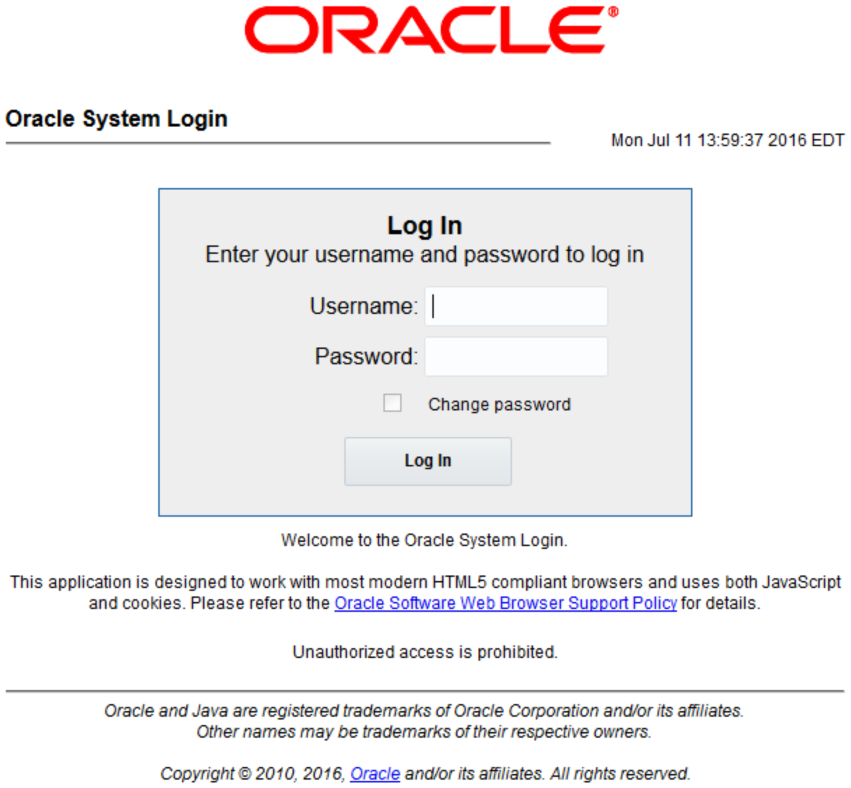
6. ☐	**IDIH Application Server GUI**: Configure the SSO domain	1. Navigate to **System > Single Sign On**.  ORACLE IDIH Home Mediation Applications System Help Single Sign On AVP Hiding Network IDIH Apply Changes IDIH OAM applica functio 2. From the **SSO Parameters** tab, select the **Edit Value** icon  System : Single Sign On SSO Zones SSO Parameters SSO Domain Domain Name : labs.nc.tekelec.com Name of the SSO Domain 3. Type a value for the **Domain Name**. ***Note:*** This should be the same domain name assigned in the DSR NOAM DNS Configuration (step 2.). 4. Select the **Save** icon.  5. Select the **Refresh** icon to display data saved for the remote zone.  Refresh Value

Procedure 56. Configure the SSO Domain

7. ☐	**IDIH Application Server GUI**: Configure the SSO remote zone	1. Navigate to **System > Single Sign On**.  ORACLE IDIH Home Mediation Applications System Help Single Sign On AVP Hiding Network IDIH Apply Changes IDIH OAM applica functio 2. From the **SSO Zones** tab.  System : Single Sign On SSO Zones SSO Parameters SSO Local Zone Local Name : Name of the SSO compatible local zone 3. Select the **Add** icon and type a value for field **Remote Name**.  SSO Remote Zones Remote Name X.509 Certificate 4. For field X.509 Certificate, paste the encoded certificate text from the clipboard.  X.509 Certificate -----BEGIN CERTIFICATE----- MIIENTCCAx2gAwIBAgIBA MA0GA1UECgwGT3JhY2xlMREwDwYDVQQLDAhBcHB CQEWEnN1cHBvcnRAb3JhY2xlLmNvbTAeFw0xNTA3M FDASBgNVBAcMC01vcnJpc3ZpbGxlMQ8wDQYDVQQK dHlwZT1BV1NTTzEhMB8GCSqGSIb3DQEJARYSc3Vwc ywYDdhXchb5bhORLUGCsSpo4RzHHlvKAu7DNi2GSs9 DrVBDyqDqmBhP1stxGAaBFhnbSuUms2Qgy4mKppfeyX LLx5+c5EwkS8OhB9AVqwjX+oETf58WYKgAgIX82c8rAW FoAUnwCZ+1CZucSz4AivgXb122X/SLYwDAYDVR0TBA tJi7N8HC9AEe0Sn8akEdE9pJHP7NwGjY1v5581Z2dnJ2 dxoXMVS5tEOO5Ea5PKk6Zyl3QCet1sEa5CRjilbOU94hj CERTIFICATE----- 5. Select the **Save** icon.  6. Select the **Refresh** icon to display the data saved for remote zone. 

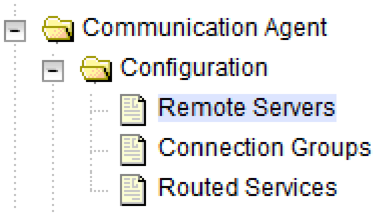
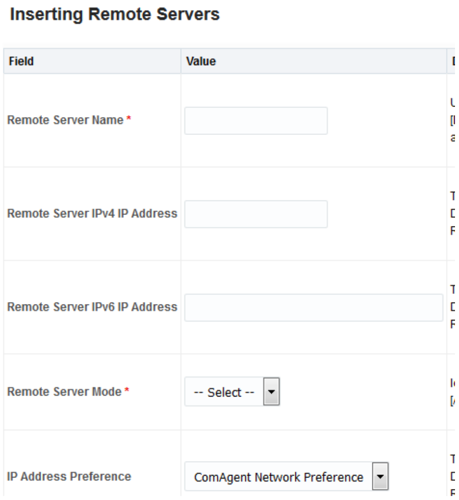
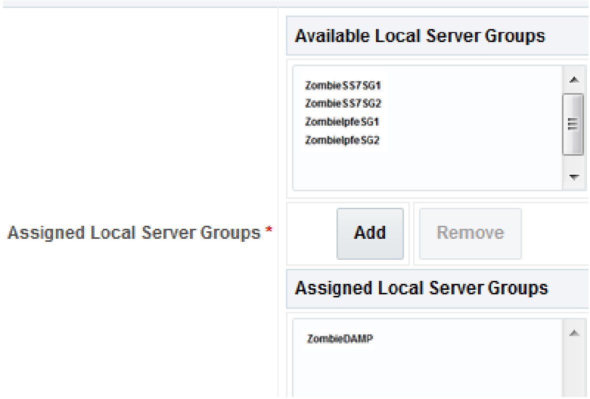
3.16.2.3 Configure IDIH in DSR

Procedure 57. Configure in DSR

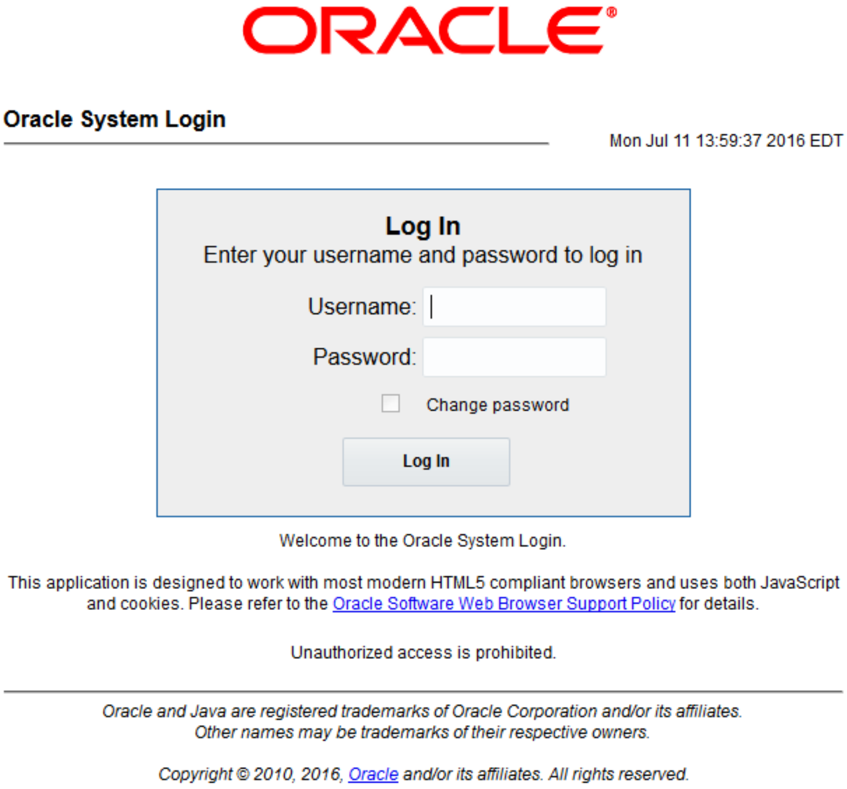
<table>
<tr><td colspan="3">This procedure completes IDIH integration on DSR.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>NOAM VIP GUI: Login</td><td>1. Establish a GUI session on the NOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of:
<code>https://<Primary_NOAM_VIP_IP_Address></code>
2. Login as the guiadmin user.


Oracle System Login
Mon Jul 11 13:59:37 2016 EDT
Log In
Enter your username and password to log in
Username:
Password:
☐ Change password

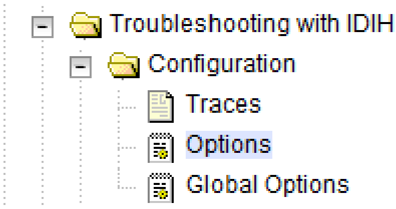
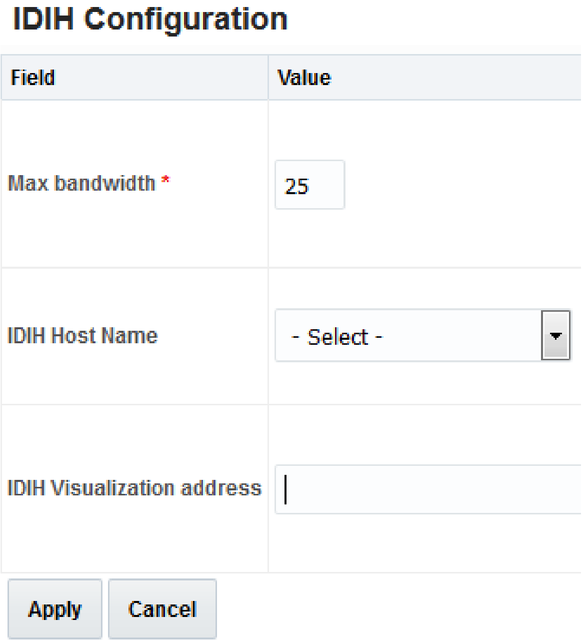
Welcome to the Oracle System Login.
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.
Unauthorized access is prohibited.
<i>Oracle and Java are registered trademarks 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></td></tr>
</table>

2. ☐	**NOAM VIP GUI**: Configure ComAgent cnnection	1. Navigate to **Communcation Agent > Configuration > Remote** Servers.  Communication Agent Configuration Remote Servers Connection Groups Routed Services 2. Click **Insert**. Insert Edit Delete 3. Add the **IDIH Mediation Server**. 4. For the **Remote Server IP Address**, type the IMI IP address of the IDIH Mediation Server. 5. For the **IP address Preference**, type the IP protocol preference (if IPv6 and IPv4 are configured). 6. Select the **Remote Server Mode** to server. 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 7. Select the **DA-MP Server Group** from the **Available Local Server Groups** column and click **Add** to assign.  Available Local Server Groups ZombieSS7SG1 ZombieSS7SG2 ZombieIpfeSG1 ZombieIpfeSG2 Assigned Local Server Groups * Add Remove Assigned Local Server Groups ZombieDAMP 8. Click **OK**.

Procedure 57. Configure in DSR

3. ☐	**SOAM VIP GUI**: Login	1. 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>` 2. Login as the **guiadmin** user.  ORACLE **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 57. Configure in DSR

4. ☐	**SOAM VIP GUI**: Configure IDIH hostname	1. Navigate to **Diameter > Troubleshooting with IDIH > Configuration > Options**.  Troubleshooting with IDIH Configuration Traces Options Global Options 2. From the IDIH Host Name options, select the **mediation** server. 3. Enter the fully qualified domain name (or IP address) of the App server as the **IDIH Visualization Address**. 4. Click **Apply**.  IDIH Configuration Field: Value Max bandwidth *: 25 IDIH Host Name: - Select - IDIH Visualization address:

3.16.2.4 Configure the Mail Server (Optional)

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.

Procedure 58. Configure Mail Server (Optional)

This procedure configures the SMTP mail server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**IDIH Application Server**: Login	Establish an SSH session to the IDIH Application Server and login as **admus**r.

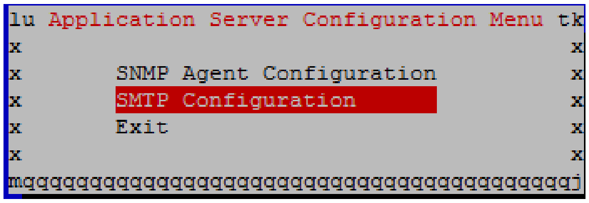
Procedure 58. Configure Mail Server (Optional)

2. ☐ **IDIH Application Server**: Configure the authenticated mail server

1. Enter the platcfg menu.

```
$ sudo su - platcfg
```

2. Navigate to **Application Server Configuration > SMTP Configuration**.



```
lu Application Server Configuration Menu tk
x                                         x
x       SNMP Agent Configuration          x
x       SMTP Configuration                x
x       Exit                              x
x                                         x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

3. Select **Edit**.
4. Enter these paraemters:
   - Mail Server IP Address
   - User
   - Password
   - Email Address (From)
   - Mail smtp timeout
   - Mail smtp connectiontimeout
   - SNMP over SSL used?
5. Select **OK**.
6. Exit out of platcfg by selecting **Exit**.

3.16.2.5 Configure the SNMP Management Server (Optional)

This procedure is optional; however, this option is required for forwarding (forwarding by SNMP filter defined) and is available only on the application server.

Procedure 59. Change SNMP Management Server (Optional)

This procedure configures the SNMP management server.

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

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

1. ☐	**IDIH Application Server**: Login	Establish an SSH session to the IDIH application server and login as **admusr**.

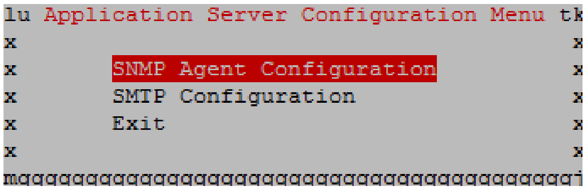
Procedure 59. Change SNMP Management Server (Optional)

<table>
<tr><td>2.
☐</td><td>IDIH Application Server: Configure SNMP management server</td><td>

1. Enter the platcfg menu.

```
$ sudo su - platcfg
```

2. Navigate to **Application Server Configuration > SNMP Agent Configuration**.



```
lu Application Server Configuration Menu tk
x                                          x
x       SNMP Agent Configuration           x
x       SMTP Configuration                 x
x       Exit                               x
x                                          x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

3. Select **Edit**.
4. Enter the **IP address** of the SNMP management server.

Note: The SNMP agent configuration is updated and the SNMP management server is automatically restarted.

5. Select **OK**.
6. Exit out of platcfg by selecting **Exit**.

</td></tr>
</table>

3.16.2.6 Change Network Interface (Optional)

Notes:

- 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. Changing this interface could degrade performance of the TTR transmission.
- A script is provided to manage the settings so the operator does not 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 and is the only specified interface 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.

Procedure 60. Change Network Interface (Optional)

<table>
<tr><td colspan="3">This procedure changes the default network interface.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>IDIH Mediation Server: Login</td><td>

1. Establish an SSH session to the IDIH mediation server login as **admusr**.
2. Login as tekelec user.

```
$ sudo su - tekelec
```

</td></tr>
</table>

Procedure 60. Change Network Interface (Optional)

2. ☐	**IDIH Mediation Server**: Execute the change interface script	`$ chgIntf.sh` 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 CTLR-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...
```

3.16.2.7 CPU Pinning

Follow section 3.13 for CPU pinning on servers that host IDIH VMs.

3.16.2.8 Generate Disaster Recovery FDC File (Optional)

Procedure 61. Back Up the Upgrade and Disaster Recovery FDC File (Optional)

This procedure generates a disaster recovery FDC file. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Identify backup server	Identify an external server to use as a backup server for this procedure. The server should not be co-located with any of these systems: • TVOE • PMAC • DSR NOAM • DSR SOAM
2. ☐	**PMAC Server**: Login	Establish an SSH session to the PMAC server and login as admusr.

Procedure 61. Back Up the Upgrade and Disaster Recovery FDC File (Optional)

3. ☐ **PMAC**: Verify upgrade fdc file exists

Execute these commands to verify the upgrade FDC file for IDIH exists.

```
$ cd /var/TKLC/smac/guest-dropin
$ ls –l *.xml
```

This output is expected:

```
-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
```

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

1. Log into the backup server identified in step 1. and copy the backup image to the customer server where it can be safely stored.
2. If the customer system is a Linux system, copy the backup image to the customer system.

```
$ sudo scp <idih_upgrade.xml>  /path/to/destination/
$ sudo scp <idih_install.xml>  /path/to/destination/
```

3. Enter the **admusr** user password and press **Enter**.

If the customer system is a Windows system, refer to [14], the Using WinSCP procedure, to copy the backup image to the customer system.

5. ☐ **PMAC Server**: Back up FDC file

1. Transfer the fdc file to the fdc directory so the file can be backed up with PMAC backups.
2. Ensure the directory where the backups will be stored exists.

```
$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/fdc
```

If you receive an error such as this:

```
-bash: ls: /usr/TKLC/smac/etc/fdc: No such file or
directory
```

Create the directory by issuing this command.

```
$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/fdc
```

3. Copy the fdc files to the fdc backup directory.

```
$ sudo cp /var/TKLC/smac/guest-
dropin<idih_upgrade.xml>  /usr/TKLC/smac/etc/fdc/
$ sudo cp /var/TKLC/smac/guest-
dropin<idih_install.xml>  /usr/TKLC/smac/etc/fdc/
```

3.17 Post Installation Procedures

3.17.1 Optimization (DSR and Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 (10Gbps) Only)

Procedure 62. Optimization Procedure

This procedure runs optimization scripts for Oracle X5-2/Netra X5-2/X6-2/HP DL380 Gen 9 (10Gbps) only.

Prerequisite: Completed all previous DSR installation procedures.

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

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

1. ☐	**DSR NOAM VIP**: Login	Establish an SSH to the NOAM VIP address and login as **admusr**.

2.
☐
	DSR NOAM VIP: Execute the performance optimization script on the active NOAM	`$ cd /usr/TKLC/dsr/bin/`
		`$ sudo ./rmsNoamConfig.sh`
		Configuration Successful output should display.

3.17.2 Configure ComAgent Connections (DSR and SDS Only)

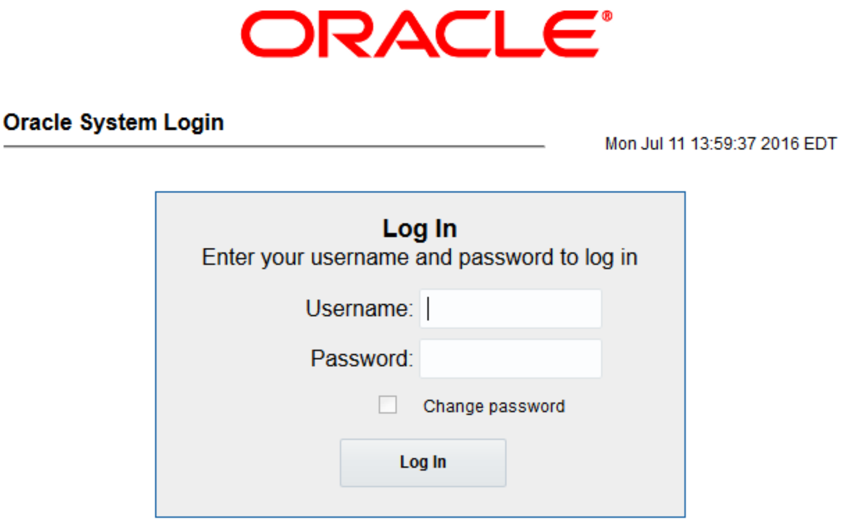
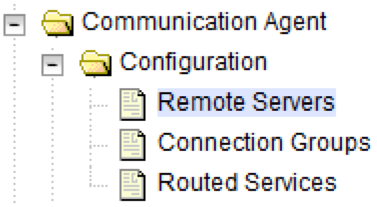
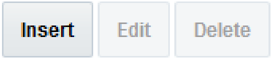
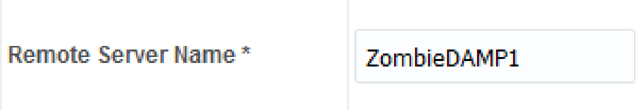
Procedure 63. Configure ComAgent Connections

This procedure configures ComAgent connections on DSR/SDS for use in the FABR application.

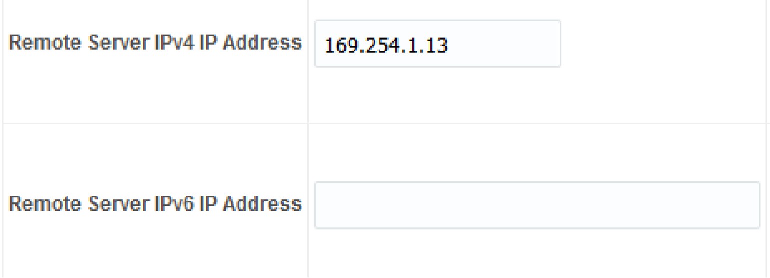
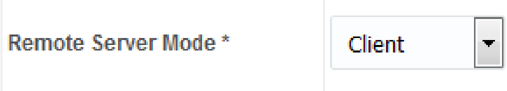
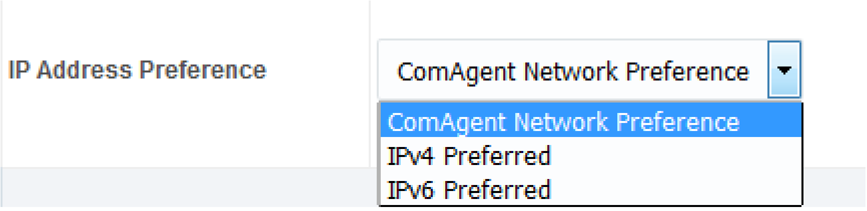
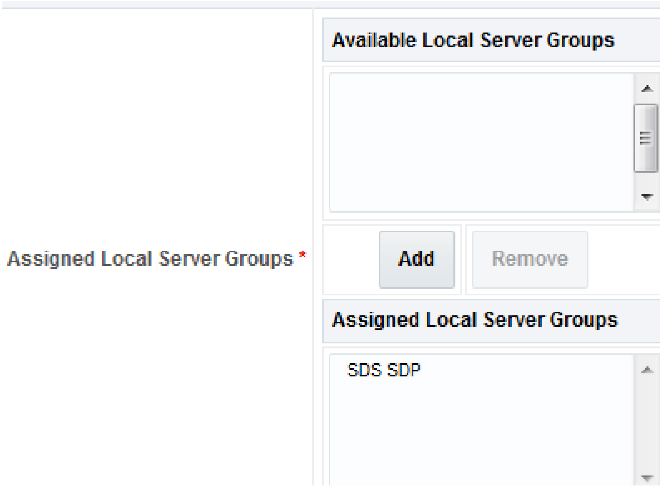
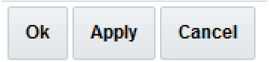
Prerequisite: Activated FABR application.

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

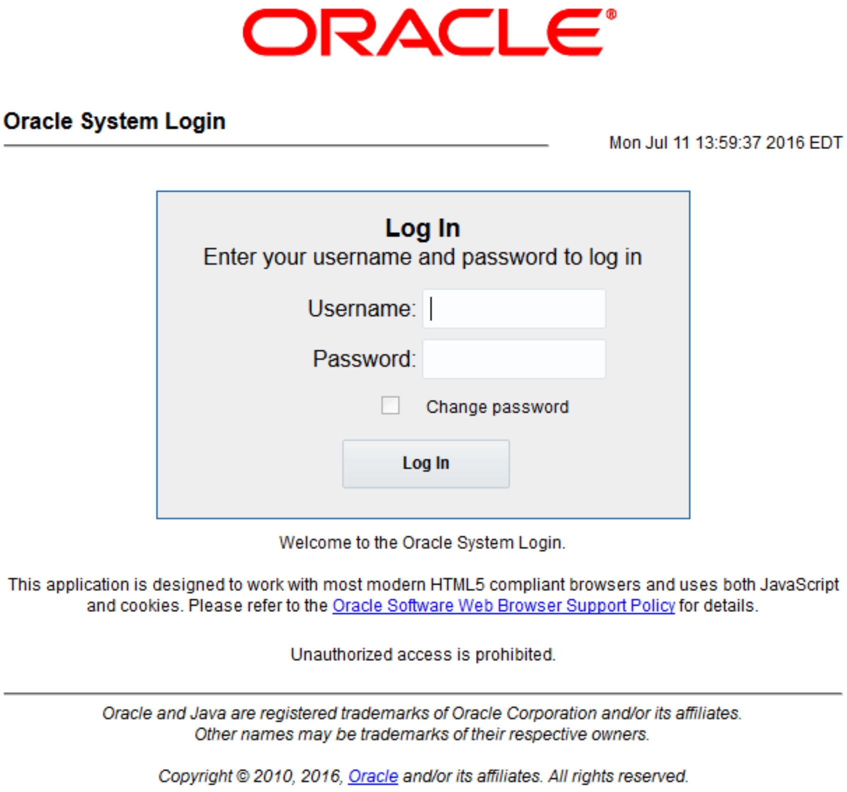
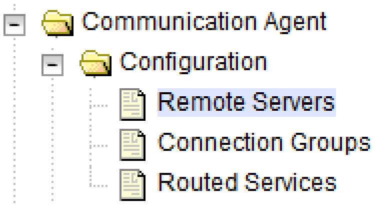
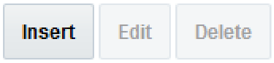
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**SDS NOAM VIP GUI**: Login	1. 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>` 2. Login as the **guiadmin** user.  ORACLE **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
2. ☐	**SDS NOAM VIP GUI**: Configure remote server IP address	1. Navigate to **Communication Agent > Configuration > Remote Servers**.  Communication Agent Configuration Remote Servers Connection Groups Routed Services 2. Click **Insert**. 
3. ☐	**SDS NOAM VIP GUI**: Configure remote server IP address	1. Enter the **Remote Server Name** for the DSR MP server.  Remote Server Name * ZombieDAMP1 2. Enter the **Remote Server IMI IP Address**.

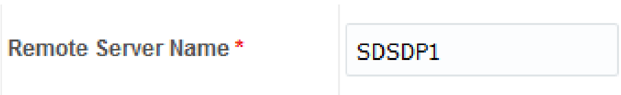
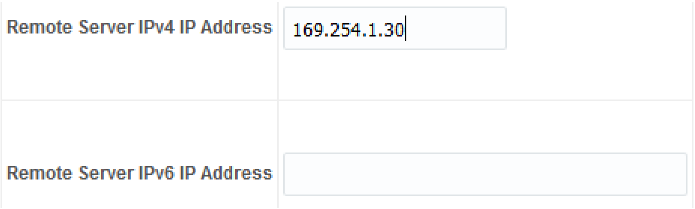
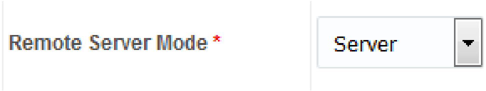
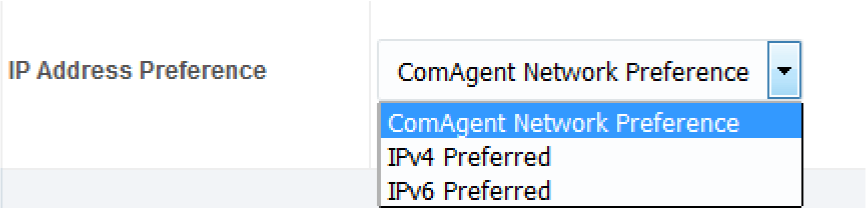
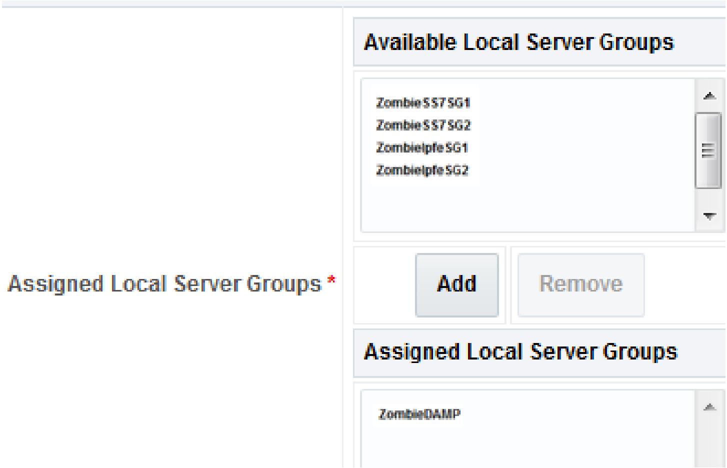
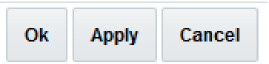
Procedure 63. Configure ComAgent Connections

		 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. 3. Select **Client** from the Remote Server Mode options.  Remote Server Mode *: Client 4. Select **IP Address Preference** (ComAgent Network Preference, IPv4, or IPv6).  IP Address Preference: ComAgent Network Preference ComAgent Network Preference IPv4 Preferred IPv6 Preferred 5. 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 Add Remove Assigned Local Server Groups Assigned Local Server Groups: SDS SDP 6. Click **Apply**.  Ok Apply Cancel
4. ☐	**SDS NOAM VIP GUI**: Repeat	Repeat steps 2. though 3. for each remote MP in the same SOAM NE.

Procedure 63. Configure ComAgent Connections

5. ☐	**DSR NOAM VIP GUI**: Login	1. Establish a GUI session on the DSR NOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of: `https://<Primary_DSR_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*
6. ☐	**DSR NOAM VIP GUI**: Configure remote server IP address	1. Navigate to **Communication Agent > Configuration > Remote Servers**.  Communication Agent Configuration Remote Servers Connection Groups Routed Services 2. Click **Insert**. 

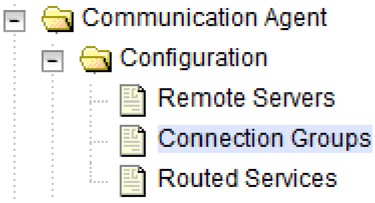
Procedure 63. Configure ComAgent Connections

7. ☐	**DSR NOAM VIP GUI**: Configure remote server IP address	1. Enter the **Remote Server Name** for the SDS DP server: Remote Server Name * SDSDP1 2. Enter the **Remote Server IMI IP Address**. 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. 3. Select **Server** from the Remote Server Mode options. Remote Server Mode * Server 4. Select **IP Address Preference** (ComAgent Network Preference, IPv4, or IPv6). IP Address Preference ComAgent Network Preference ComAgent Network Preference IPv4 Preferred IPv6 Preferred 5. Select the **Local Server Group** from the available SDS DP server groups and click **Add** to assign.  Available Local Server Groups ZombieSS7SG1 ZombieSS7SG2 ZombieIpfeSG1 ZombieIpfeSG2 Add Remove Assigned Local Server Groups * ZombieDAMP 6. Click **Apply**.  Ok Apply Cancel
8. ☐	**DSR NOAM VIP GUI**: Repeat	Repeat steps 6. through 7. for each remote DP in the same SOAM NE.

Procedure 63. Configure ComAgent Connections

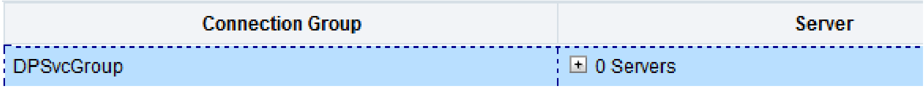
<table>
<tr>
<td>9.
☐</td>
<td>DSR NOAM VIP GUI: Edit connection groups</td>
<td>

1. Navigate to **Communication Agent > Configuration > Connection Groups**.



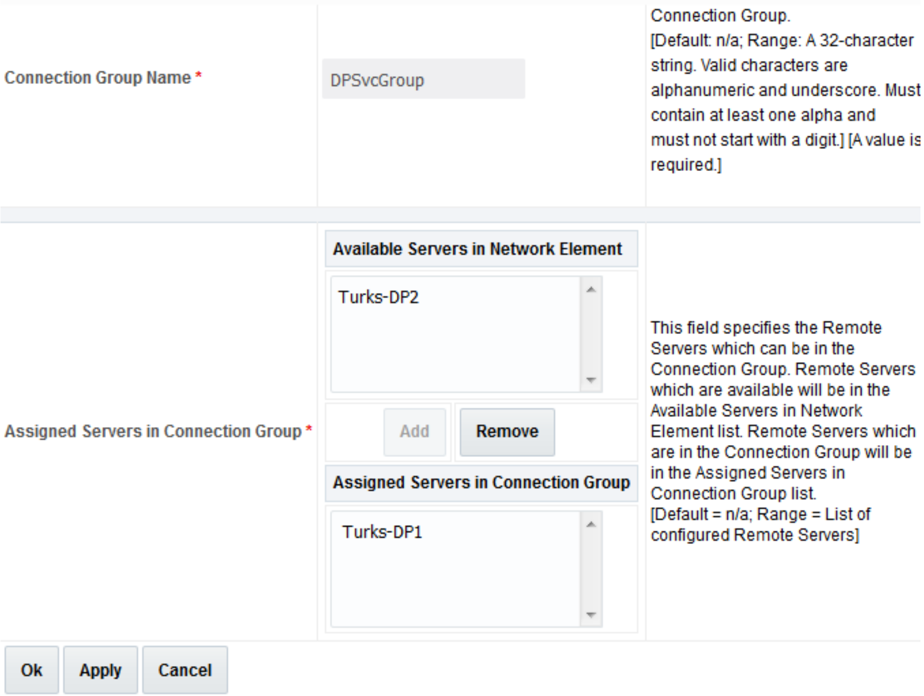
2. Select the **DPSvcGroup** connection group.

If DPSvcGroup Connection Group is not present please refer section 3.17.3 Activate Optional Features to actiate FABR apppication.



Connection Group	Server
DPSvcGroup	⊞ 0 Servers

3. Click **Edit**.
4. Select the desired DP servers from the **Available Servers in Network Element**.
5. Click **Add**.



Connection Group Name * DPSvcGroup

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.]

Assigned Servers in Connection Group *

Available Servers in Network Element: Turks-DP2

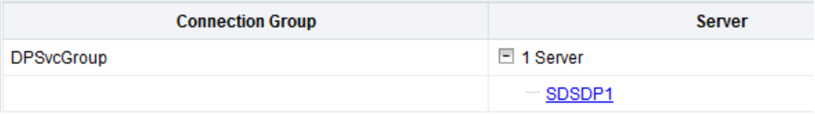
Assigned Servers in Connection Group: Turks-DP1

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]

6. Click **OK**.

</td>
</tr>
<tr>
<td>10.
☐</td>
<td>DSR NOAM VIP GUI: Verify the correct number of servers in group</td>
<td>

Verify the correct number of servers are in the connection group.



Connection Group	Server
DPSvcGroup	⊟ 1 Server
	SDSDP1

</td>
</tr>
</table>

3.17.3 Activate Optional Features

Procedure 64. Activate Optional Features

This procedure installs DSR optional components once regular installation is complete. ***Prerequisite***: Completed all previous DSR installation procedures. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Refer to Installation Guides for optional features to complete installation	Refer to section 1.5 for a list of feature install documents whose procedures are to be executed at this moment.

2. ☐	**DR NOAM**:
	Feature activation
		1. If the DR NOAM was configured in section 3.15.3, and MAPIWF has been activated in step 1. ; ssh to the active DR NOAM and login as **admusr**.
		2. Execute these commands.
		`$ cd /usr/TKLC/dsr/prod/maint/loaders/activate`
		`$ sudo ./load.mapinterworkingActivateAsourced`
		3. Repeat this step for the standby DR NOAM.

3.17.4 Shared Secret Encryption Key Revocation (RADIUS Only)

Procedure 65. Shared Secret Encryption Key Revocation (RADIUS Only)

This procedure changes the shared secret encryption key on DSR RADIUS setup. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact 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] DSR RADIUS Shared Secret Encryption Key Revocation. ***Note:*** It is highly recommended to change the key after installation due to security reasons.

3.17.5 Enable/Disable DTLS (SCTP Diameter Connections Only)

Procedure 66. Enable/Disable DTLS (SCTP Diameter Connections Only)

This procedure prepared clients before configuring SCTP diameter connections. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact 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. Customers should prepare clients before the DSR connections are established after installation. This ensures the DSR-to-client SCTP connection establishes 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.

3.17.6 Back Up TVOE Configuration

Procedure 67. Back Up TVOE Configuration

This procedure backs up each TVOE rack mounter server after a successful installation. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Identify backup server	Identify an external server to use as a backup server for this procedure. The server should not be co-located with any of these systems: • TVOE • PMAC • DSR NOAM • DSR SOAM • SDS NOAM • SDS DP SOAM
2. ☐	**TVOE Server**: Login	Establish an SSH session to the TVOE host server and login as **admusr**.

Procedure 67. Back Up TVOE Configuration

3. ☐ **TVOE Server**: Back up the ISO file

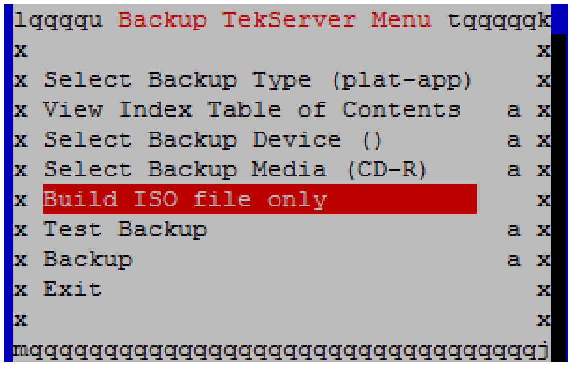
1. Enter the platcfg menu from the TVOE server.

```
$ sudo su - platcfg
```

2. Navigate to **Maintenance > Backup and Restore > Backup Platform (CD/DVD)**.

Note: If no cdrom device is found by TPD, a **No disk device available. This is normal on systems without a cdrom device** error displays. Press **Enter**.

3. Navigate to **Build ISO file only** and press **Enter**.



```
lqqqqu Backup TekServer Menu tqqqqqk
x                                  x
x Select Backup Type (plat-app)    x
x View Index Table of Contents   a x
x Select Backup Device ()        a x
x Select Backup Media (CD-R)     a x
x Build ISO file only              x
x Test Backup                    a x
x Backup                         a x
x Exit                             x
x                                  x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

Note: Creating the ISO image may happen so quickly that this screen may only display for an instant.

4. Exit out of platcfg by selecting **Exit**.

After the ISO is created, platcfg returns to the Backup TekServer menu. The ISO has 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**.

5. Move the TVOE backup to a customer provided backup server for safe keeping.

4. ☐ **Backup Server**: Transfer TVOE files to backup server

1. Login to the backup server identified in step 1. and copy the backup image to the customer server where it can be safely stored.
2. If the customer system is a Linux system, copy the backup image to the customer system.

```
$ sudo scp tvoexfer@<TVOE IP Address>:/var/TKLC/bkp/*
/path/to/destination/
```

3. Move the TVOE backup to a customer-provided backup server for safe keeping.
4. Enter the tvoexfer user password and press **Enter.**

If the customer system is a Windows system, refer to [14], the Using WinSCP procedure, to copy the backup image to the customer system.

5. ☐ Repeat for additional TVOE servers

Repeat steps 2. through 4. for additional TVOE servers

3.17.7 Back Up PMAC Application

Procedure 68. Back Up PMAC Application

This procedure backs up each PMAC application.

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

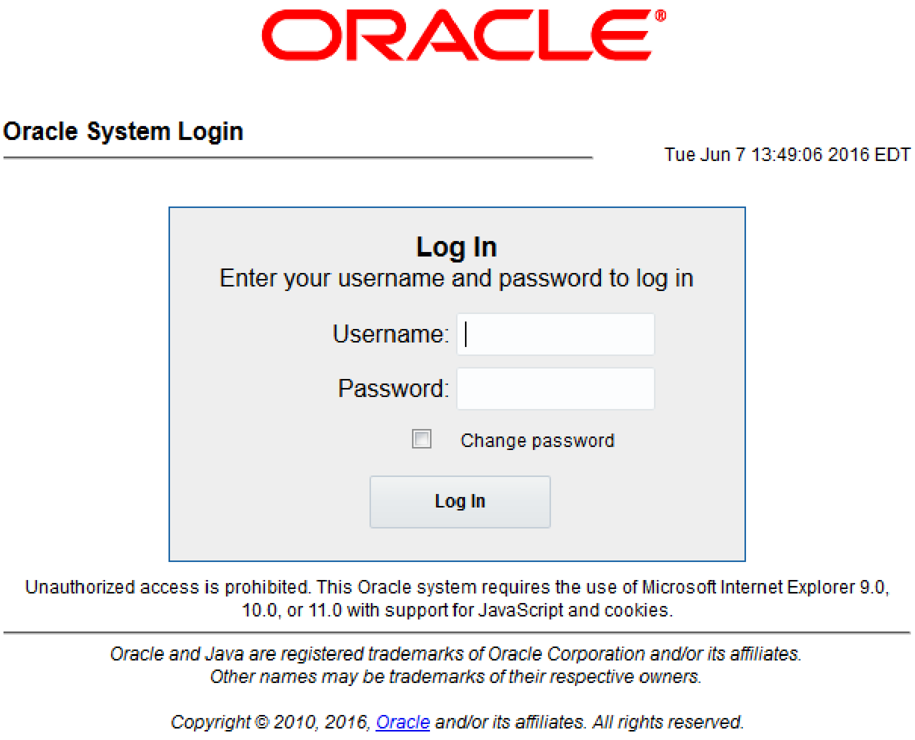
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	Identify backup server	Identify an external server to use as a backup server for this procedure. The server should not be co-located with any of these systems: • TVOE • PMAC • DSR NOAM • DSR SOAM • SDS NOAM • SDS DP SOAM
2. ☐	**PMAC Server**: Login	Establish an SSH session to the PMAC server and login as **admusr**.

3.
☐
	PMAC Server: Build backup file	Execute this command from the PMAC server:
		`$ sudo /usr/TKLC/smac/bin/pmacadm backup`
		`PM&C backup been successfully initiated as task ID 7`
		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**.

Procedure 68. Back Up PMAC Application

<table>
<tr>
<td>4.
☐</td>
<td>PMAC GUI: Login</td>
<td>
1. Open the web browser and navigate to the PMAC GUI:
<pre>http://<PMAC_network_IP></pre>
2. Login as the guiadmin user.



Oracle System Login

Tue Jun 7 13:49:06 2016 EDT

Log In

Enter your username and password to log in

Username:

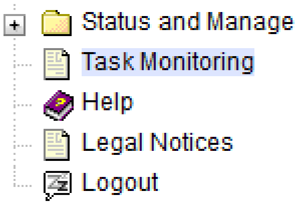
Password:

☐ Change password

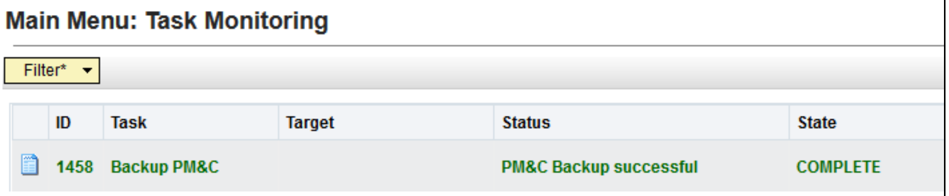
Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.

<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>
</td>
</tr>
<tr>
<td>5.
☐</td>
<td>PMAC Server GUI: Monitor/Verify backup task completion</td>
<td>
1. Navigate to Task Monitoring.



2. Monitor the Backup PMAC task.


Main Menu: Task Monitoring

<table>
<tr><th></th><th>ID</th><th>Task</th><th>Target</th><th>Status</th><th>State</th></tr>
<tr><td></td><td>1458</td><td>Backup PM&C</td><td></td><td>PM&C Backup successful</td><td>COMPLETE</td></tr>
</table>

<i>Note:</i> Alternatively, you can monitor the backup task by executing this command:
<pre>$ sudo pmaccli getBgTasks</pre>
</td>
</tr>
</table>

Procedure 68. Back Up PMAC Application

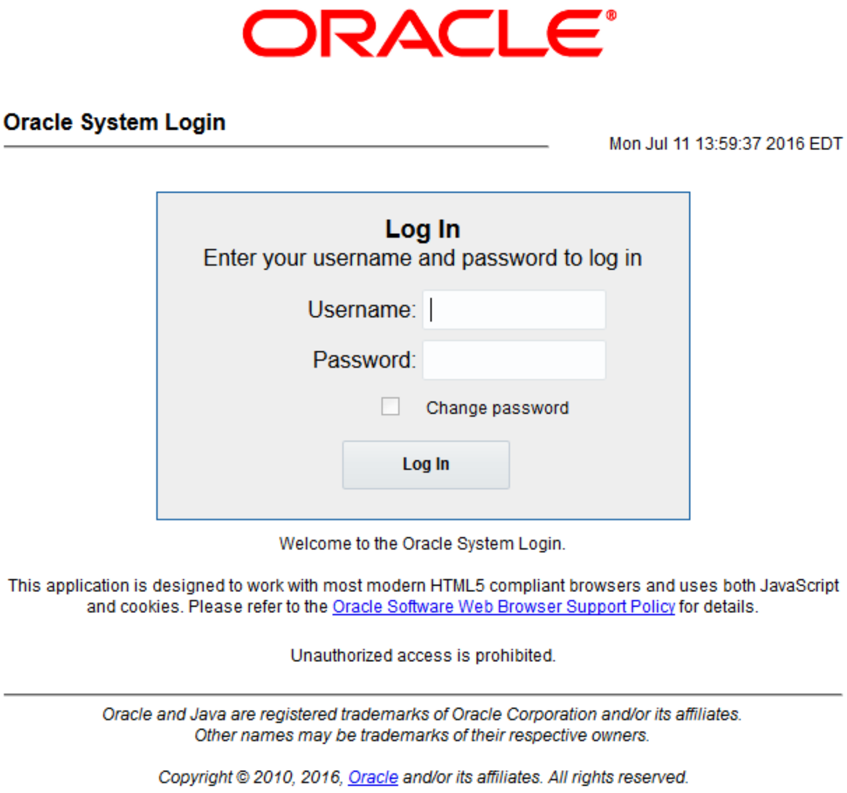
6. ☐	**Backup Server**: transfer PMAC file to backup server	1. Log into the backup server identified in step 1. and copy the backup image to the customer server where it can be safely stored. 2. If the customer system is a Linux system, copy the backup image to the customer system. `$ sudo scp admusr@<PMAC_IP_Address>:/var/TKLC/smac/backup/* /path/to/destination/` 3. Enter the **admusr** user password and press **Enter**. If the customer system is a Windows system, refer to [14], the Using WinSCP procedure, to copy the backup image to the customer system.
7. ☐	Repeat for additional PMAC servers	Repeat steps 2. though 6. for additional PMAC servers.

3.17.8 Back Up NOAM Database

Procedure 69. Back Up NOAM Database

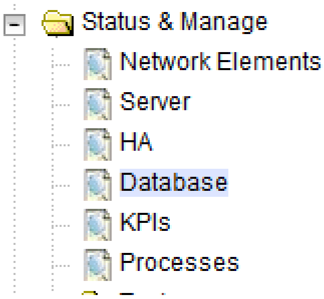
This procedure backs up the NOAM database. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Identify backup server	Identify an external server to use as a backup server for this procedure. The server should not be co-located with any of these systems: • TVOE • PMAC • DSR NOAM • DSR SOAM • SDS NOAM • SDS DP SOAM

Procedure 69. Back Up NOAM Database

2. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  ORACLE **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.*

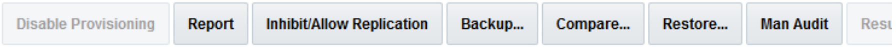
Procedure 69. Back Up NOAM Database

<table>
<tr>
<td>3.
☐</td>
<td>**SOAM VIP GUI**: Perform database backup</td>
<td>
1. Navigate to **Status & Manage > Database**.


Status & Manage
Network Elements
Server
HA
Database
KPIs
Processes

2. Select the active NOAM.

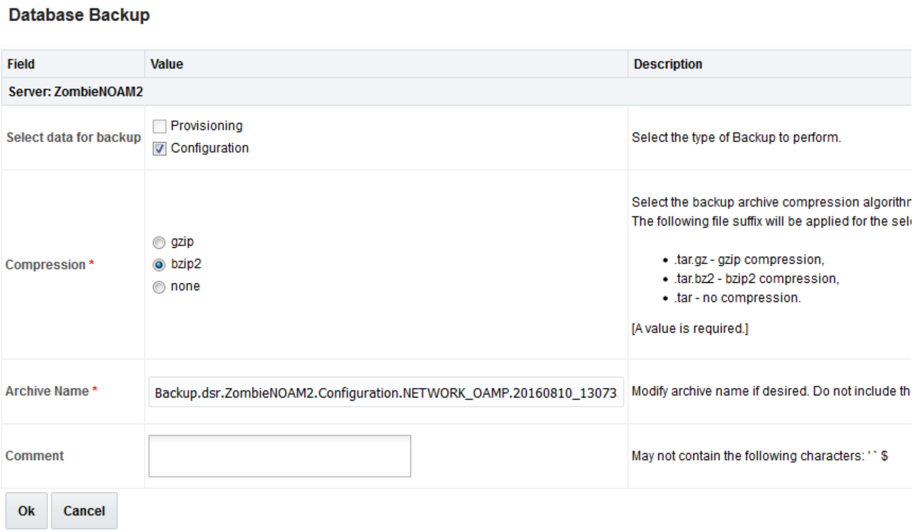
3. Click **Backup**.


Disable Provisioning
Report
Inhibit/Allow Replication
Backup...
Compare...
Restore...
Man Audit
Resu

4. Select the desired file compression method.

5. Provide the archive file name, if needed.

6. Click **OK**.



Database Backup

<table>
<tr><th>Field</th><th>Value</th><th>Description</th></tr>
<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 algorithr
The following file suffix will be applied for the sel
• .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 th</td></tr>
<tr><td>Comment</td><td></td><td>May not contain the following characters: ' ` $</td></tr>
</table>

</td>
</tr>
</table>

Procedure 69. Back Up NOAM Database

4.
☐
	Backup Server: Transfer file to backup server	1. Login to the backup server identified in step 1. and copy the backup image and key file (RADIUS only) to the customer server where it can be safely stored.
		2. If the customer system is a Linux system, copy the backup image to the customer system.
		`$ sudo scp admusr@<NOAM`
		`VIP>:/var/TKLC/db/filemgmt/backup/*`
		`/path/to/destination/`
		3. Encrypt the key file before sending it to the filemgmt area.
		`$ ./sharedKrevo –encr`
		4. Copy key file to customer server.
		`$ sudo scp admusr@<NOAM`
		`VIP>:/var/TKLC/db/filemgmt/DpiKf.bin.encr`
		`/path/to/destination/`
		5. Enter the **admusr** user password and press **Enter**.
		If the customer system is a Windows system, refer to [14], the Using WinSCP procedure, to copy the backup image to the customer system.

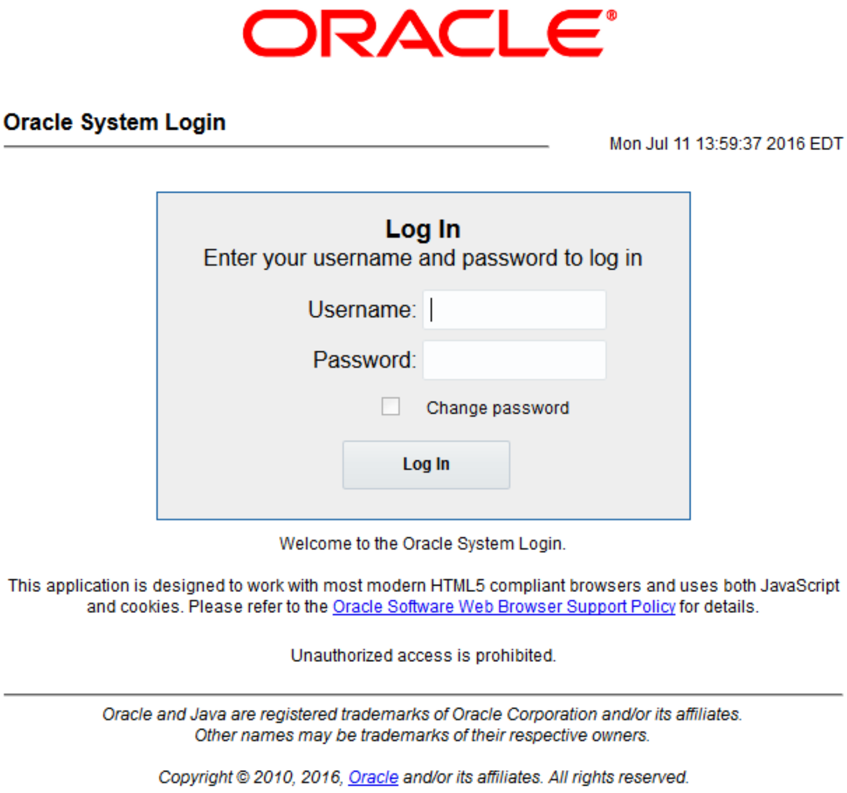
5. ☐	Repeat for additional NOAM aervers	Repeat steps 2. though 4. for additional DSR and SDS NOAM sites.

3.17.9 Back Up SOAM Database

Procedure 70. Back Up SOAM Database

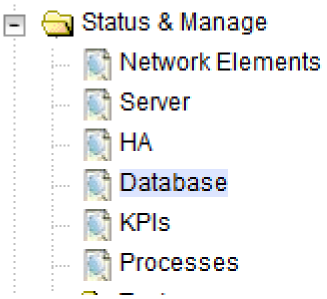
<table>
<tr><td colspan="3">This procedure backs up the SOAM database.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>Identify backup server</td><td>Identify an external server to use as a backup server for this procedure. The server should not be co-located with any of these systems:
• TVOE
• PMAC
• DSR NOAM
• DSR SOAM
• SDS NOAM
• SDS DP SOAM</td></tr>
</table>

Procedure 70. Back Up SOAM Database

2. ☐	**SOAM VIP GUI**: Login	1. 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>` 2. Login as the **guiadmin** user.  ORACLE **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.*

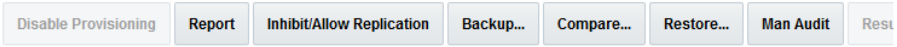
Procedure 70. Back Up SOAM Database

<table>
<tr>
<td>3.
☐</td>
<td>SOAM VIP GUI: Perform database backup</td>
<td>
1. Navigate to Status & Manage > Database.


Status & Manage
Network Elements
Server
HA
Database
KPIs
Processes

2. Select the active SOAM.

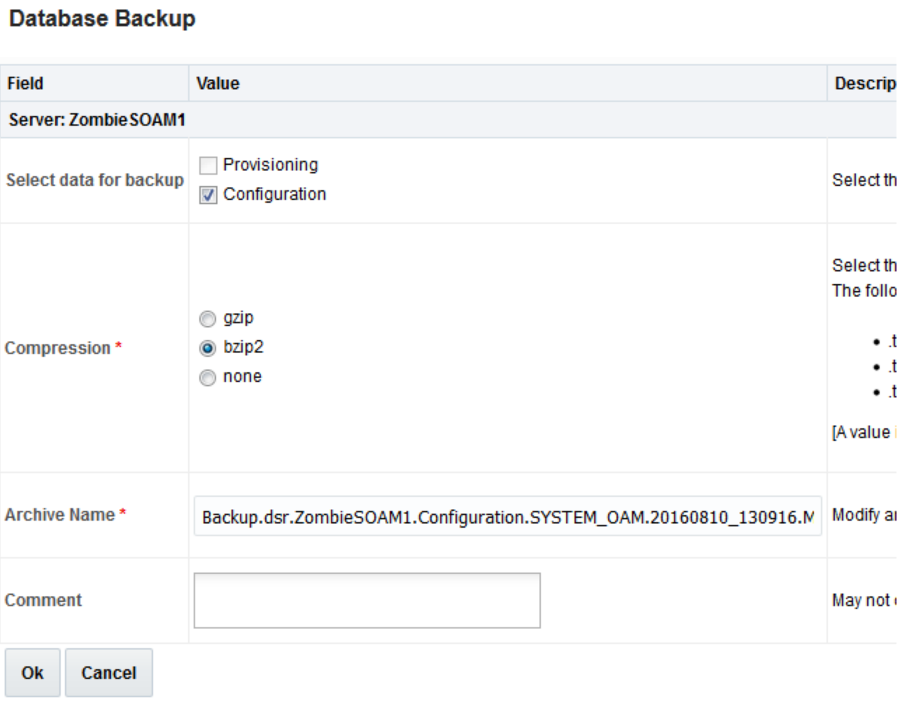
3. Click Backup.


Disable Provisioning
Report
Inhibit/Allow Replication
Backup...
Compare...
Restore...
Man Audit
Resu

4. Select the desired file compression method.

5. Provide the archive file name, if needed.

6. Click OK.



Database Backup

<table>
<tr><th>Field</th><th>Value</th><th>Descrip</th></tr>
<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 a</td></tr>
<tr><td>Comment</td><td></td><td>May not</td></tr>
</table>

</td>
</tr>
</table>

Procedure 70. Back Up SOAM Database

4. ☐	**Backup Server**: Transfer SOAM file to backup server	1. Log into the backup server identified in step 1. and copy the backup image to the customer server where it can be safely stored. 2. If the customer system is a Linux system, copy the backup image to the customer system. `$ sudo scp admusr@<SOAM VIP>:/var/TKLC/db/filemgmt/backup/* /path/to/destination/` 3. Enter the **admusr** user password and press **Enter**. If the customer system is a Windows system, refer to [14], the Using WinSCP procedure, to copy the backup image to the customer system.
5. ☐	Repeat for additional TVOE servers	Repeat steps 2. through 4. for additional DSR SOAM sites.

Appendix A. Pre-IPM Procedures

Appendix A.1 Set the Server's CMOS Clock

Set the date and time in the server's CMOS clock accurately before running the IPM procedures.

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.

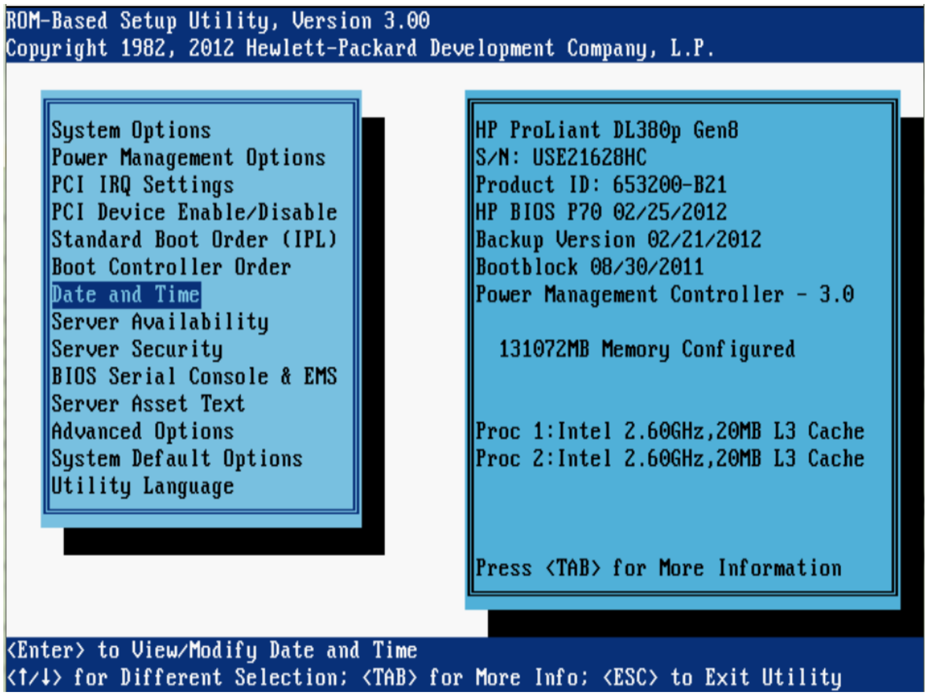
Appendix A.2 Configure the RMS Server BIOS Settings

Appendix A.2.1 Configure HP Gen 8 Servers

Procedure 71. Configure HP Gen 8 Server BIOS Settings

This procedure configures HP DL380 server BIOS settings. Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**HP DL380 Server**: Connect VGA monitor and USB keyboard	Connect using a VGA monitor and USB keyboard.

Procedure 71. Configure HP Gen 8 Server BIOS Settings

2. ☐	**HP DL380 Server**: Reboot	Reboot the server and after the server is powered on, press **F9** when asked to access the ROM-Based Setup Utility.  ROM-Based Setup Utility, Version 3.00 Copyright 1982, 2012 Hewlett-Packard Development Company, L.P. HP ProLiant DL380p Gen8 S/N: USE21628HC Product ID: 653200-B21 HP BIOS P70 02/25/2012 Backup Version 02/21/2012 Bootblock 08/30/2011 Power Management Controller - 3.0 131072MB Memory Configured Proc 1:Intel 2.60GHz,20MB L3 Cache Proc 2:Intel 2.60GHz,20MB L3 Cache Press <TAB> for More Information <Enter> to View/Modify Date and Time <↑/↓> for Different Selection; <TAB> for More Info; <ESC> to Exit Utility System Options Power Management Options PCI IRQ Settings PCI Device Enable/Disable Standard Boot Order (IPL) Boot Controller Order Date and Time Server Availability Server Security BIOS Serial Console & EMS Server Asset Text Advanced Options System Default Options Utility Language
3. ☐	**HP DL380 Server**: Set the date and time	1. Select **Date and Time** to set the date and time to GMT (Greenwich Mean Time). 2. Press **Esc** to navigate to the main menu.
4. ☐	**HP DL380 Server**: Set the server availability	1. Select **Server Availability**. 2. Change Automatic Power-On to **Enabled**. 3. Change Power-On Delay to **No Delay**. 4. Press **Esc** to navigate to the main menu.
5. ☐	**HP DL380 Server**: System options	1. Select **System Options**. 2. Select **Power Management Options**. 3. Select **HP Power Regulator**. 4. Select **HP Status High Performance Mode**. 5. Press **Esc** to navigate to the main menu.
6. ☐	**HP DL380 Server**: Power management options	1. Select **System Options**. 2. Select **Processor Options**. 3. Change Intel Virtualization Technology to **Enabled**. 4. Select **Serial Port Options**. 5. Press **Esc** to return to System Options.

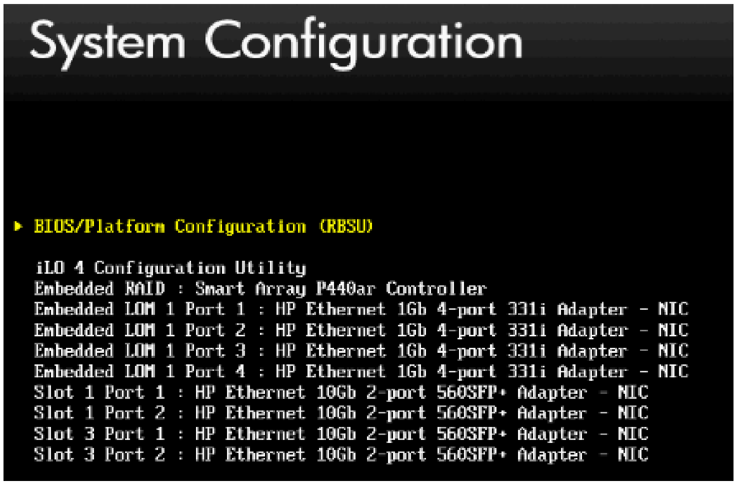
Procedure 71. Configure HP Gen 8 Server BIOS Settings

7. ☐	**HP DL380 Server**: Exit ROM-based utility	Press **Esc** to **Save & Exit** from the ROM-Based Setup Utility.

Appendix A.2.2 Configure HP Gen 9 Servers

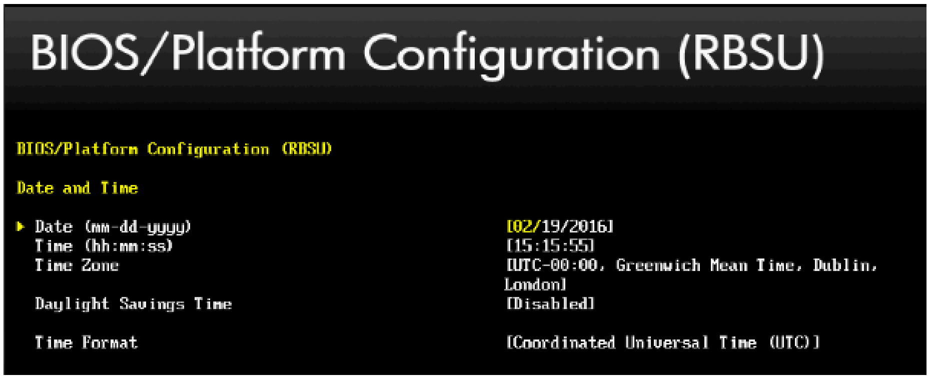
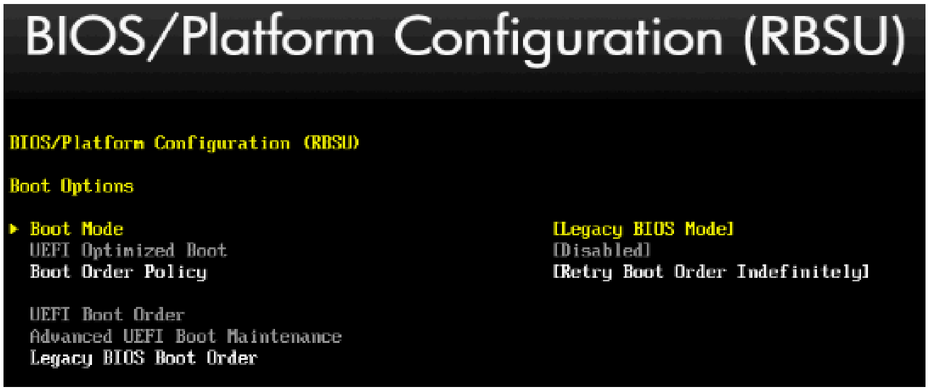
The HP Gen 9 systems can have UEFI boot enabled. Since TPD is configured to use the legacy BIOS option, rack mount Gen 9 servers should have their BIOS settings checked before IPM. Rack mount servers should also have the iLO serial port configured at this time. Directions for both settings are provided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

Procedure 72. Configure HP Gen 8 Server BIOS Settings

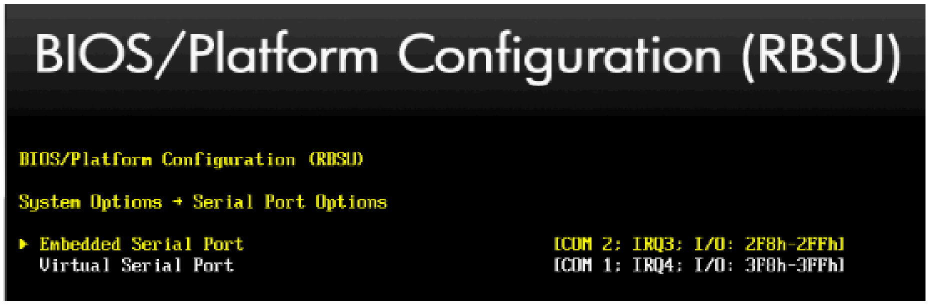
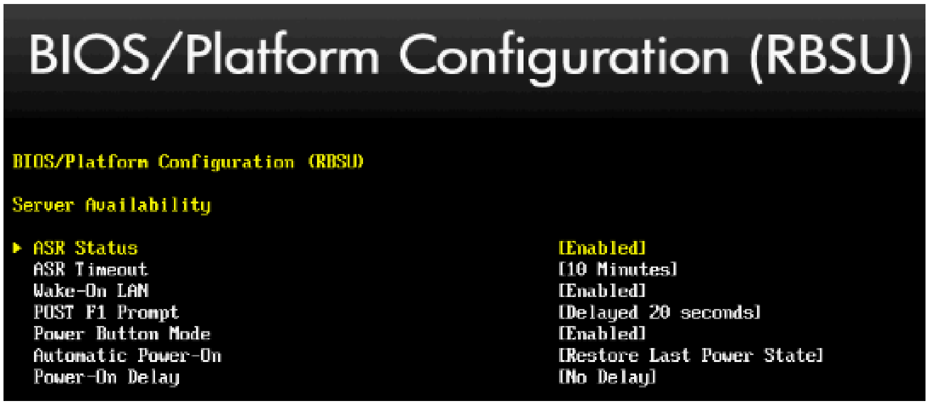
<table>
<tr><td colspan="3">This procedure configures HP Gen 9 server BIOS settings.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under ach step number.
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>HP Gen 9 Server: Connect VGA Monitor and USB Keyboard</td><td>Connect via a VGA monitor and USB keyboard.</td></tr>
<tr><td>2.
☐</td><td>HP Gen 9 Server: Reboot</td><td>Reboot the server. After the server is powered on, press F9 when prompted to access the System Utilities menu.
Navigate to System Configuration > BIOS/Platform Configuration (RBSU).

System Configuration
▸ BIOS/Platform Configuration (RBSU)
iLO 4 Configuration Utility
Embedded RAID : Smart Array P440ar Controller
Embedded LOM 1 Port 1 : HP Ethernet 1Gb 4-port 331i Adapter - NIC
Embedded LOM 1 Port 2 : HP Ethernet 1Gb 4-port 331i Adapter - NIC
Embedded LOM 1 Port 3 : HP Ethernet 1Gb 4-port 331i Adapter - NIC
Embedded LOM 1 Port 4 : HP Ethernet 1Gb 4-port 331i Adapter - NIC
Slot 1 Port 1 : HP Ethernet 10Gb 2-port 560SFP+ Adapter - NIC
Slot 1 Port 2 : HP Ethernet 10Gb 2-port 560SFP+ Adapter - NIC
Slot 3 Port 1 : HP Ethernet 10Gb 2-port 560SFP+ Adapter - NIC
Slot 3 Port 2 : HP Ethernet 10Gb 2-port 560SFP+ Adapter - NIC

</td></tr>
</table>

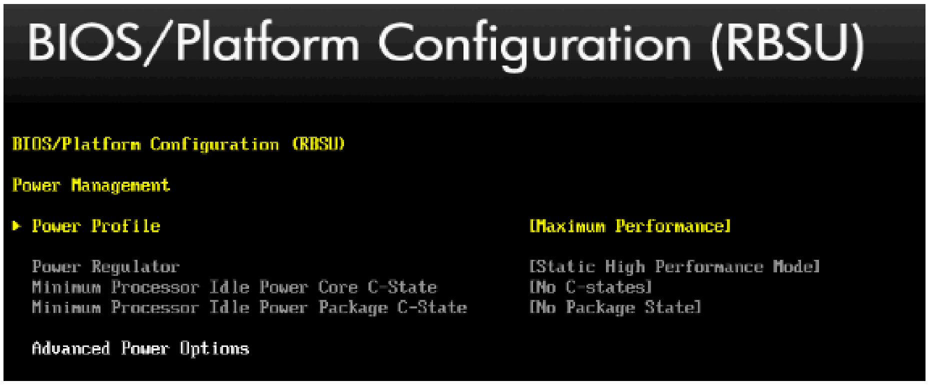
Procedure 72. Configure HP Gen 8 Server BIOS Settings

3. ☐	**HP Gen 9 Server**: Set the date and time	1. Navigate to **Date and Time**. 2. Set the data and time, and time format. BIOS/Platform Configuration (RBSU) BIOS/Platform Configuration (RBSU) Date and Time ▸ Date (mm-dd-yyyy) [02/19/2016] Time (hh:mm:ss) [15:15:55] Time Zone [UTC-00:00, Greenwich Mean Time, Dublin, London] Daylight Savings Time [Disabled] Time Format [Coordinated Universal Time (UTC)] 3. Press **Esc** to navigate to the main menu.
4. ☐	**HP Gen 9 Server**: System configuration	1. 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 the next step. BIOS/Platform Configuration (RBSU) BIOS/Platform Configuration (RBSU) Boot Options ▸ Boot Mode [Legacy BIOS Mode] UEFI Optimized Boot [Disabled] Boot Order Policy [Retry Boot Order Indefinitely] UEFI Boot Order Advanced UEFI Boot Maintenance Legacy BIOS Boot Order 2. Select **Legacy BIOS Mode**. 3. Press **Esc** once to back out to the BIOS/Platform Configuration (RBSU) menu.

Procedure 72. Configure HP Gen 8 Server BIOS Settings

5. ☐	**HP Gen 9 Server**: System Configuration	1. Select the **System Options** menu 2. Select the **Serial Port Options** menu. 3. Change Embedded Serial Port to **COM2**. 4. Change Virtual Serial Port to **COM1**.  BIOS/Platform Configuration (RBSU) BIOS/Platform Configuration (RBSU) System Options → Serial Port Options ▸ Embedded Serial Port [COM 2: IRQ3: I/O: 2F8h-2FFh] Virtual Serial Port [COM 1: IRQ4: I/O: 3F8h-3FFh] 5. Press **Esc** twice to back out to the BIOS/Platform Configuration (RBSU) menu.
6. ☐	**HP Gen 9 Server**: Server Availability	1. Select the **Server Availability** menu. 2. Set the Automatic Power-On to **Restore Last Power State**. 3. Set Power-On Delay to **No Delay**.  BIOS/Platform Configuration (RBSU) BIOS/Platform Configuration (RBSU) Server Availability ▸ ASR Status [Enabled] ASR Timeout [10 Minutes] Wake-On LAN [Enabled] POST F1 Prompt [Delayed 20 seconds] Power Button Mode [Enabled] Automatic Power-On [Restore Last Power State] Power-On Delay [No Delay] 4. Press **Esc** twice to back out to the BIOS/Platform Configuration (RBSU) menu.

Procedure 72. Configure HP Gen 8 Server BIOS Settings

7. ☐	**HP Gen 9 Server**: Power Management	1. Select the **Power Management** menu. 2. Set HP Power Profile to **Maximum Performance**. BIOS/Platform Configuration (RBSU) BIOS/Platform Configuration (RBSU) Power Management ▸ Power Profile [Maximum Performance] Power Regulator [Static High Performance Mode] Minimum Processor Idle Power Core C-State [No C-states] Minimum Processor Idle Power Package C-State [No Package State] Advanced Power Options 3. Press **Esc** once to back out to the BIOS/Platform Configuration (RBSU) menu.
8. ☐	**HP Gen 9 Server**: Save settings and exit	1. Press **F10** to save the updated settings, then **y** to confirm the settings change. 2. Press **Esc** twice to back out to the **System Utilities** menu.
9. ☐	**HP Gen 9 Server**: Reboot	Select **Reboot the System** and press **Enter** to confirm.

Appendix A.2.3 Configure Oracle X5-2/Netra X5-2/X6-2/X7-2 Server

Procedure 73. Configure Oracle X5-2/Netra X5-2/X6-2/X7-2 Server BIOS Settings

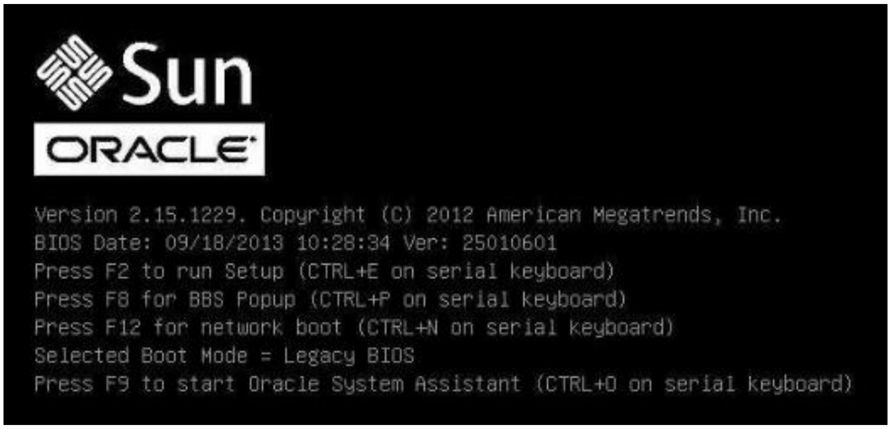
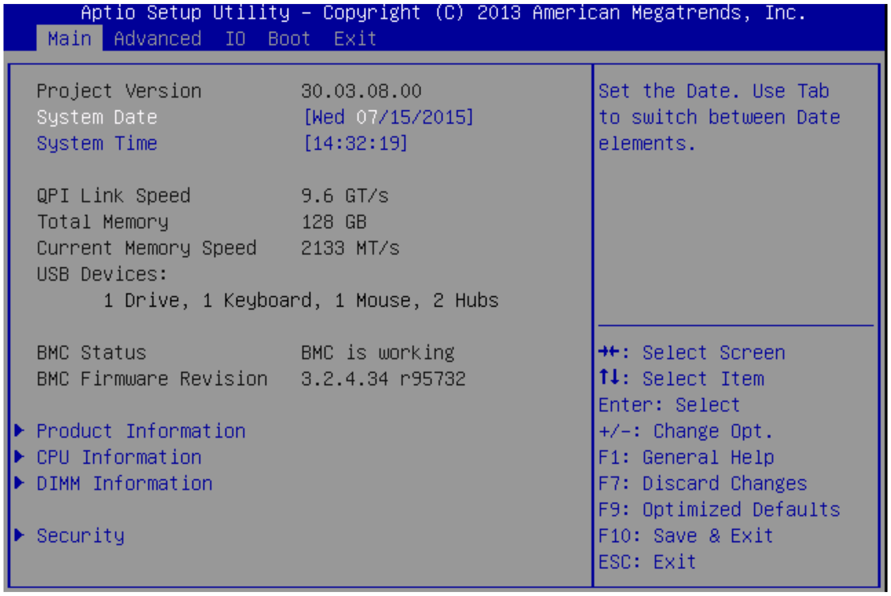
This procedure configures Oracle rack mount server BIOS settings.

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

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

1. ☐	**Oracle X5-2/Netra X5-2/X6-2/X7-2**: Access iLO GUI	Obtain access to the Oracle X5-2/Netra X5-2/X6-2/X7-2 iLOM by following Appendix D.2 Access the iLOM GUI (Oracle X5-2/Netra X5-2/X6-2/X7-2).

Procedure 73. Configure Oracle X5-2/Netra X5-2/X6-2/X7-2 Server BIOS Settings

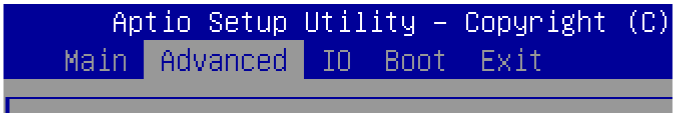
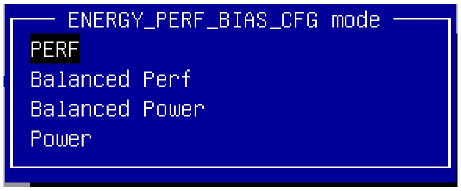
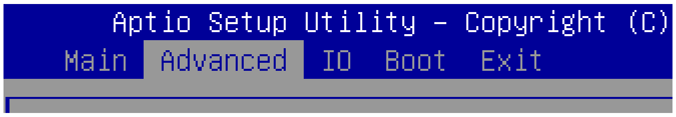
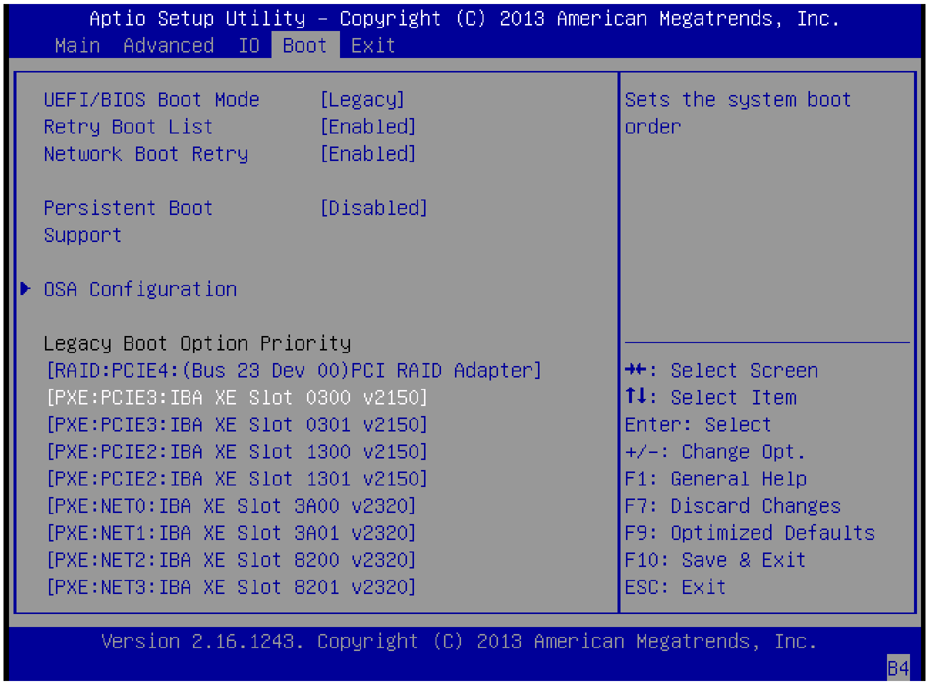
2. ☐	**Oracle X5-2/Netra X5-2/X6-2/X7-2**: Reboot	1. Reboot the server. 2. After the server is powered on, press **F2** when prompted to access the Setup Utility.  This action takes you to the Main Menu. 

```
Version 2.15.1229. Copyright (C) 2012 American Megatrends, Inc.
BIOS Date: 09/18/2013 10:28:34 Ver: 25010601
Press F2 to run Setup (CTRL+E on serial keyboard)
Press F8 for BBS Popup (CTRL+P on serial keyboard)
Press F12 for network boot (CTRL+N on serial keyboard)
Selected Boot Mode = Legacy BIOS
Press F9 to start Oracle System Assistant (CTRL+O on serial keyboard)
```

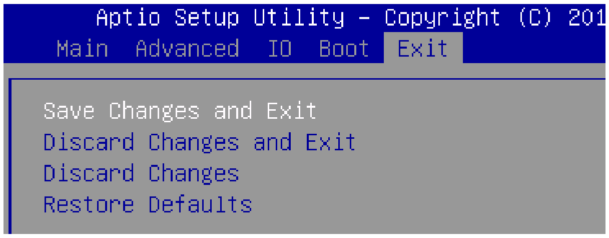
```
       Aptio Setup Utility – Copyright (C) 2013 American Megatrends, Inc.
   Main  Advanced  IO  Boot  Exit

   Project Version          30.03.08.00          Set the Date. Use Tab
   System Date              [Wed 07/15/2015]     to switch between Date
   System Time              [14:32:19]           elements.

   QPI Link Speed           9.6 GT/s
   Total Memory             128 GB
   Current Memory Speed     2133 MT/s
   USB Devices:
         1 Drive, 1 Keyboard, 1 Mouse, 2 Hubs

   BMC Status               BMC is working       →←: Select Screen
   BMC Firmware Revision    3.2.4.34 r95732      ↑↓: Select Item
                                                 Enter: Select
 ▶ Product Information                           +/-: Change Opt.
 ▶ CPU Information                               F1: General Help
 ▶ DIMM Information                              F7: Discard Changes
                                                 F9: Optimized Defaults
 ▶ Security                                      F10: Save & Exit
                                                 ESC: Exit
```

3. ☐	**Oracle X5-2/Netra X5-2/X6-2**: Set the server date and time	Set the **System Date** and **System Time**.

Procedure 73. Configure Oracle X5-2/Netra X5-2/X6-2/X7-2 Server BIOS Settings

4. ☐	**Oracle X5-2/Netra X5-2/X6-2**: Advanced menu	1. Select the **Advanced** menu.  Aptio Setup Utility – Copyright (C) Main Advanced IO Boot Exit 2. Select the **CPU Power Management Configuration** option. 3. Make sure the ENERGY_PERF_BIAS_CFG mode is set to **PERF** and press **Enter**. ENERGY_PERF_BIAS_CFG mode PERF Balanced Perf Balanced Power Power 4. Press **Esc** to return to the advanced menu.  Aptio Setup Utility – Copyright (C) Main Advanced IO Boot Exit
5. ☐	**Oracle X5-2/Netra X5-2/X6-2**: Advanced menu	1. Select the **Boot** menu. 2. 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.  Aptio Setup Utility – Copyright (C) 2013 American Megatrends, Inc. Main Advanced IO Boot Exit UEFI/BIOS Boot Mode [Legacy] Retry Boot List [Enabled] Network Boot Retry [Enabled] Persistent Boot Support [Disabled] ▶ OSA Configuration Legacy Boot Option Priority [RAID:PCIE4:(Bus 23 Dev 00)PCI RAID Adapter] [PXE:PCIE3:IBA XE Slot 0300 v2150] [PXE:PCIE3:IBA XE Slot 0301 v2150] [PXE:PCIE2:IBA XE Slot 1300 v2150] [PXE:PCIE2:IBA XE Slot 1301 v2150] [PXE:NET0:IBA XE Slot 3A00 v2320] [PXE:NET1:IBA XE Slot 3A01 v2320] [PXE:NET2:IBA XE Slot 8200 v2320] [PXE:NET3:IBA XE Slot 8201 v2320] Sets the system boot order →←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F7: Discard Changes F9: Optimized Defaults F10: Save & Exit ESC: Exit Version 2.16.1243. Copyright (C) 2013 American Megatrends, Inc. B4

Procedure 73. Configure Oracle X5-2/Netra X5-2/X6-2/X7-2 Server BIOS Settings

6. ☐	**Oracle X5-2/Netra X5-2/X6-2**: Save changes and exit	1. Select the **Exit** menu.  Aptio Setup Utility – Copyright (C) 201 Main Advanced IO Boot Exit Save Changes and Exit Discard Changes and Exit Discard Changes Restore Defaults 2. Select **Save Changes and Exit**. 3. Click **Yes** to confirm.
7. ☐	Oracle X7-2 server BIOS settings	Refer to [21] Oracle TPD Initial Product Manufacture Software Installation Procedure for BIOS configuration parameters and BIOS setup utility menu sections for details on executing the above required procedures for X7-2 BIOS settings.

Procedure 74. Enable Oracle Netra X5-2 CPU Power Limit for NEBS (Optional)

This procedure configures 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**Oracle Netra X5-2**: Enable CPU power limit after IPM	Log into the TVOE as **admusr**. `$ sudo /usr/TKLC/plat/sbin/cpuPowerLimit --enable`
2. ☐	**Oracle Netra X5-2**: Reboot server	Reboot the server. `$ sudo init 6`
3. ☐	**Oracle Netra X5-2**: Check current setting	Check the current CPU power limit setting. `$ sudo /usr/TKLC/plat/sbin/cpuPowerLimit --status`

Procedure 75. Disable Oracle Netra X5-2/X6-2/X7-2 CPU Power Limit for NEBS (Optional)

This procedure disables 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**Oracle Netra X5-2**: Disable CPU power limit after IPM	Log into the TVOE as **admusr**. `$ sudo /usr/TKLC/plat/sbin/cpuPowerLimit --disable`
2. ☐	**Oracle Netra X5-2**: Reboot server	Reboot the server. `$ sudo init 6`
3. ☐	**Oracle Netra X5-2**: Check current setting	Check the current CPU power limit setting. `$ sudo /usr/TKLC/plat/sbin/cpuPowerLimit --status`

Appendix B. Upgrade Server Firmware

Appendix B.1 HP DL380 Server

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

The Service Pack for ProLiant (SPP) installer automatically detects the firmware components available on the target server and only upgrades 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_HPSPP_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 Materials:

- HP service pack for ProLiant (SPP) firmware ISO image (minimum version 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

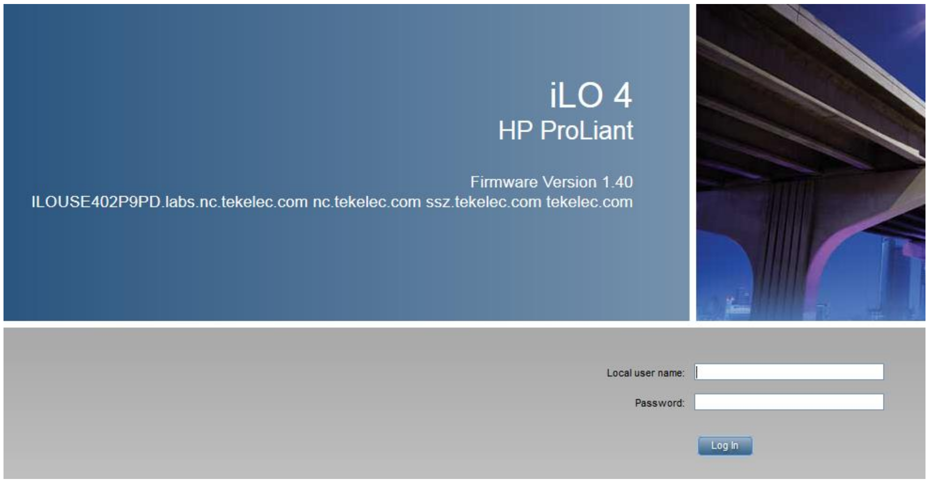
Note: For the **Update Firmware Errata** step, check the HP Solutions Firmware Upgrade Pack Release notes [1] to see if there are any firmware errata items that apply to the server being upgraded. If there is, there is a directory matching the errata's ID in the **/errata** directory of the HP MISC firmware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

Procedure 76. Upgrade HP DL380 Server Firmware

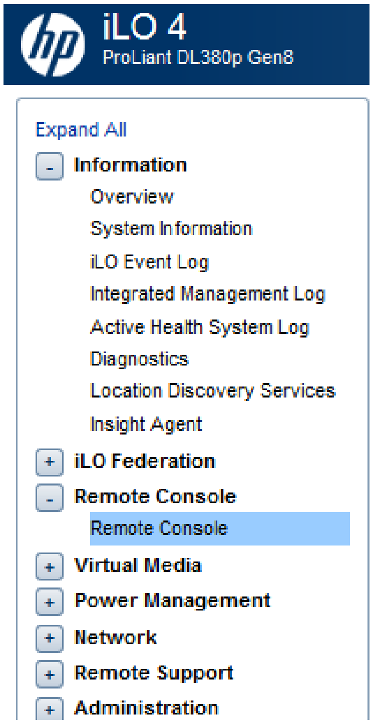
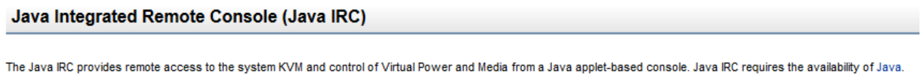
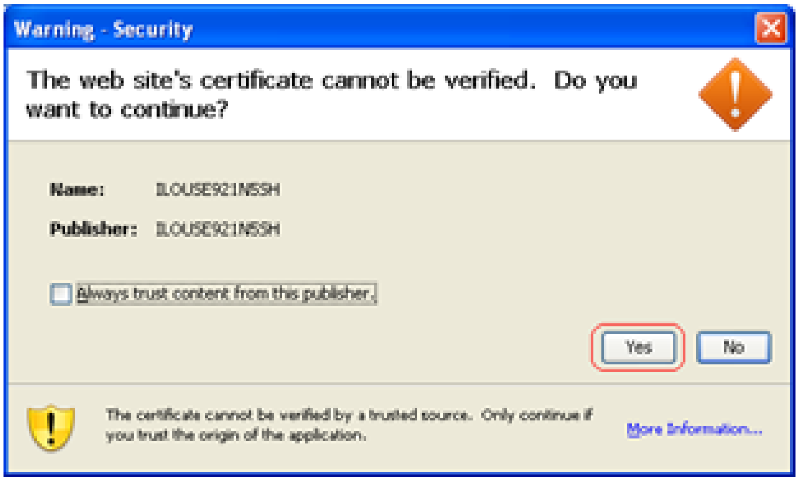
This procedure upgrades the DL380 server firmware.

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

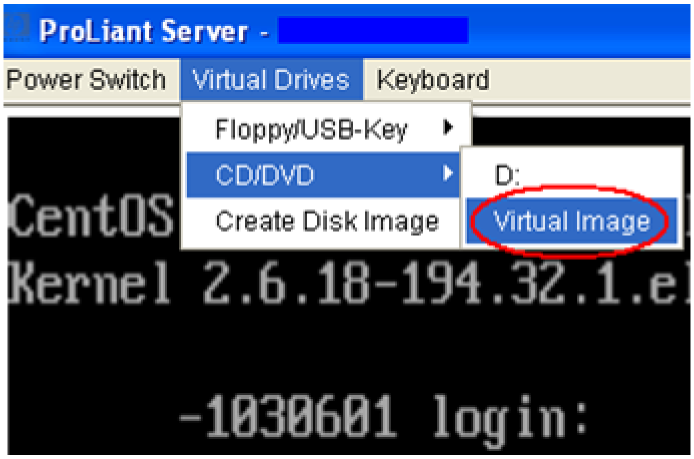
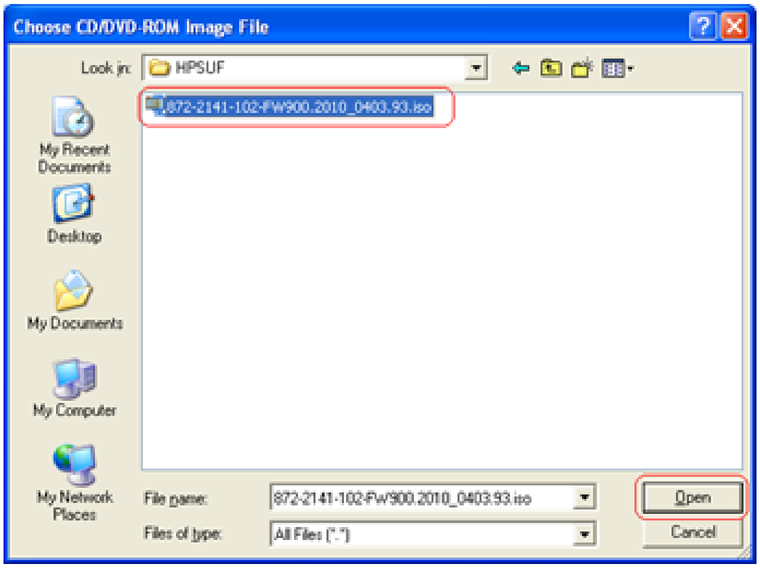
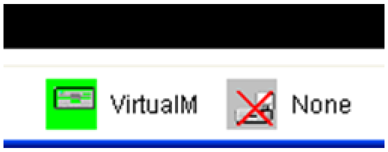
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**Local Work Station**: Log into the iLO web GUI	Access the iLO web GUI. `https://<iLO_IP>/`  iLO 4 HP ProLiant Firmware Version 1.40 ILOUSE402P9PD.labs.nc.tekelec.com nc.tekelec.com ssz.tekelec.com tekelec.com Local user name: Password: Log In **Username**: <iLO_admin_user> **Password**: <iLO_admin_password>

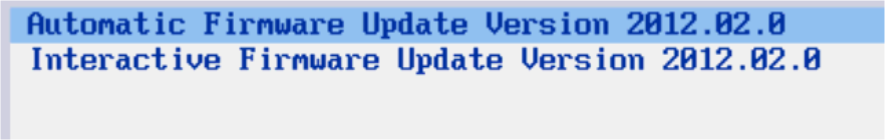
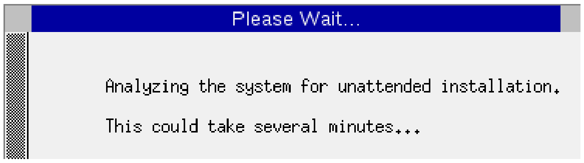
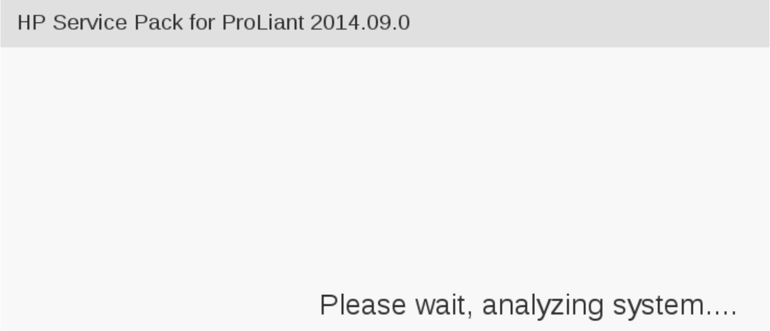
Procedure 76. Upgrade HP DL380 Server Firmware

2. ☐	**iLO4 Web GUI**: Launch remote console	1. Launch the Java Integrated Remote Console applet. 2. Navigate to the **Remote Console** page. Under Java Integrated Remote Console (Java IRC), click **Launch**.  iLO 4 ProLiant DL380p Gen8 Expand All - Information Overview System Information iLO Event Log Integrated Management Log Active Health System Log Diagnostics Location Discovery Services Insight Agent + iLO Federation - Remote Console Remote Console + Virtual Media + Power Management + Network + Remote Support + Administration  **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. 3. Click **Yes** to acknowledge the security warning, if presented.  **Warning - Security** The web site's certificate cannot be verified. Do you want to continue? **Name:** ILOUSE921N5SH **Publisher:** ILOUSE921N5SH ☐ Always trust content from this publisher. The certificate cannot be verified by a trusted source. Only continue if you trust the origin of the application. Yes No More Information...

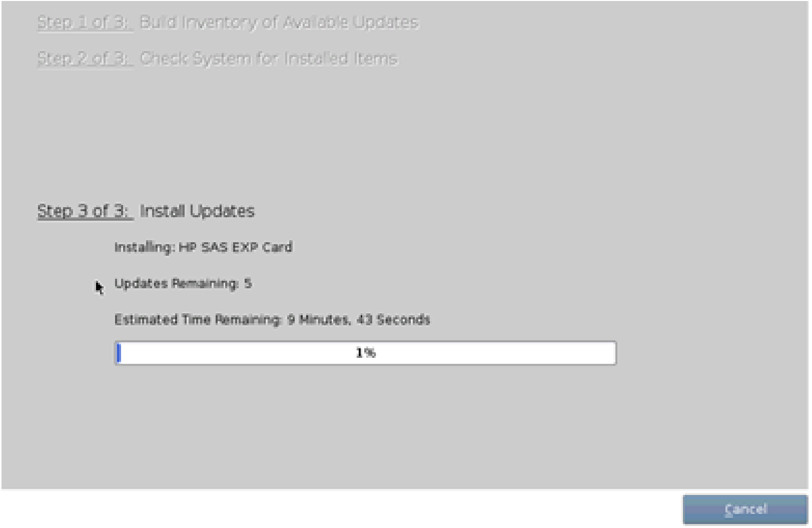
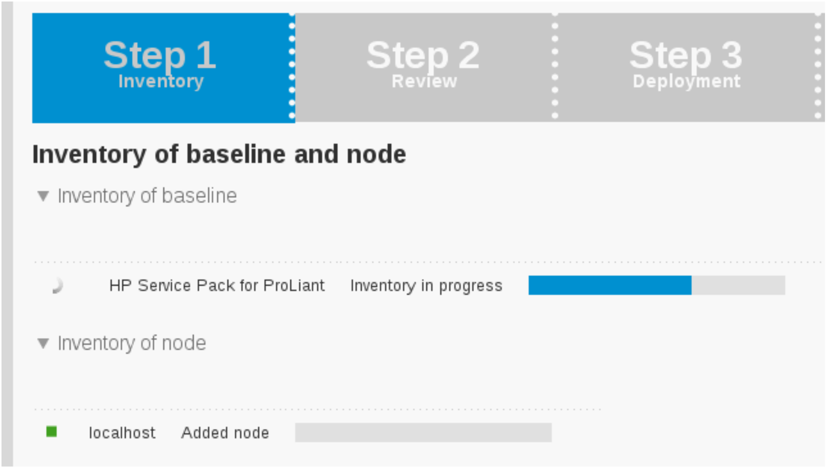
Procedure 76. Upgrade HP DL380 Server Firmware

3. ☐	**iLO4 Remote Console**: Create virtual drive connection	⚠ If using SPP USB media plugged into the server, skip this step ⚠ 1. Navigate to **Virtual Drives > CD/DVD > Virtual Image**.  ProLiant Server - [redacted] Power Switch Virtual Drives Keyboard Floppy/USB-Key CD/DVD Create Disk Image D: Virtual Image CentOS Kernel 2.6.18-194.32.1.el -1030601 login: 2. Browse to the **HP Support Pack for ProLiant ISO** file copied to the workstation and click **Open**.  Choose CD/DVD-ROM Image File Look in: HPSUF 872-2141-102-FW900.2010_0403.93.iso My Recent Documents Desktop My Documents My Computer My Network Places Open Cancel File name: 872-2141-102-FW900.2010_0403.93.iso Files of type: All Files (*.*) At the bottom of the remote console screen, the VirtualIM green highlighted drive icon displays.  VirtualM None
4. ☐	**iLO4 Remote Console**: Login	Log into the server as **admusr**.
5. ☐	**iLO4 Remote Console**: Reboot the server	`$ sudo init 6`

Procedure 76. Upgrade HP DL380 Server Firmware

6. ☐	**iLO4 Remote Console**: Perform an unattended firmware upgrade	Press **Enter** to select the **Automatic Firmware Update** procedure.  Automatic Firmware Update Version 2012.02.0 Interactive Firmware Update Version 2012.02.0 ***Note:*** If no key is pressed in 30 seconds, the system automatically performs an automatic firmware update.
7. ☐	**iLO4 Remote Console**: Monitor installation	***Important***: Do not click inside the remote console during the rest of the firmware upgrade process. The firmware install stays at the EULA acceptance screen for a short period. The time it takes to complete this process varies by server and network connection speed and takes several minutes. Depending on the hardware, these screens display.  Please Wait... Analyzing the system for unattended installation. This could take several minutes...  HP Service Pack for ProLiant 2014.09.0 Please wait, analyzing system.... ***Note:*** No progress indication displays. The installation proceeds automatically to the next step.

Procedure 76. Upgrade HP DL380 Server Firmware

8. ☐	**iLO4 Remote Console**: Monitor installation	Once analysis is complete, the installer begins to upgrade inventory and deploy the eligible firmware components. A progress indicator displays. If iLO firmware is applied, the remote console disconnects, but continues upgrading. If the remote console closes due to the iLO upgrading, wait 3-5 minutes and log back into 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, these screens display.  Step 1 of 3: Build Inventory of Available Updates Step 2 of 3: Check System for Installed Items Step 3 of 3: Install Updates Installing: HP SAS EXP Card Updates Remaining: 5 Estimated Time Remaining: 9 Minutes, 43 Seconds 1%  Inventory of baseline and node Inventory of baseline HP Service Pack for ProLiant Inventory in progress Inventory of node localhost Added node ***Note:*** If the iLO firmware is to be upgraded, it is upgraded last. At this point the iLO 2 session is terminated and you lose the remote console, virtual media, and web GUI connections to the server. This is expected and does not impact the firmware upgrade process.
9. ☐	**Local Work Station**: Clean up	Once the firmware updates have been completed, the server automatically reboots. Closing the remote console window disconnects 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.

Procedure 76. Upgrade HP DL380 Server Firmware

10. ☐	**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.
11. ☐	**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.
12. ☐	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/X7-2

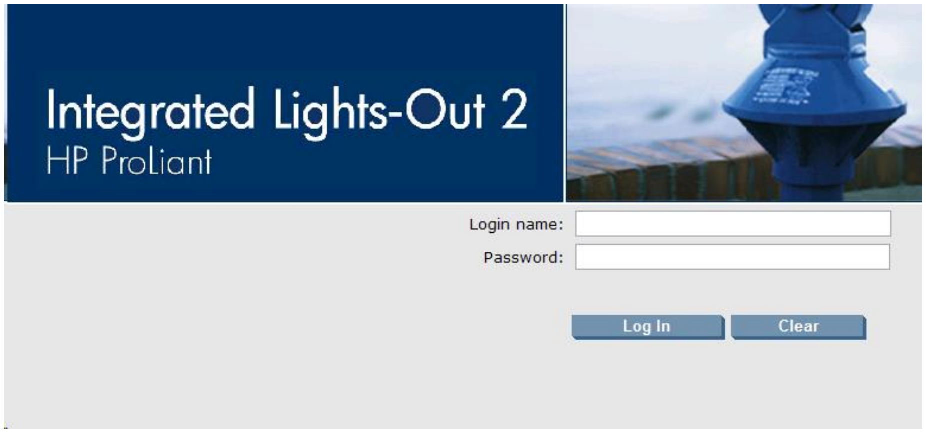
Needed Materials:

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

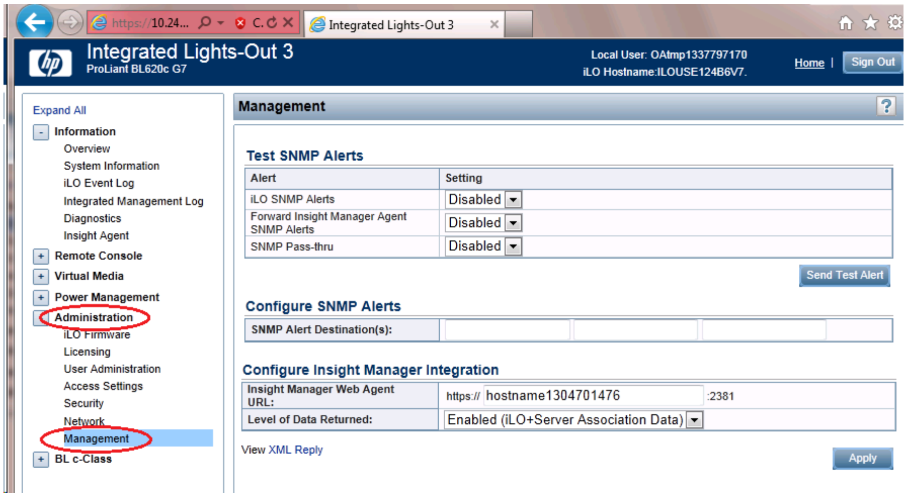
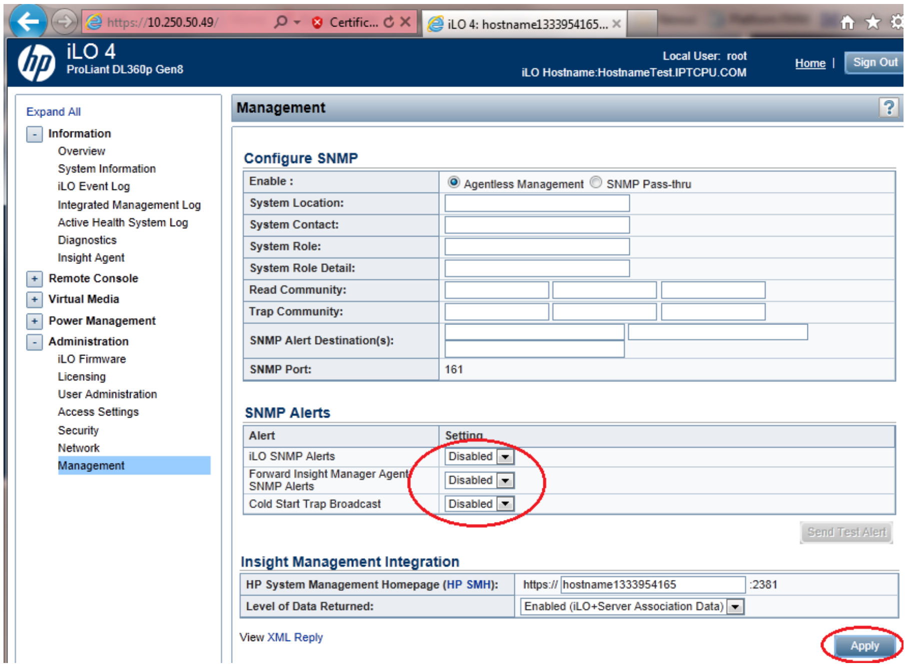
Note: The minimum supported Oracle Firmware Upgrade Pack is release 3.1.7 (X7-2: 3.1.8). However, when upgrading firmware, it is recommended that the latest release is used. Refer to the Oracle Firmware Upgrade Pack Release Notes for procedures on how to obtain the firmware, and follow the procedures in the Oracle Firmware Upgrade Pack Upgrade Guide to upgrade the firmware.

Appendix C. Change the SNMP Configuration Settings

Procedure 77. Change SNMP Configuration Settings for HP DL380

This procedure upgrades 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Local Work Station**: Log into the iLO web GUI	Access the iLO web GUI. `https://<iLO_IP>/`  Integrated Lights-Out 2 HP ProLiant Login name: Password: Log In Clear

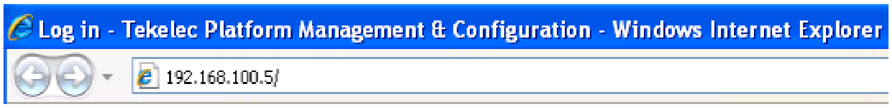
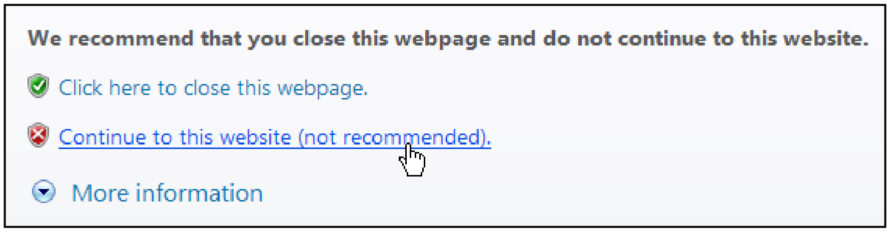
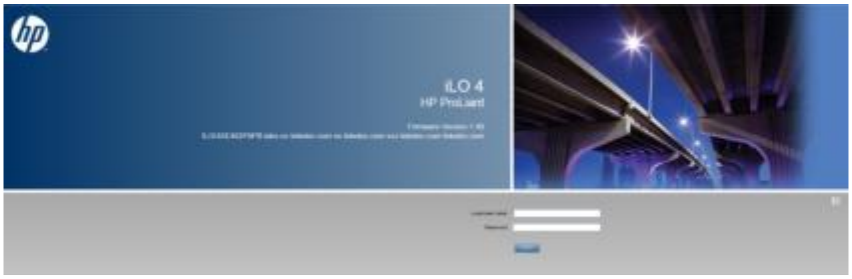
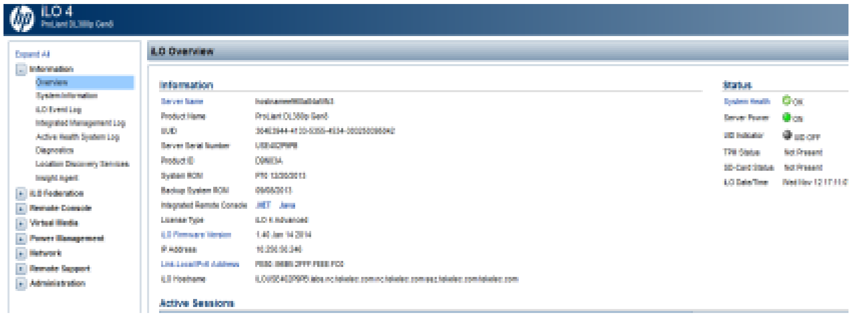
Procedure 77. Change SNMP Configuration Settings for HP DL380

2. ☐	**iLO4 GUI**: Navigate to the management screen	Navigate to **Administration > Management**.  https://10.24... Integrated Lights-Out 3 Home | Sign Out Expand All Information Overview System Information iLO Event Log Integrated Management Log Diagnostics Insight Agent Remote Console Virtual Media Power Management Administration iLO Firmware Licensing User Administration Access Settings Security Network Management BL c-Class Send Test Alert View XML Reply Apply Integrated Lights-Out 3 ProLiant BL620c G7 Local User: OAtmp1337797170 iLO Hostname:ILOUSE124B6V7. Management Test SNMP Alerts Alert: Setting iLO SNMP Alerts: Disabled Forward Insight Manager Agent SNMP Alerts: Disabled SNMP Pass-thru: Disabled Configure SNMP Alerts SNMP Alert Destination(s): Configure Insight Manager Integration Insight Manager Web Agent URL: https:// hostname1304701476 :2381 Level of Data Returned: Enabled (iLO+Server Association Data)
3. ☐	**iLO4 GUI**: Disable SNMP alerts	1. Select **Disabled** for each of the 3 SNMP alerts options.  https://10.250.50.49/ Certific... iLO 4: hostname1333954165... Home | Sign Out Expand All Information Overview System Information iLO Event Log Integrated Management Log Active Health System Log Diagnostics Insight Agent Remote Console Virtual Media Power Management Administration iLO Firmware Licensing User Administration Access Settings Security Network Management Send Test Alert View XML Reply Apply iLO 4 ProLiant DL360p Gen8 Local User: root iLO Hostname:HostnameTest.IPTCPU.COM Management Configure SNMP Enable : ● Agentless Management ○ SNMP Pass-thru System Location: System Contact: System Role: System Role Detail: Read Community: Trap Community: SNMP Alert Destination(s): SNMP Port: 161 SNMP Alerts Alert: Setting iLO SNMP Alerts: Disabled Forward Insight Manager Agent SNMP Alerts: Disabled Cold Start Trap Broadcast: Disabled Insight Management Integration HP System Management Homepage (HP SMH): https:// hostname1333954165 :2381 Level of Data Returned: Enabled (iLO+Server Association Data) 2. Click **Apply** to save the change. ***Note:*** To verify the setting changes, navigate away from the management configuration page and go back to the page to verify the SNMP settings.
4. ☐	**iLO4 GUI**: Exit	Click **Sign Out** 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 DL380 rack mount servers.

Appendix D. TVOE iLO/iLOM GUI Access

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

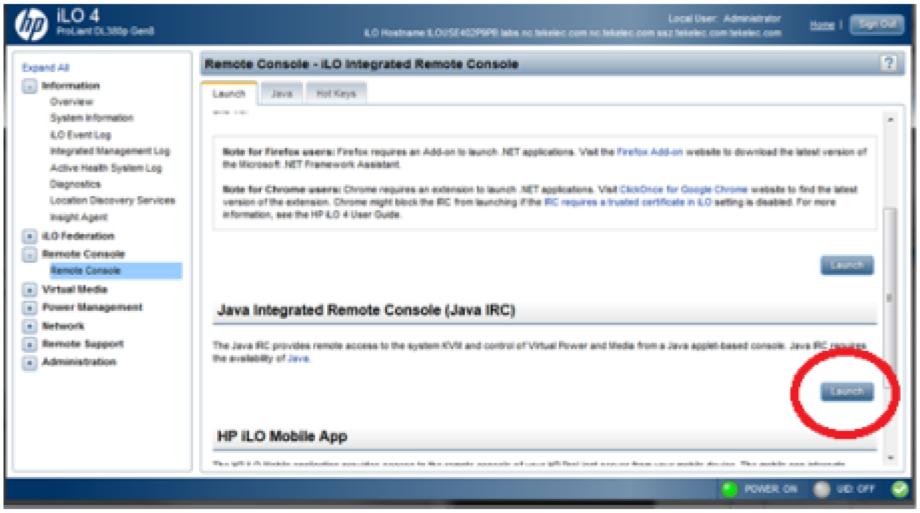
Procedure 78. Access the TVOE iLO4 GUI

This procedure accesses the TVO 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Launch Internet Explorer	1. Navigate to 192.168.100.5 (manufacturing default) or customer IP set during installation using Appendix E Change the TVOE iLO/iLOM Address.  Log in - Tekelec Platform Management & Configuration - Windows Internet Explorer 192.168.100.5/ Internet Explorer may display a warning message regarding the security certificate. 2. Click **Continue to the website (not recommended)**.  We recommend that you close this webpage and do not continue to this website. Click here to close this webpage. Continue to this website (not recommended). More information
2. ☐	Log into the iLO4	Log into the iLO4.  The iLO4 Home page displays.  iLO 4 iLO Overview Information Status Active Sessions

Procedure 78. Access the TVOE iLO4 GUI

<table>
<tr>
<td>3.
☐</td>
<td>Launch the PMAC iLO4 CLI</td>
<td>

Click **Launch** to start the PMAC iLO4 CLI.


iLO 4
ProLiant DL380p Gen8
Local User: Administrator
Home
Sign Out
Expand All
Information
Overview
System Information
iLO Event Log
Integrated Management Log
Active Health System Log
Diagnostics
Location Discovery Services
Insight Agent
iLO Federation
Remote Console
Remote Console
Virtual Media
Power Management
Network
Remote Support
Administration
Remote Console - iLO Integrated Remote Console
Launch
Java
Hot Keys
Launch
Java Integrated Remote Console (Java IRC)
Launch
HP iLO Mobile App
POWER: ON
UID: OFF

Note for Firefox users: Firefox requires an Add-on to launch .NET applications. Visit the Firefox Add-on website to download the latest version of the Microsoft .NET Framework Assistant.

Note for Chrome users: Chrome requires an extension to launch .NET applications. Visit ClickOnce for Google Chrome website to find the latest version of the extension. Chrome might block the IRC from launching if the IRC requires a trusted certificate in iLO setting is disabled. For more information, see the HP iLO 4 User Guide.

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.

</td>
</tr>
</table>

Appendix D.2 Access the iLOM GUI (Oracle X5-2/Netra X5-2/X6-2/X7-2)

Procedure 79. Access the iLOM GUI

<table>
<tr>
<td colspan="3">

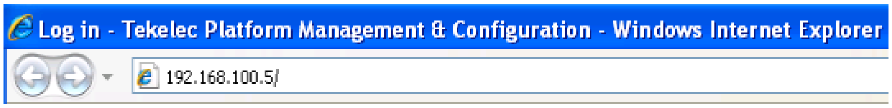
This procedure sets a static IP address on the iLOM and access the TVOE iLOM GUI.

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

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

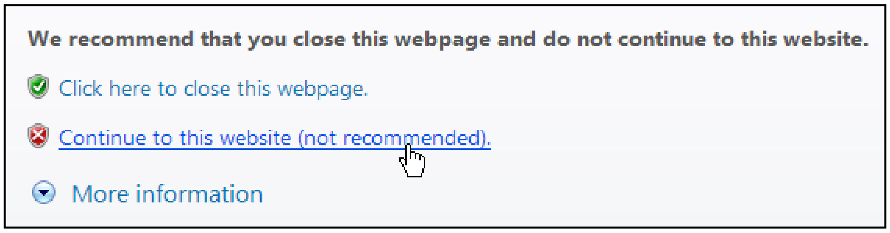
</td>
</tr>
<tr>
<td>1.
☐</td>
<td>Launch Internet Explorer</td>
<td>

1. Navigate to 192.168.100.5 (manufacturing default) or customer IP set during installation using Appendix E Change the TVOE iLO/iLOM Address.


Log in - Tekelec Platform Management & Configuration - Windows Internet Explorer
192.168.100.5/

Internet Explorer may display a warning message regarding the security certificate.

2. Click **Continue to the website (not recommended)**.



We recommend that you close this webpage and do not continue to this website.

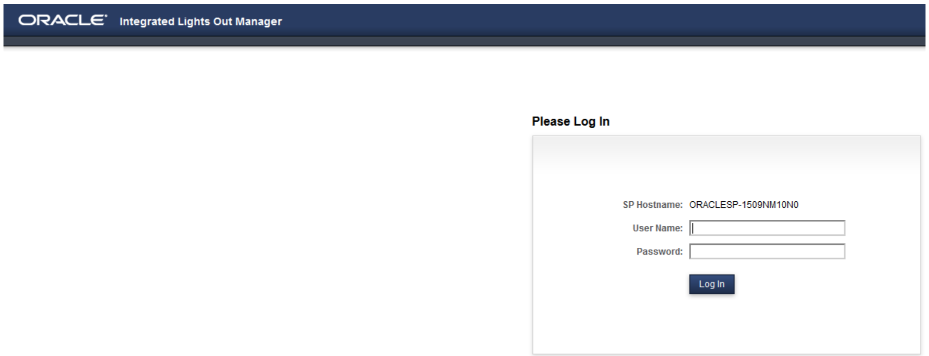
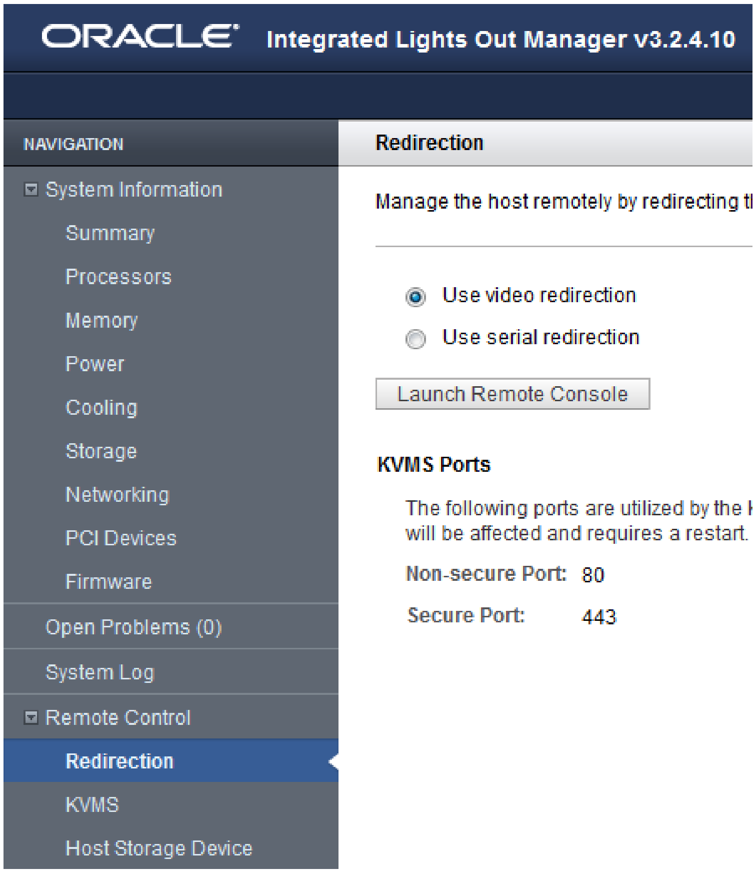
Click here to close this webpage.

Continue to this website (not recommended).

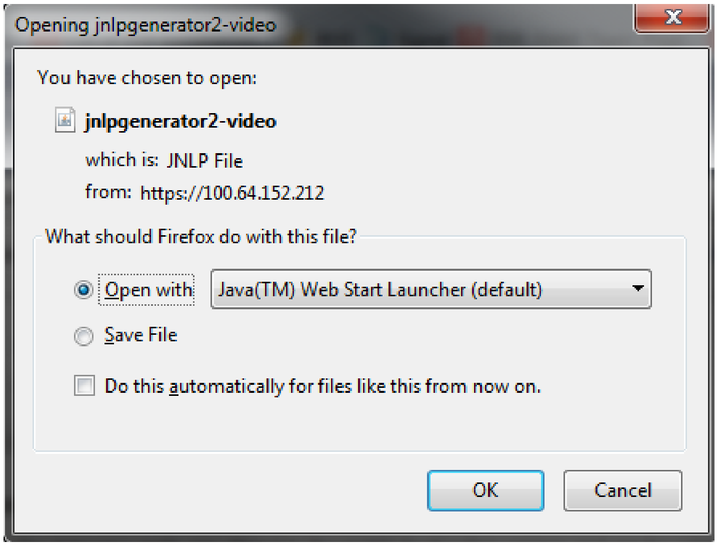
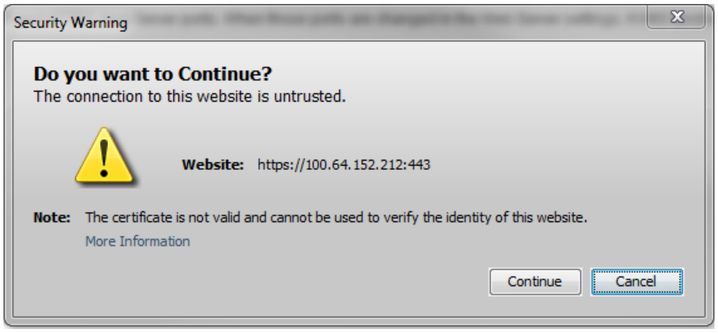
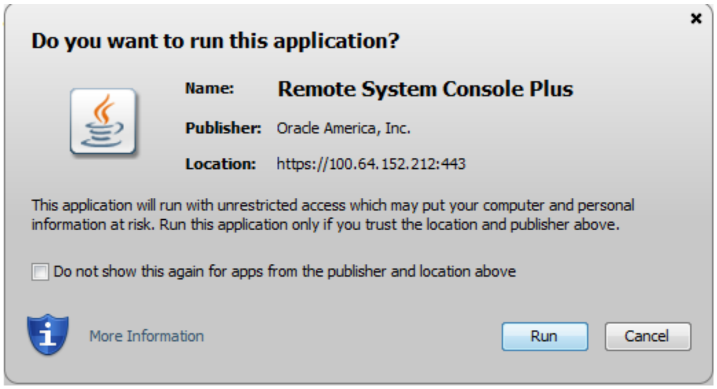
More information

</td>
</tr>
</table>

Procedure 79. Access the iLOM GUI

2. ☐	**Oracle X5-2/Netra X5-2/X6-2/X7-2**: Login	Log into the Oracle rack mount server ILOM.  ORACLE Integrated Lights Out Manager Please Log In User Name: Password: Log In SP Hostname: ORACLESP-1509NM10N0
3. ☐	**Oracle X5-2/Netra X5-2/X6-2/X7-2**: Access the remote console	1. Navigate to **Remote Control > Redirection**. 2. Click **Launch Remote Console**.  ORACLE Integrated Lights Out Manager v3.2.4.10 NAVIGATION System Information Summary Processors Memory Power Cooling Storage Networking PCI Devices Firmware Open Problems (0) System Log Remote Control Redirection KVMS Host Storage Device Redirection Launch Remote Console KVMS Ports Manage the host remotely by redirecting t ● Use video redirection ○ Use serial redirection The following ports are utilized by the will be affected and requires a restart. Non-secure Port: 80 Secure Port: 443

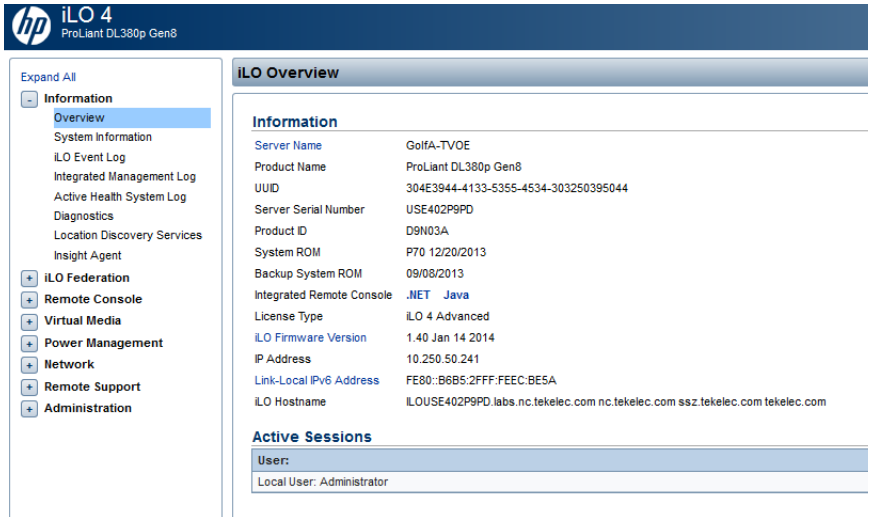
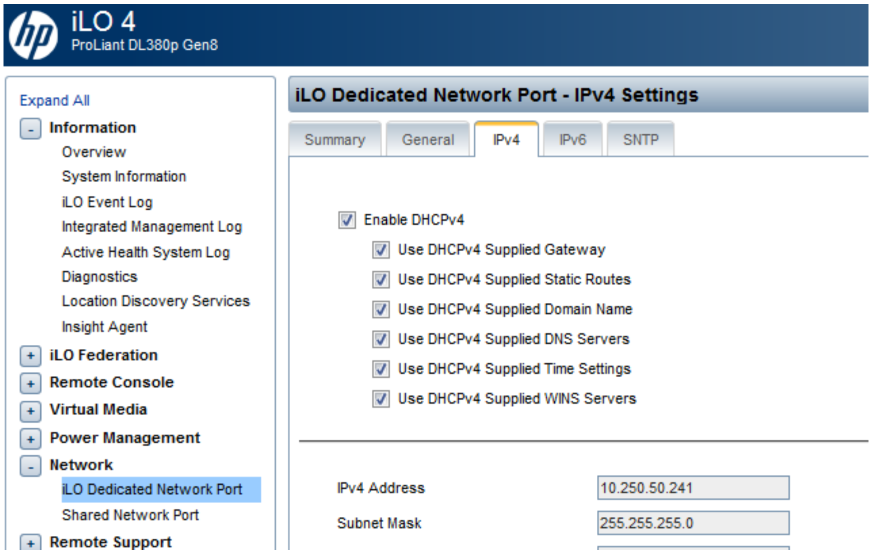
Procedure 79. Access the iLOM GUI

4. ☐	**Oracle X5-2/Netra X5-2/X6-2/X7-2**: Access the remote console	1. Click **OK** and open with **Java Web Start Launcher**.  Opening jnlpgenerator2-video You have chosen to open: **jnlpgenerator2-video** which is: JNLP File from: https://100.64.152.212 What should Firefox do with this file? ● Open with Java(TM) Web Start Launcher (default) ○ Save File ☐ Do this automatically for files like this from now on. 2. Select **Continue**.  Security Warning **Do you want to Continue?** The connection to this website is untrusted. **Website:** https://100.64.152.212:443 **Note:** The certificate is not valid and cannot be used to verify the identity of this website. More Information 3. Click **Run** for any security warning prompts.  **Do you want to run this application?** **Name:** **Remote System Console Plus** **Publisher:** Oracle America, Inc. **Location:** https://100.64.152.212:443 This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above. ☐ Do not show this again for apps from the publisher and location above More Information

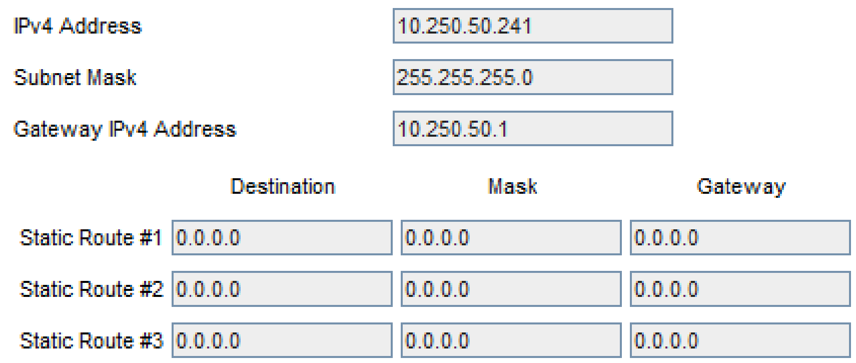
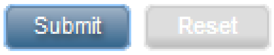
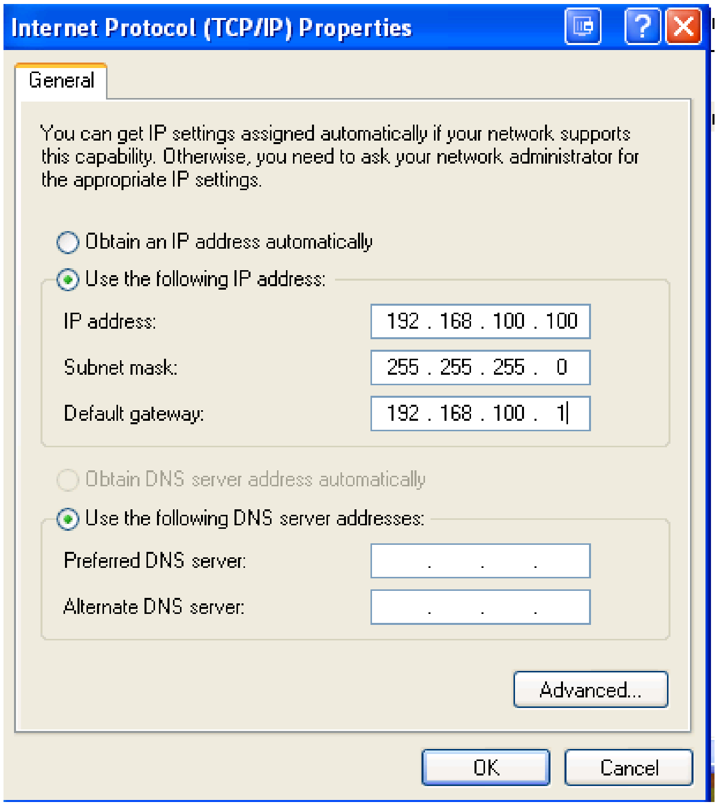
Appendix E. Change the TVOE iLO/iLOM Address

Appendix E.1 HP DL380 Servers (iLO4)

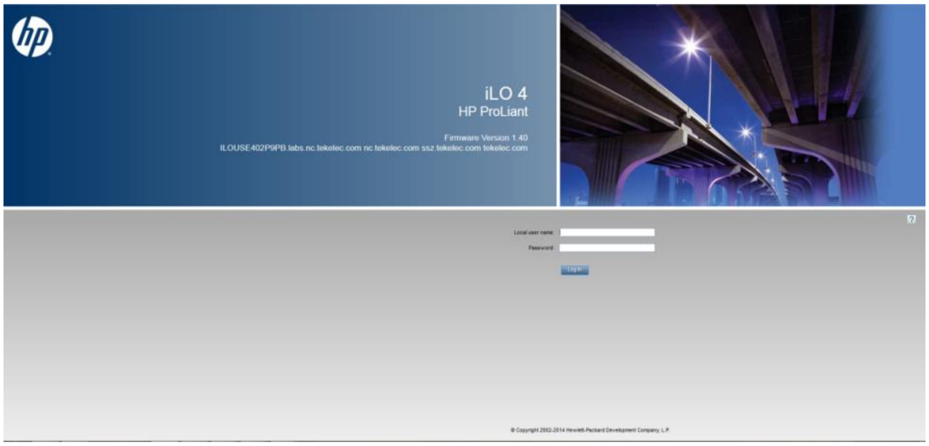
Procedure 80. Change the TVOE iLO Address

This procedure sets the IP address of the TVOE iLO4 on HP DL380 servers to the customer's network so 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**HP DL380**: Connect to the TVOE iLO GUI	Using the instructions in Appendix D TVOE iLO/iLOM GUI Access and connect to the iLO4 GUI.  iLO 4 ProLiant DL380p Gen8 Expand All Information Overview System Information iLO Event Log Integrated Management Log Active Health System Log Diagnostics Location Discovery Services Insight Agent iLO Federation Remote Console Virtual Media Power Management Network Remote Support Administration iLO Overview Information Server Name GolfA-TVOE Product Name ProLiant DL380p Gen8 UUID 304E3944-4133-5355-4534-303250395044 Server Serial Number USE402P9PD Product ID D9N03A System ROM P70 12/20/2013 Backup System ROM 09/08/2013 Integrated Remote Console .NET Java License Type iLO 4 Advanced iLO Firmware Version 1.40 Jan 14 2014 IP Address 10.250.50.241 Link-Local IPv6 Address FE80::B6B5:2FFF:FEEC:BE5A iLO Hostname ILOUSE402P9PD.labs.nc.tekelec.com nc.tekelec.com ssz.tekelec.com tekelec.com Active Sessions User: Local User: Administrator
2. ☐	**iLO4 GUI**: Navigate to network menu	1. Navigate to **Network > iLO Dedicated Network Port**.  iLO 4 ProLiant DL380p Gen8 Expand All Information Overview System Information iLO Event Log Integrated Management Log Active Health System Log Diagnostics Location Discovery Services Insight Agent iLO Federation Remote Console Virtual Media Power Management Network iLO Dedicated Network Port Shared Network Port Remote Support iLO Dedicated Network Port - IPv4 Settings Summary General IPv4 IPv6 SNTP ☑ Enable DHCPv4 ☑ Use DHCPv4 Supplied Gateway ☑ Use DHCPv4 Supplied Static Routes ☑ Use DHCPv4 Supplied Domain Name ☑ Use DHCPv4 Supplied DNS Servers ☑ Use DHCPv4 Supplied Time Settings ☑ Use DHCPv4 Supplied WINS Servers IPv4 Address 10.250.50.241 Subnet Mask 255.255.255.0 2. Select the tab for either IPv4 or IPv6.

Procedure 80. Change the TVOE iLO Address

3. ☐	**iLO4 GUI**: Change IP information	1. Change the IP address, subnet Mask/prefix, and Gateway address to the values supplied in the NAPD for the TVOE iLO.  IPv4 Address: 10.250.50.241 Subnet Mask: 255.255.255.0 Gateway IPv4 Address: 10.250.50.1 Destination / Mask / Gateway Static Route #1: 0.0.0.0 / 0.0.0.0 / 0.0.0.0 Static Route #2: 0.0.0.0 / 0.0.0.0 / 0.0.0.0 Static Route #3: 0.0.0.0 / 0.0.0.0 / 0.0.0.0 2. Click **Submit**.  ***Note:*** Access is lost at this point and is expected.
4. ☐	**Local Machine**: Reset the computer's network connection	Reset the computer'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.  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: . . .

Procedure 80. Change the TVOE iLO Address

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 from step 3.  iLO 4 HP ProLiant Firmware Version 1.40 ILOUSE402P9PB.labs.nc.tekelec.com nc.tekelec.com ssz.tekelec.com tekelec.com Local user name: Password: Log In © Copyright 2002-2014 Hewlett-Packard Development Company, L.P.

Appendix E.2 Oracle X5-2/Netra X5-2/X6-2 Servers (Change iLOM IP Address using Keyboard/Monitor)

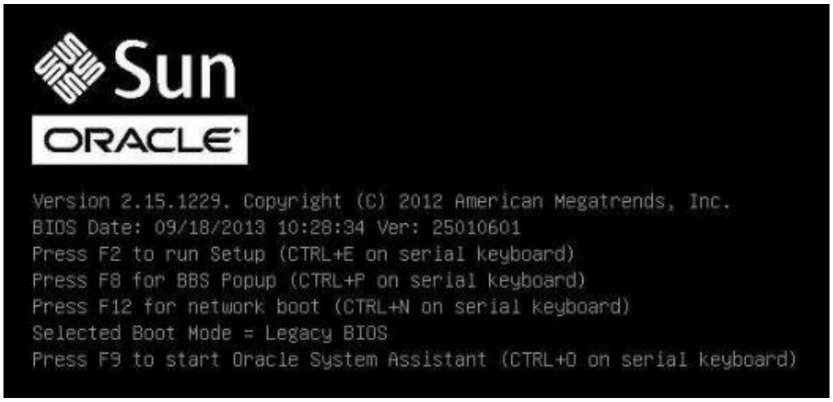
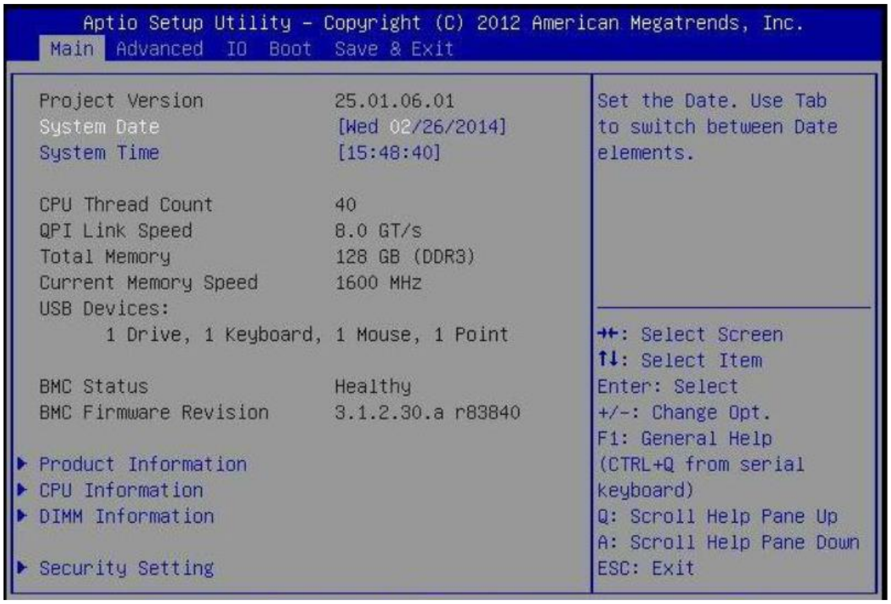
Procedure 81. Change the TVOE Oracle X5-2/Netra X5-2/X6-2iLOM Address

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

Note: By default the ILOM is configured to get its IP address dynamically through DHCP. This procedure describes 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.

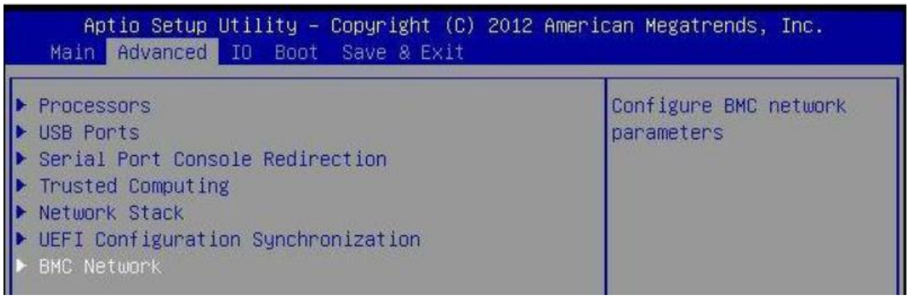
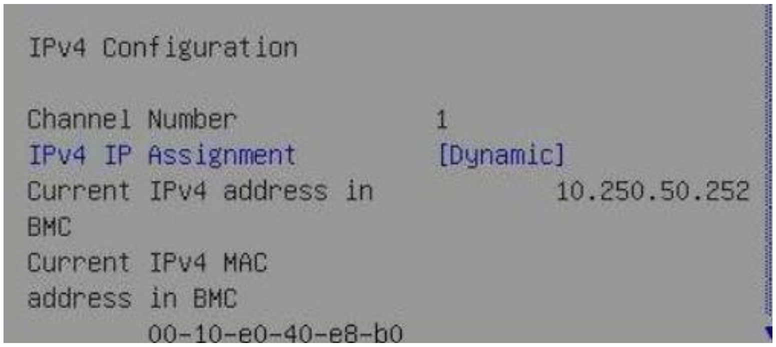
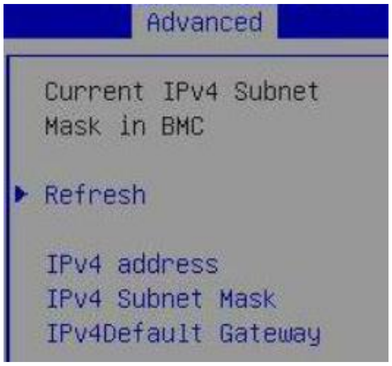
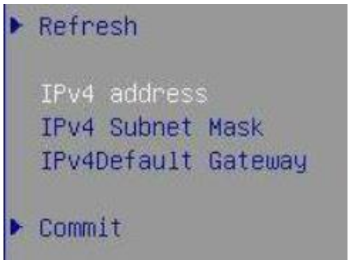
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**Oracle X5-2/Netra X5-2/X6-2**: Reboot and access BIOS configuration menu	1. Reboot the server. 2. After the server is powered on, press **F2** when prompted to enter the BIOS configuration menu.  This action takes you to the Main Menu. 

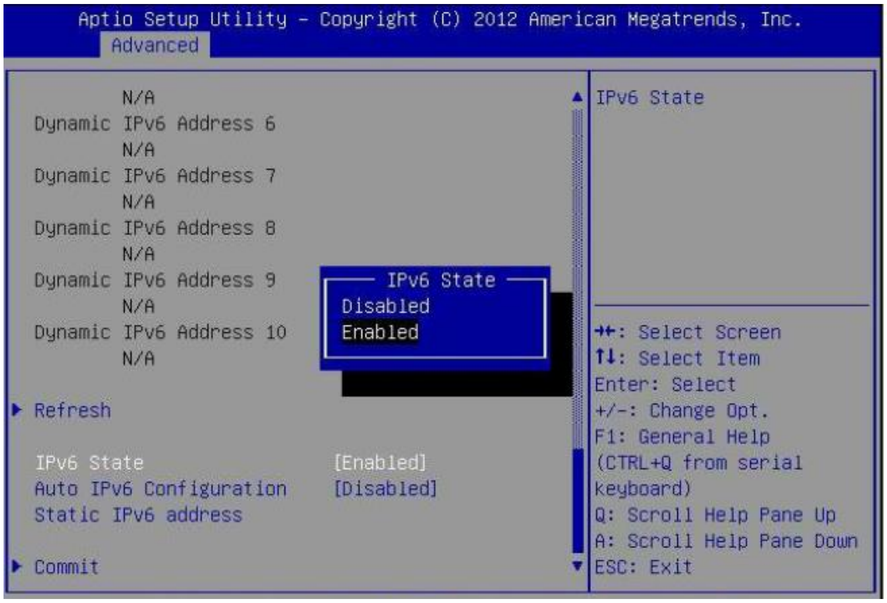
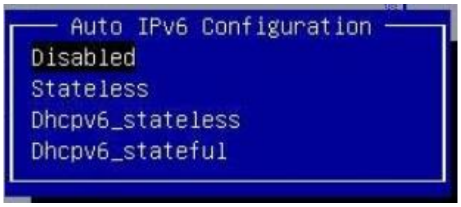
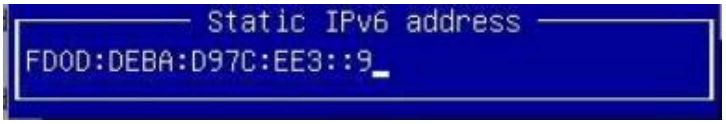
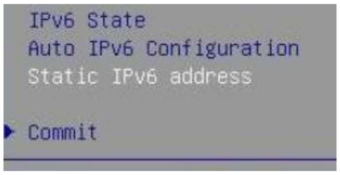
```
Version 2.15.1229. Copyright (C) 2012 American Megatrends, Inc.
BIOS Date: 09/18/2013 10:28:34 Ver: 25010601
Press F2 to run Setup (CTRL+E on serial keyboard)
Press F8 for BBS Popup (CTRL+P on serial keyboard)
Press F12 for network boot (CTRL+N on serial keyboard)
Selected Boot Mode = Legacy BIOS
Press F9 to start Oracle System Assistant (CTRL+O on serial keyboard)
```

```
      Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
   Main  Advanced  IO  Boot  Save & Exit

  Project Version             25.01.06.01           Set the Date. Use Tab
  System Date                 [Wed 02/26/2014]      to switch between Date
  System Time                 [15:48:40]            elements.

  CPU Thread Count            40
  QPI Link Speed              8.0 GT/s
  Total Memory                128 GB (DDR3)
  Current Memory Speed        1600 MHz
  USB Devices:
        1 Drive, 1 Keyboard, 1 Mouse, 1 Point       →←: Select Screen
                                                    ↑↓: Select Item
  BMC Status                  Healthy               Enter: Select
  BMC Firmware Revision       3.1.2.30.a r83840     +/-: Change Opt.
                                                    F1: General Help
▶ Product Information                               (CTRL+Q from serial
▶ CPU Information                                   keyboard)
▶ DIMM Information                                  Q: Scroll Help Pane Up
                                                    A: Scroll Help Pane Down
▶ Security Setting                                  ESC: Exit
```

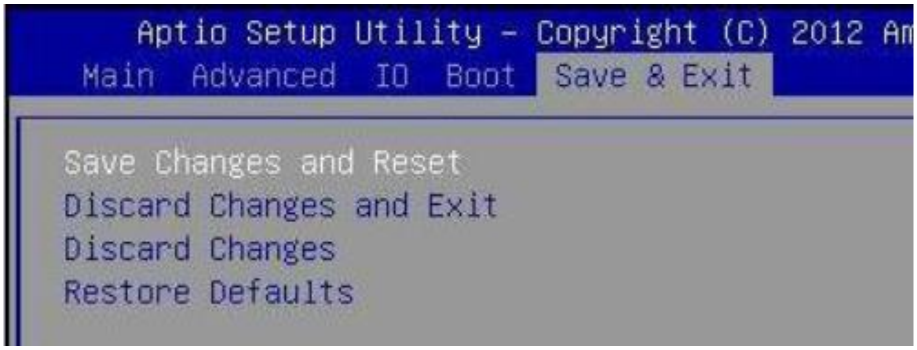
Procedure 81. Change the TVOE Oracle X5-2/Netra X5-2/X6-2iLOM Address

2. ☐	**Oracle X5-2/Netra X5-2/X6-2**: Access the Configuration Menu	1. Select the **Advanced** menu. 2. Select the **BMC Network** option.  Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc. Main Advanced IO Boot Save & Exit Processors USB Ports Serial Port Console Redirection Trusted Computing Network Stack UEFI Configuration Synchronization BMC Network Configure BMC network parameters
3. ☐	**Oracle X5-2/Netra X5-2/X6-2:** Configure the static IPv4 addresses IPv6 skip this step	1. Highlight IPv4 IP Assignment and press **Enter**.  IPv4 Configuration Channel Number 1 IPv4 IP Assignment [Dynamic] Current IPv4 address in BMC 10.250.50.252 Current IPv4 MAC address in BMC 00-10-e0-40-e8-b0 2. Highlight **Static** and press **Enter**. 3. Highlight **IPv4 address** and press **Enter**.  Advanced Current IPv4 Subnet Mask in BMC Refresh IPv4 address IPv4 Subnet Mask IPv4Default Gateway 4. Enter the desired IPv4 address and press **Enter**. 5. Repeat for the **IPv4 Subnet Mask** and **IPv4 Default Gateway**. 6. Select **Commit** BELOW the IPv4 fields.  Refresh IPv4 address IPv4 Subnet Mask IPv4Default Gateway Commit

Procedure 81. Change the TVOE Oracle X5-2/Netra X5-2/X6-2iLOM Address

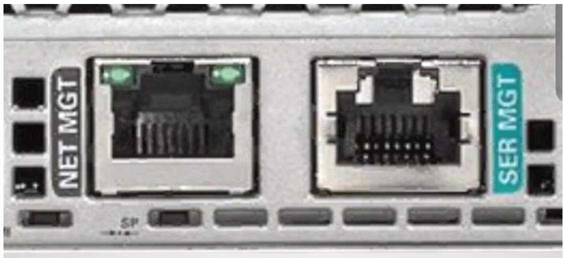
4. ☐	**Oracle X5-2/Netra X5-2/X6-2**: Configure static IPv6 addresses	1. Page down to the IPv6 configuration settings, set **IPv6 State** to **Enabled** and press **Enter**. Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc. Advanced N/A Dynamic IPv6 Address 6 N/A Dynamic IPv6 Address 7 N/A Dynamic IPv6 Address 8 N/A Dynamic IPv6 Address 9 N/A Dynamic IPv6 Address 10 N/A ▸ Refresh IPv6 State [Enabled] Auto IPv6 Configuration [Disabled] Static IPv6 address ▸ Commit IPv6 State Disabled Enabled IPv6 State →←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help (CTRL+Q from serial keyboard) Q: Scroll Help Pane Up A: Scroll Help Pane Down ESC: Exit 2. Navigate to Auto IPv6 Configuration, set **Auto IPv6 Configuration** to **Disabled** and press **Enter**. Auto IPv6 Configuration Disabled Stateless Dhcpv6_stateless Dhcpv6_stateful 3. Highlight **Static IPv6 address** and press **Enter**. 4. Enter the IPv6 address and press **Enter**. Static IPv6 address FD0D:DEBA:D97C:EE3::9_ 5. Select **Commit** BELOW the IPv6 fields. IPv6 State Auto IPv6 Configuration Static IPv6 address ▸ Commit

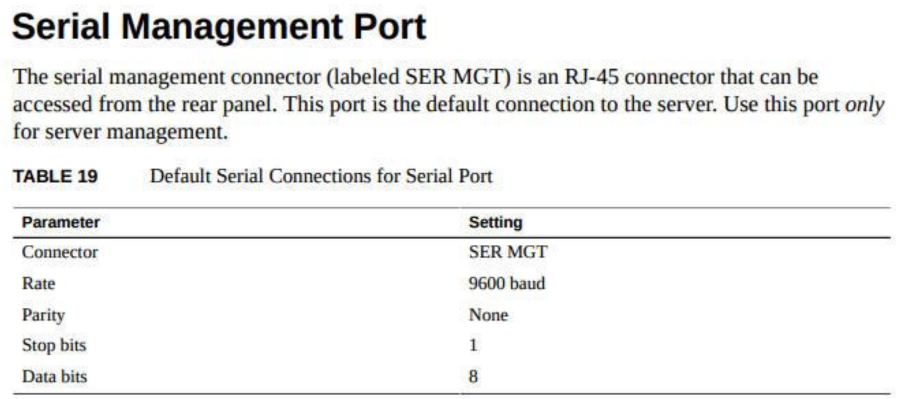
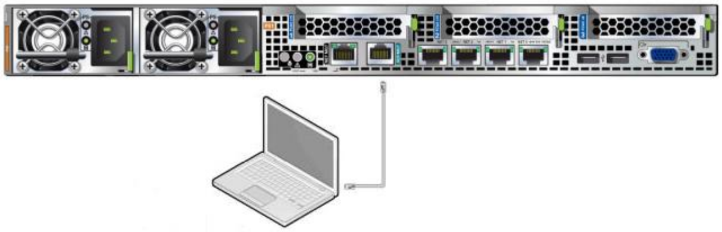
Procedure 81. Change the TVOE Oracle X5-2/Netra X5-2/X6-2iLOM Address

5. ☐	**Oracle X5-2/Netra X5-2/X6-2**: Save and exit	1. Press **Esc** to exit the **BMC Network** menu. 2. Select the **Save & Exit** menu.  Aptio Setup Utility – Copyright (C) 2012 Am Main Advanced IO Boot Save & Exit Save Changes and Reset Discard Changes and Exit Discard Changes Restore Defaults 3. Select **Save Changes and Reset**. 4. Click **Yes** to confirm **Save configuration and reset?** The server reboots.

Appendix E.3 Oracle X5-2/Netra X5-2/X6-2/X7-2 Servers (Change iLOM IP Address using Serial Console)

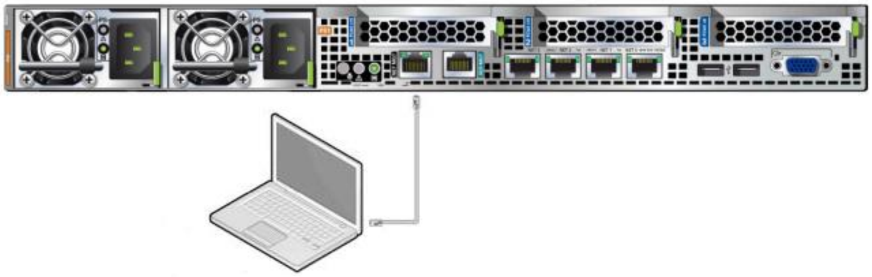
Procedure 82. Change the TVOE Oracle X5-2/Netra X5-2/X6-2iLOM Address

<table>
<tr><td colspan="3">This procedure sets the IP address of the TVOE iLOM on Oracle X5-2/Netra X5-2/X6-2/X7-2 servers to the customer’s network so it can be accessed by Oracle support.
<i>Note:</i> By default the ILOM is configured to get its IP address dynamically through DHCP. This procedure describes 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>Oracle X5-2/Netra X5-2/X6-2/X7-2 Server</td><td>1. Connect to the serial management port.



<h3>Serial Management Port</h3>
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>
2. Connect a laptop to the serial management (SER MGT) port on the server.
</td></tr>
<tr><td>2.
☐</td><td>Log into the serial console</td><td>1. Press Enter on the terminal.
2. Type your Oracle ILOM user name (default user: root) and press Enter.
3. Type the password associated with your user name and press Enter.
Oracle ILOM displays the default command prompt (->), indicating that you have successfully logged in.</td></tr>
</table>

Procedure 82. Change the TVOE Oracle X5-2/Netra X5-2/X6-2iLOM Address

3.
☐
	Configure NET_MGT network interface	1. Navigate to the /SP/network target.
		`> cd /SP/network`
		2. Ensure 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: 

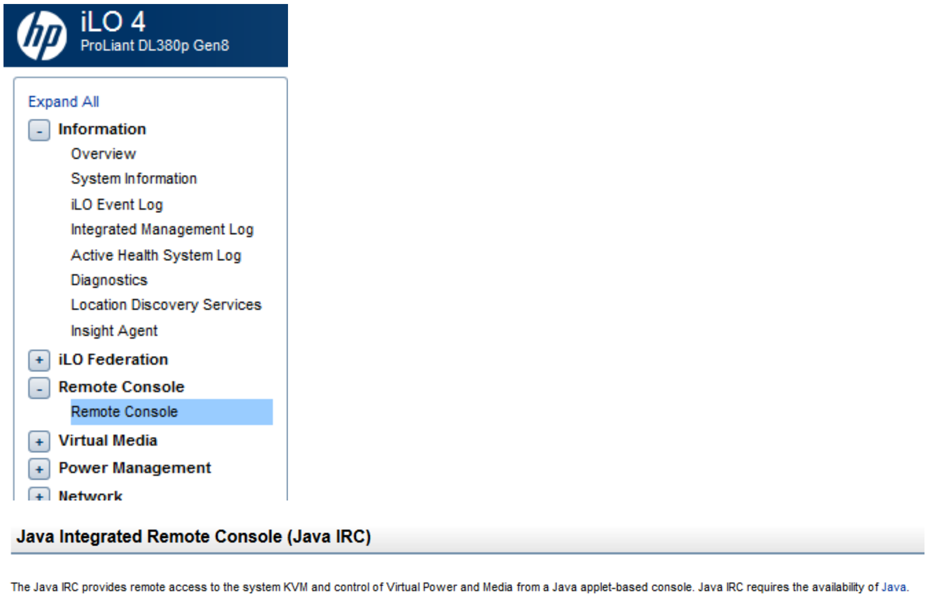
Appendix F. Attach an ISO Image to a Server using the iLO or iLOM

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

Appendix F.1 HP DL380 Servers (iLO4)

Procedure 83. Mount HP DL380 Servers with ISO Image using iLO4

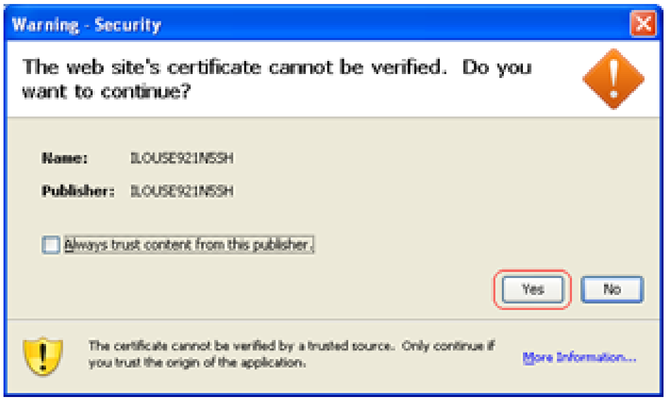
<table>
<tr><td colspan="3">This procedure attaches an ISO image to HP DL380 servers using the iLO4.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>iLO4 Web GUI: Launch remote console</td><td>1. Launch the Java Integrated Remote Console applet.
2. Navigate to the Remote Console page. Under Java Integrated Remote Console (Java IRC), click Launch.


iLO 4
ProLiant DL380p Gen8
Expand All
Information
Overview
System Information
iLO Event Log
Integrated Management Log
Active Health System Log
Diagnostics
Location Discovery Services
Insight Agent
iLO Federation
Remote Console
Remote Console
Virtual Media
Power Management
Network

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.

3. Click Yes to acknowledge the security warning, if presented.


Warning - Security
Yes
No
More Information...

The web site's certificate cannot be verified. Do you want to continue?

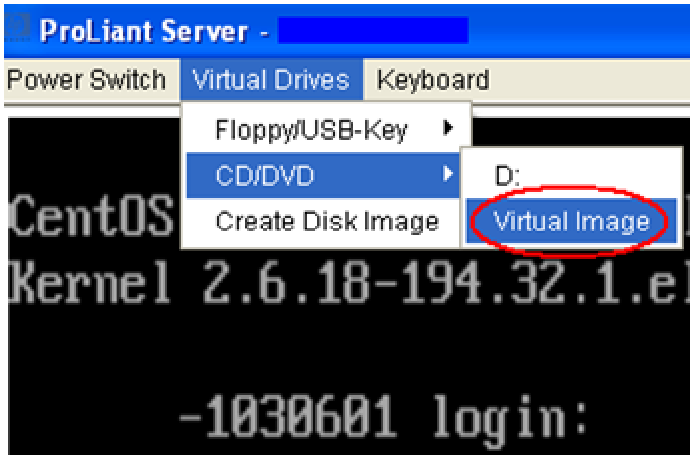
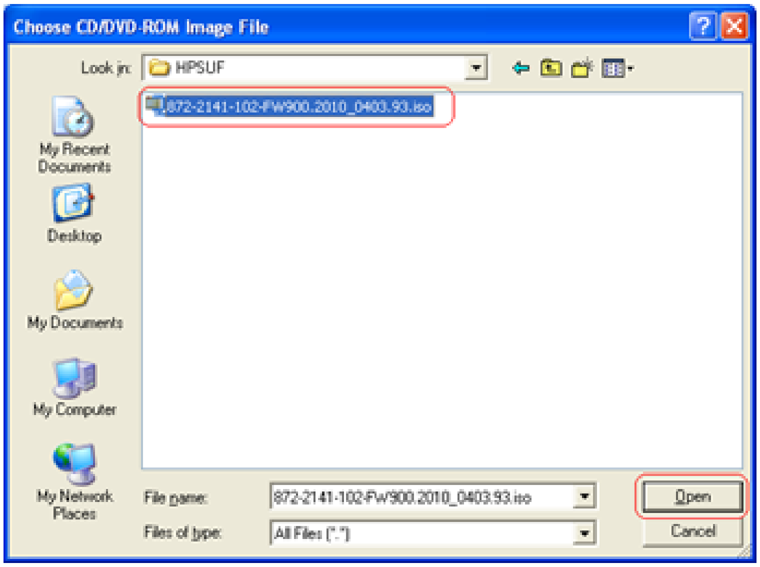
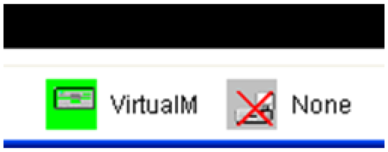
Name: ILOUSE921N5SH

Publisher: ILOUSE921N5SH

☐ Always trust content from this publisher.

The certificate cannot be verified by a trusted source. Only continue if you trust the origin of the application.</td></tr>
</table>

Procedure 83. Mount HP DL380 Servers with ISO Image using iLO4

2. ☐	**iLO4 Remote Console**: Create virtual drive connection	1. Navigate to **Virtual Drives > CD/DVD > Virtual Image**.  ProLiant Server - [redacted] Power Switch Virtual Drives Keyboard Floppy/USB-Key CD/DVD Create Disk Image D: Virtual Image CentOS Kernel 2.6.18-194.32.1.e -1030601 login: 2. Browse to the **HP Support Pack for ProLiant ISO** file copied to the workstation and click **Open**.  Choose CD/DVD-ROM Image File Look in: HPSUF 872-2141-102-FW900.2010_0403.93.iso My Recent Documents Desktop My Documents My Computer My Network Places Open Cancel File name: 872-2141-102-FW900.2010_0403.93.iso Files of type: All Files (*.*) At the bottom of the remote console screen, the VirtualIM green highlighted drive icon displays.  VirtualM None

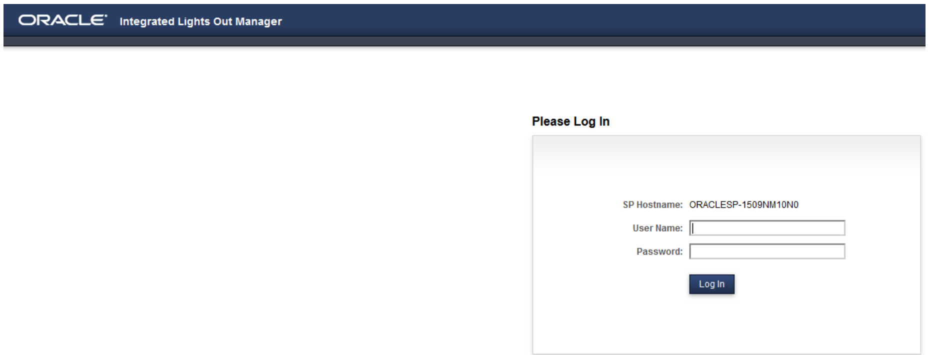
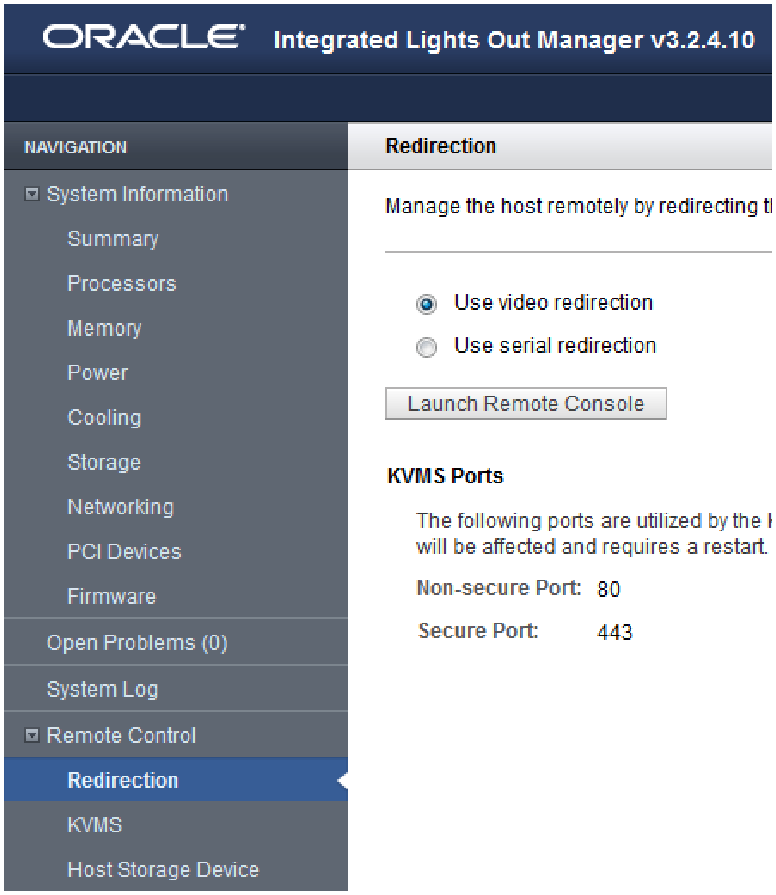
Appendix F.2 Oracle X5-2/Netra X5-2/X6-2/X7-2 Servers (iLOM)

Procedure 84. Mount Oracle X5-2/Netra X5-2/X6-2/X7-2 Servers with ISO Image using iLOM

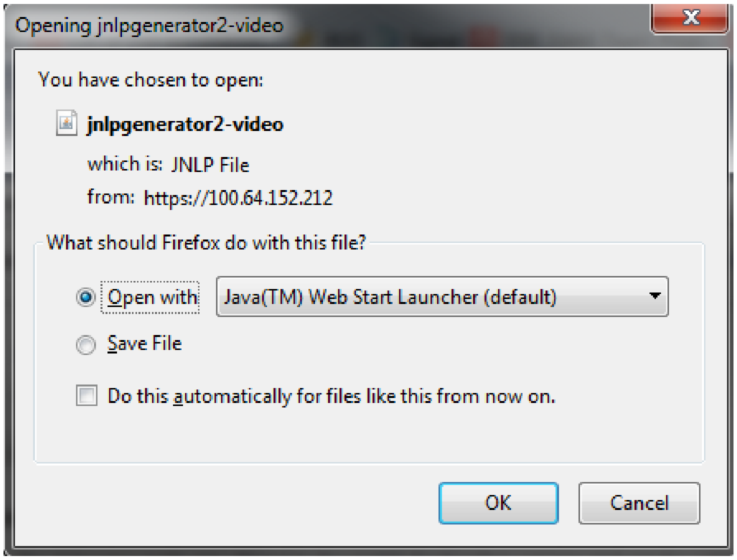
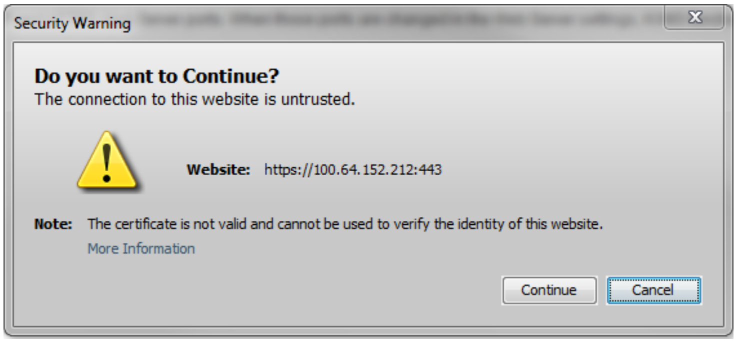
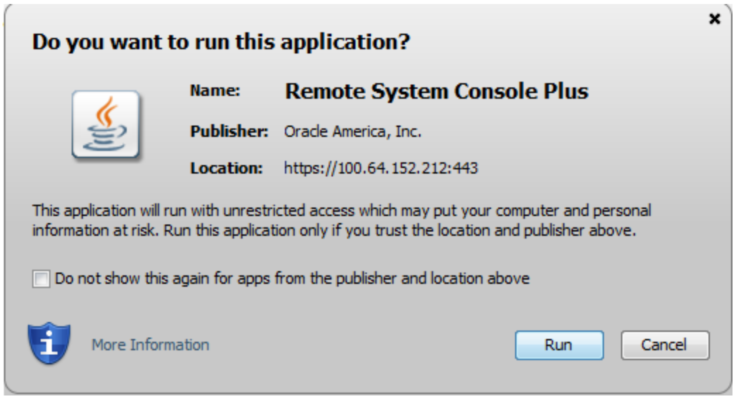
This procedure attaches an ISO image to Oracle rack mount servers using the iLOM.

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

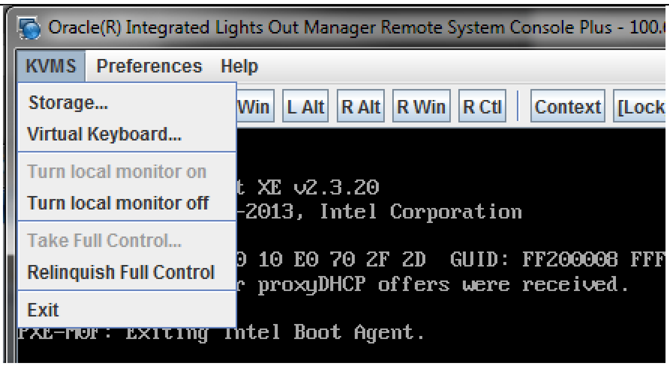
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**Oracle X5-2/Netra X5-2/X6-2**: Login	Log into the Oracle rack mount server ILOM.  ORACLE Integrated Lights Out Manager Please Log In User Name: Password: Log In SP Hostname: ORACLESP-1509NM10N0
2. ☐	**Oracle X5-2/Netra X5-2/X6-2**: Access the remote console	1. Navigate to **Remote Control > Redirection**. 2. Click **Launch Remote Console**.  ORACLE Integrated Lights Out Manager v3.2.4.10 NAVIGATION System Information Summary Processors Memory Power Cooling Storage Networking PCI Devices Firmware Open Problems (0) System Log Remote Control Redirection KVMS Host Storage Device Redirection Launch Remote Console KVMS Ports Manage the host remotely by redirecting tl ● Use video redirection ○ Use serial redirection The following ports are utilized by the I will be affected and requires a restart. Non-secure Port: 80 Secure Port: 443

Procedure 84. Mount Oracle X5-2/Netra X5-2/X6-2/X7-2 Servers with ISO Image using iLOM

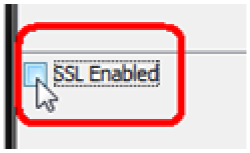
3. ☐	**Oracle X5-2/Netra X5-2/X6-2/X7-2**: Access the remote console	1. Click **OK** and open with **Java Web Start Launcher**. Opening jnlpgenerator2-video You have chosen to open: **jnlpgenerator2-video** which is: JNLP File from: https://100.64.152.212 What should Firefox do with this file? ● Open with Java(TM) Web Start Launcher (default) ○ Save File ☐ Do this automatically for files like this from now on. OK Cancel 2. Click **Continue**. Security Warning **Do you want to Continue?** The connection to this website is untrusted. **Website:** https://100.64.152.212:443 **Note:** The certificate is not valid and cannot be used to verify the identity of this website. More Information Continue Cancel 3. Click **Run** for any security warning prompts. **Do you want to run this application?** **Name:** **Remote System Console Plus** **Publisher:** Oracle America, Inc. **Location:** https://100.64.152.212:443 This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above. ☐ Do not show this again for apps from the publisher and location above More Information Run Cancel
4. ☐	**Oracle X5-2/Netra X5-2/X6-2/X7-2**: Mount the ISO from the remote console	1. Navigate to **KVMS > Storage**.

Procedure 84. Mount Oracle X5-2/Netra X5-2/X6-2/X7-2 Servers with ISO Image using iLOM

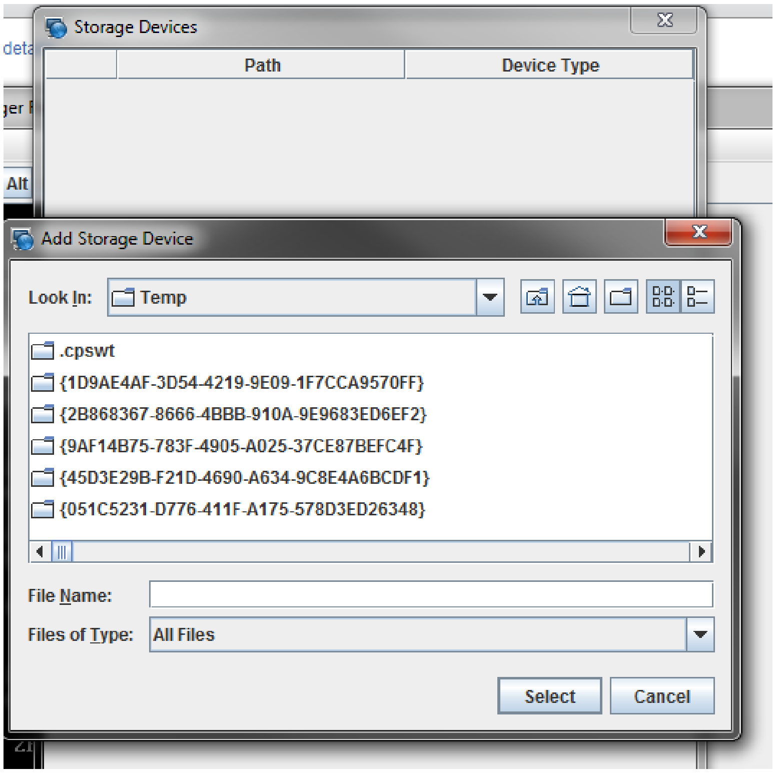

Oracle(R) Integrated Lights Out Manager Remote System Console Plus - 100.
KVMS
Preferences
Help
Storage...
Virtual Keyboard...
Turn local monitor on
Turn local monitor off
Take Full Control...
Relinquish Full Control
Exit
Win
L Alt
R Alt
R Win
R Ctl
Context
[Lock

```
t XE v2.3.20
-2013, Intel Corporation

0 10 E0 70 2F 2D  GUID: FF200008 FFF
r proxyDHCP offers were received.
PXE-M0F: Exiting Intel Boot Agent.
```

Note: If using a Windows 7 computer to configure the storage, ensure the **SSL Enabled** checkbox is NOT marked:

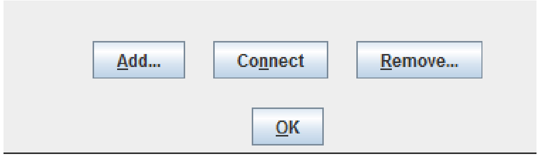

SSL Enabled

2. Click **Add** and browse to the ISO located on the local computer.

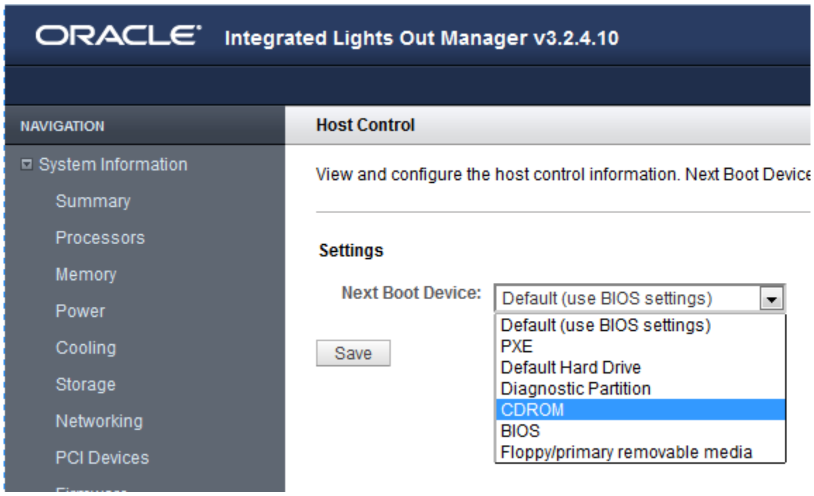
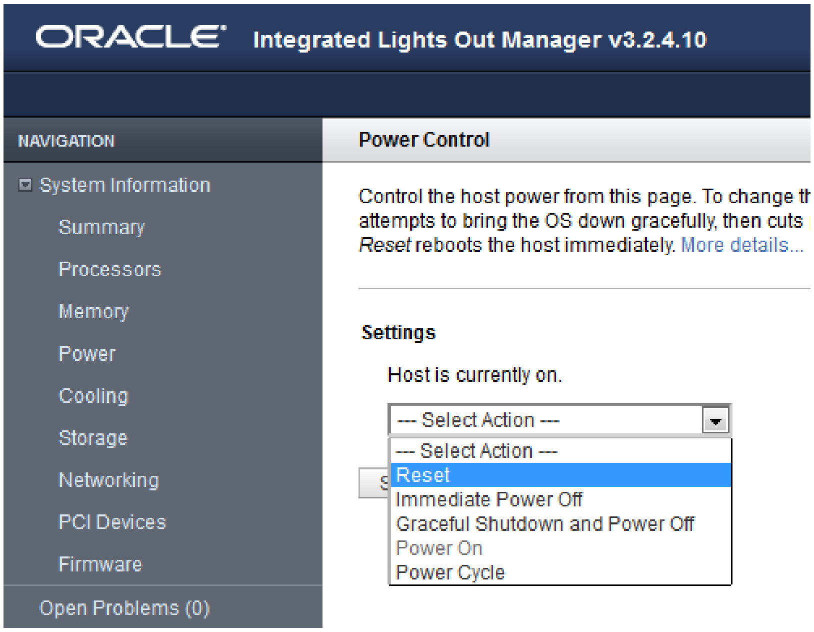

Storage Devices
Path
Device Type
Add Storage Device
Look In:
Temp
.cpswt
{1D9AE4AF-3D54-4219-9E09-1F7CCA9570FF}
{2B868367-8666-4BBB-910A-9E9683ED6EF2}
{9AF14B75-783F-4905-A025-37CE87BEFC4F}
{45D3E29B-F21D-4690-A634-9C8E4A6BCDF1}
{051C5231-D776-411F-A175-578D3ED26348}
File Name:
Files of Type:
All Files
Select
Cancel

3. Click **Select**.

4. Once the ISO image is selected, click **Connect**.


Add...
Connect
Remove...
OK

Procedure 84. Mount Oracle X5-2/Netra X5-2/X6-2/X7-2 Servers with ISO Image using iLOM

5. ☐	**Oracle X5-2/Netra X5-2/X6-2/X7-2**: Change the device for next boot	1. Navigate to **Host Management > Host Control**. 2. Select the **CDROM** option.  ORACLE Integrated Lights Out Manager v3.2.4.10 NAVIGATION System Information Summary Processors Memory Power Cooling Storage Networking PCI Devices Host Control Settings Save Default (use BIOS settings) PXE Default Hard Drive Diagnostic Partition CDROM BIOS Floppy/primary removable media View and configure the host control information. Next Boot Device Next Boot Device: Default (use BIOS settings) 3. Click **Save**.
6. ☐	**Oracle X5-2/Netra X5-2/X6-2/X7-2**: Reboot the rack mount server to start the install	1. Navigate to Host Management > Power Control. 2. Select the **Reset** option.  ORACLE Integrated Lights Out Manager v3.2.4.10 NAVIGATION System Information Summary Processors Memory Power Cooling Storage Networking PCI Devices Firmware Open Problems (0) Power Control Settings --- Select Action --- Reset Immediate Power Off Graceful Shutdown and Power Off Power On Power Cycle Control the host power from this page. To change th attempts to bring the OS down gracefully, then cuts *Reset* reboots the host immediately. More details... Host is currently on. --- Select Action --- 3. Click **Save**. Save 4. Confirm Save.

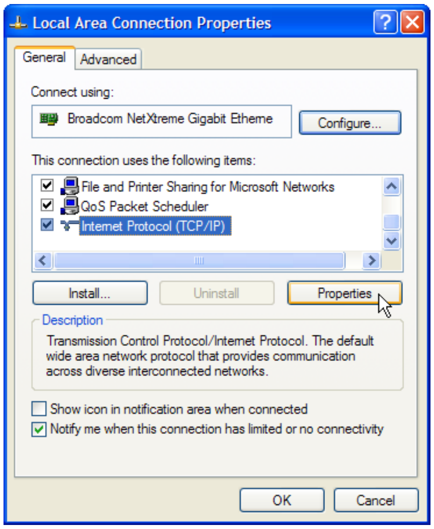
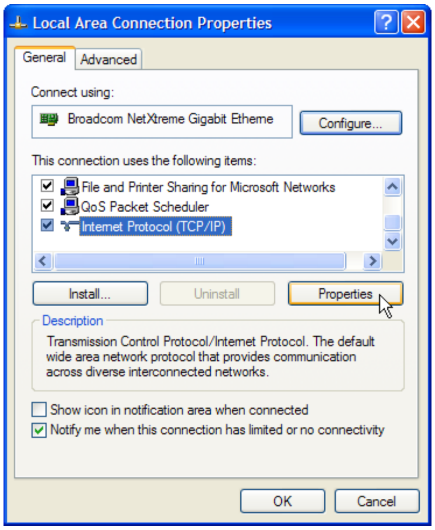
Appendix G. Configure TVOE iLO Access

Procedure 85. Connect to the TVOE iLO

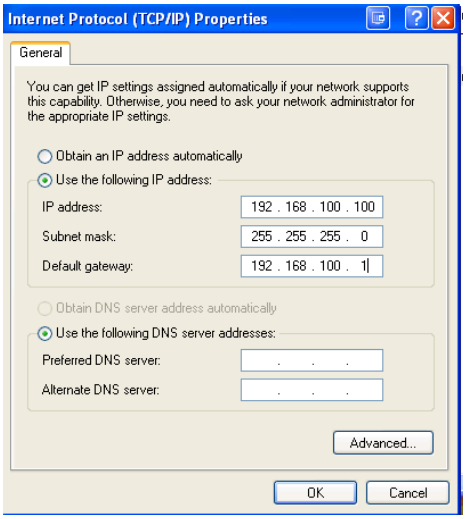
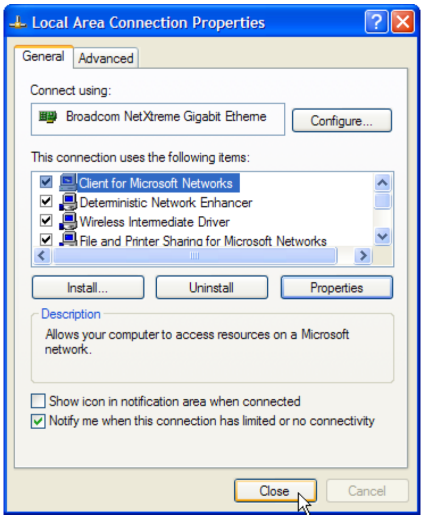
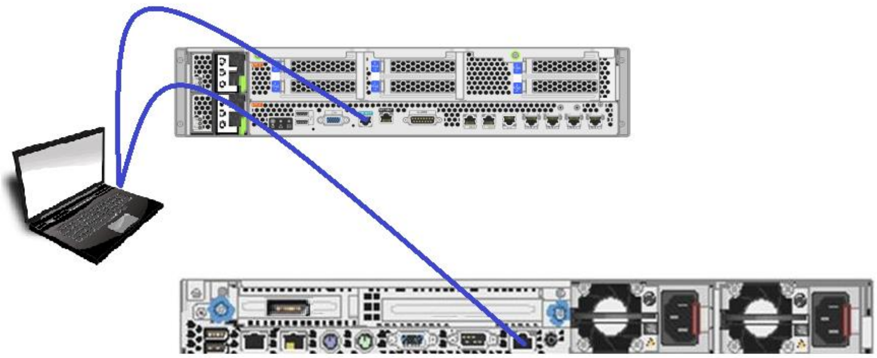
This procedure connects a laptop to the TVOE iLO using a directly cabled ethernet connection.

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

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

		Windows XP	**Windows 7**
1. ☐	Access the laptop network interface cards TCP/IP Properties screen. ***Note***: For this step, follow the procedure specific to the laptop's OS (XP or 7).	1. From the **Control Panel**, double click on **Network Connections**. 2. Right-click on the wired Ethernet Interface icon and click **Properties**. 3. Select **Internet Protocol (TCP/IP)**. 4. Click **Properties**.  Local Area Connection Properties General Advanced Configure... Install... Uninstall Properties OK Cancel Connect using: Broadcom NetXtreme Gigabit Etheme This connection uses the following items: ☑ File and Printer Sharing for Microsoft Networks ☑ QoS Packet Scheduler ☑ Internet Protocol (TCP/IP) Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. ☐ Show icon in notification area when connected ☑ Notify me when this connection has limited or no connectivity	1. From the **Control Panel**, double click on **Network and Sharing Center**. 2. Select **Change Adapter Settings** (left menu). 3. Right-click on the **Local Area Connection** icon and select **Properties**. 4. Click **Internet Protocol Version 4 (TCP/IPv4)**.  Local Area Connection Properties General Advanced Configure... Install... Uninstall Properties OK Cancel Connect using: Broadcom NetXtreme Gigabit Etheme This connection uses the following items: ☑ File and Printer Sharing for Microsoft Networks ☑ QoS Packet Scheduler ☑ Internet Protocol (TCP/IP) Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. ☐ Show icon in notification area when connected ☑ Notify me when this connection has limited or no connectivity

Procedure 85. Connect to the TVOE iLO

2. ☐	Set the IP properties	1. Click **Use the following IP address**. 2. Set the **IP address** to 192.168.100.100. 3. Set the **Subnet mask** to 255.255.255.0. 4. Set the **Default gateway** to 192.168.100.1. 5. Click **OK**. 6. Click **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:  Local Area Connection Properties General Advanced Connect using: Broadcom NetXtreme Gigabit Etherne This connection uses the following items: ☑ Client for Microsoft Networks ☑ Deterministic Network Enhancer ☑ Wireless Intermediate Driver ☑ File and Printer Sharing for Microsoft Networks 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 Configure... Install... Uninstall Properties 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

Procedure 86. Configure SNMP

This workaround configures SNMP with **SNMPv2c and SNMPv3** as the enabled versions for SNMP traps configuration since PMAC does not support SNMPv3.

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

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

1. ☐ **NOAM VIP GUI**: Login

Note: This workaround step should be performed only in these cases:

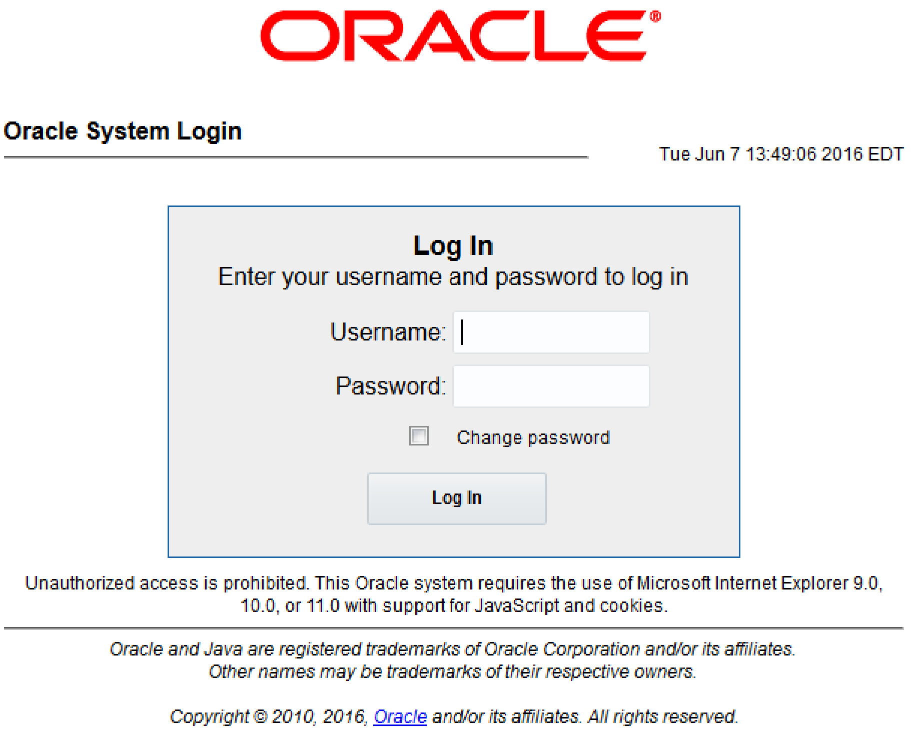
- If SNMP is not configured.
- If SNMP is already configured and SNMPv3 is selected as enabled version.

Note: This is a workaround step to configure SNMP with 'SNMPv2c and SNMPv3' as the enabled versions for SNMP Traps configuration, since PMAC does not support SNMPv3.

1. Establish a GUI session on the NOAM server using the VIP IP address of the NOAM server.
2. Open the web browser and enter a URL of:

```
https://<Primary_NOAM_VIP_IP_Address>
```

3. Log into the NOAM GUI as the **guiadmin** user:



Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies.

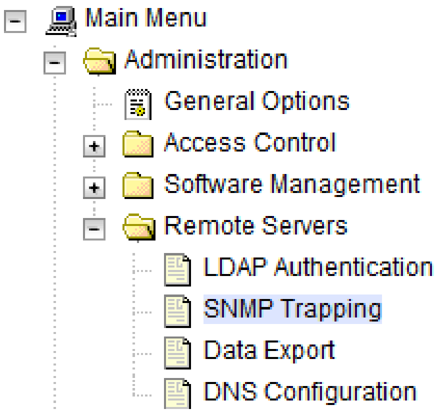
Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

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

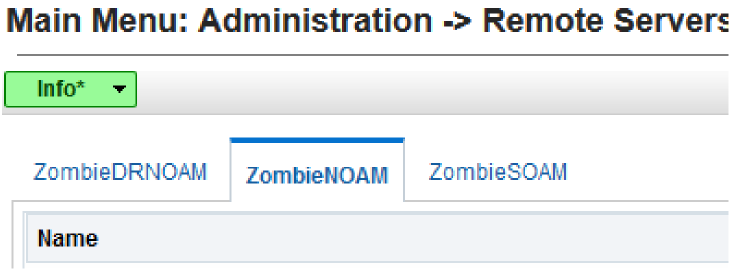
2. ☐ **NOAM VIP GUI**: Configure system-wide SNMP trap receiver(s)

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

Procedure 86. Configure SNMP

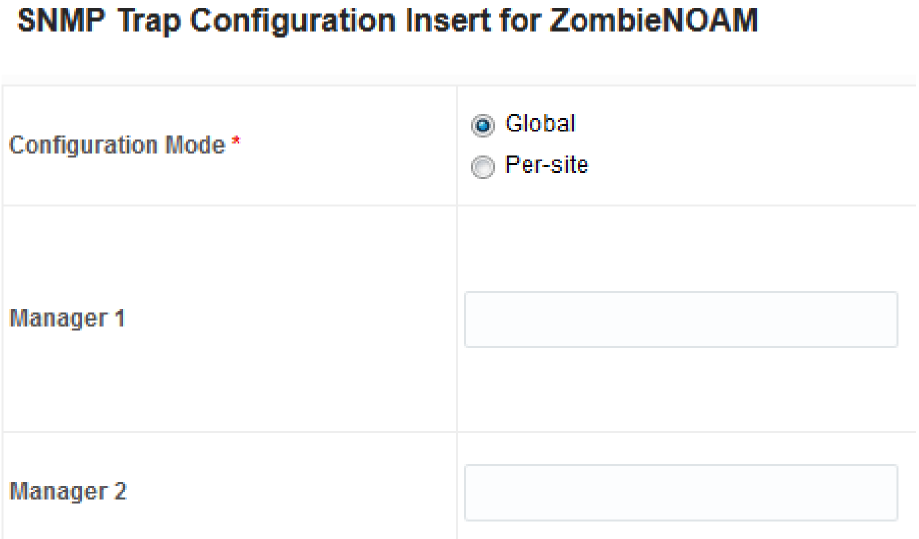

Main Menu
Administration
General Options
Access Control
Software Management
Remote Servers
LDAP Authentication
SNMP Trapping
Data Export
DNS Configuration

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


Main Menu: Administration -> Remote Servers
Info*
ZombieDRNOAM
ZombieNOAM
ZombieSOAM
Name

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

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

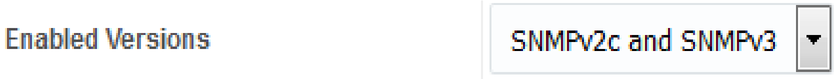

SNMP Trap Configuration Insert for ZombieNOAM

Configuration Mode * ● Global ○ Per-site

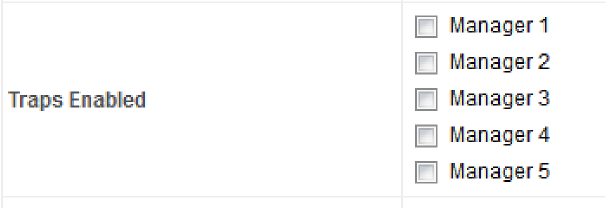
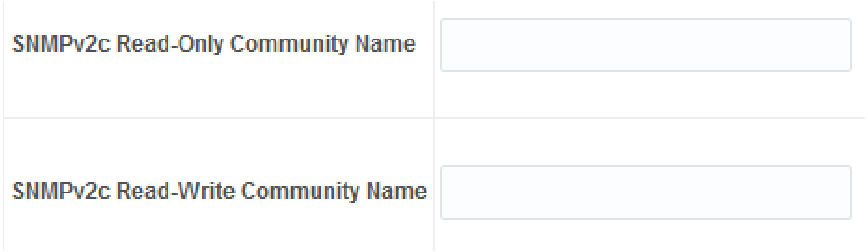
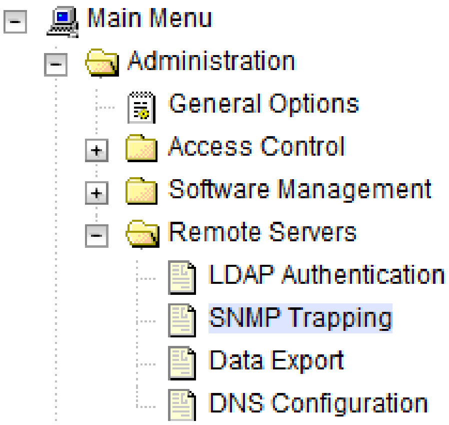
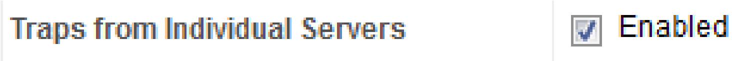
Manager 1

Manager 2

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


Enabled Versions: SNMPv2c and SNMPv3

Procedure 86. Configure SNMP

		6. Check **Traps Enabled** checkboxes for the Manager servers being configured.  Traps Enabled ☐ Manager 1 ☐ Manager 2 ☐ Manager 3 ☐ Manager 4 ☐ Manager 5 7. Type the SNMP Community Name.  SNMPv2c Read-Only Community Name SNMPv2c Read-Write Community Name 8. Leave all other fields at their default values. 9. Click **OK.**
3. ☐	**NOAMP VIP**: Enable traps from individual servers (optional)	***Note:*** By default SNMP traps from MPs are aggregated and displayed at the active NOAMP. If, instead, you want every server to send its own traps directly to the NMS, then execute this procedure. This procedure requires all servers, including MPs, to have an XMI interface on which the customer SNMP target server (NMS) is reachable. 1. Navigate to **Administration > Remote Servers > SNMP Trapping**.  Main Menu Administration General Options Access Control Software Management Remote Servers LDAP Authentication SNMP Trapping Data Export DNS Configuration 2. Make sure the **Enabled** checkbox is marked.  Traps from Individual Servers ☑ Enabled 3. Click **Apply** and verify the data is committed.

Procedure 86. Configure SNMP

4. ☐	**PMAC GUI**: Update the TVOE host SNMP community string	1. Establish an SSH session to the PMAC. 2. Login as **admusr**. 3. Update the TVOE hos community string with this command. `$ sudo pmaccli setCommStr --accessType=rw  --commStr=<site specific value>` ***Note:*** When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest on the PMAC control network are updated. All those servers that match the existing Site Specific Community String are not updated again until the string name is changed.

Appendix I. Install NetBackup Client

NetBackup is a utility that manages backups and recovery of remote systems. The NetBackup suite is used to support disaster recovery at the customer site. These procedures install and configure the NetBackup client software on an application server using two methods: first, using platcfg; and second, using nbAutoInstall (push Configuration). The supported versions of NetBackup are 7.6, and 7.7.

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.

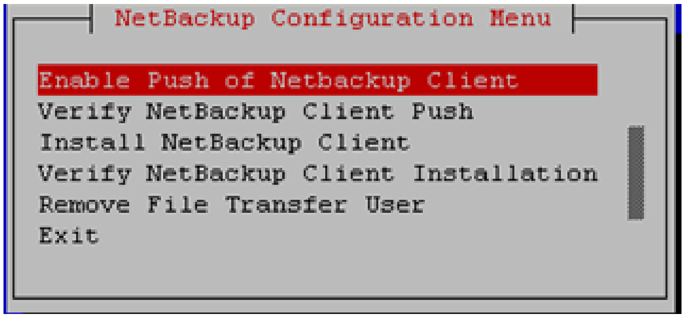
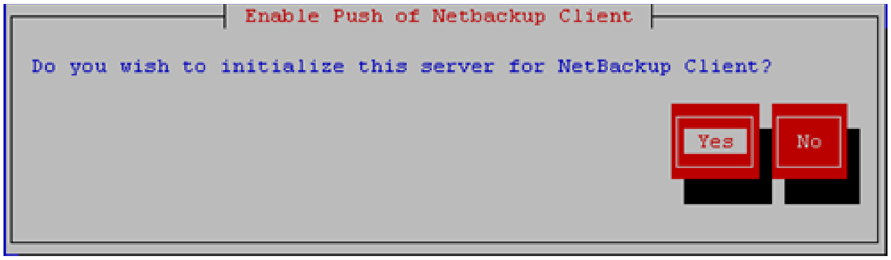
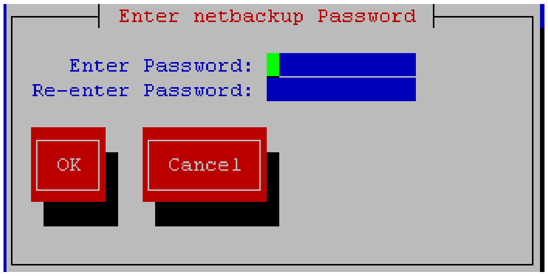
Appendix I.1 Install NetBackup Client Using platcfg

Execute this procedure to switch/migrate NetBackup installation using platcfg, instead of using NBAutoInstall (push configuration).

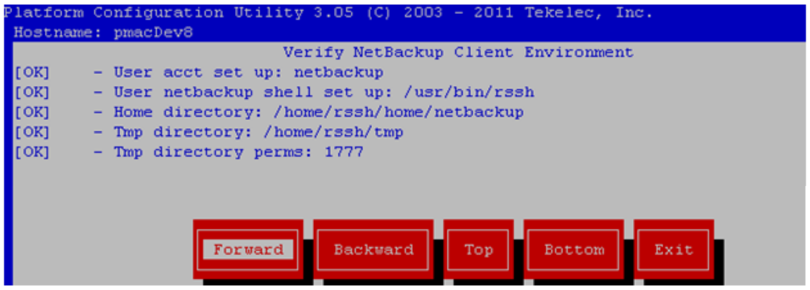
Procedure 87. Install NetBackup Client Using platcfg

S T E P #	This procedure installs NetBackup using platcfg. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Application Server**: Login	1. Login and launch the integrated remote console. 2. SSH to the application server (PMAC or NOAM) as **admusr** using the management network for the PMAC or XMI network for the NOAM.

Procedure 87. Install NetBackup Client Using platcfg

2. ☐	**Application Server iLO**: Navigate to NetBackup configuration	1. Enter the platcfg menu. `$ sudo su - platcfg` 2. Navigate to **NetBackup > Configuration**.  NetBackup Configuration Menu Enable Push of Netbackup Client Verify NetBackup Client Push Install NetBackup Client Verify NetBackup Client Installation Remove File Transfer User Exit
3. ☐	**Application Server iLO**: Enable push of NetBackup client	Navigate to **NetBackup Configuration > Enable Push of NetBackup Client**.  Enable Push of Netbackup Client Do you wish to initialize this server for NetBackup Client? Yes No
4. ☐	**Application Server iLO**: Enter NetBackup password	1. Enter the **NetBackup password**.  Enter netbackup Password Enter Password: Re-enter Password: OK Cancel 2. Select **OK**. 3. 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 being pushed.

Procedure 87. Install NetBackup Client Using platcfg

5. ☐	**Application Server iLO**: Verify NetBackup client software push is enabled	1. Navigate to **NetBackup Configuration > Verify NetBackup Client Push**. Platform Configuration Utility 3.05 (C) 2003 - 2011 Tekelec, Inc. Hostname: pmacDev8 Verify NetBackup Client Environment [OK] - User acct set up: netbackup [OK] - User netbackup shell set up: /usr/bin/rssh [OK] - Home directory: /home/rssh/home/netbackup [OK] - Tmp directory: /home/rssh/tmp [OK] - Tmp directory perms: 1777 2. Verify list entries indicate **OK** for NetBackup client software environment. 3. Select **Exit** to return to NetBackup Configuration menu.
6. ☐	**NetBackup Server**: Push appropriate NetBackup client software to application server	***Notes***: - The NetBackup server is not an application asset. Access to the NetBackup server and location path of the NetBackup Client software is under the control of the customer. These steps are required on the NetBackup server to push the NetBackup client software to the application server. These example steps assume the NetBackup server is executing in a Linux environment. - The backup server is supported by the customer, and the backup utility software provider. If this procedural STEP, executed at the backup utility server, fails to execute successfully, STOP and contact the Customer Care Center of the backup and restore utility software provider being used at this site. 1. Log into the NetBackup server using password provided by customer. 2. Navigate to the appropriate NetBackup Client software path. Example input: `$ cd /usr/openv/netbackup/client/Linux/RedHat2.6.18/` 3. Execute the **sftp_to_client** netbackup utility using the application IP address and application NetBackup user: **Note**: If the sftp fails, try to login to the DSR server using "netbackup" user and provide the password which was set in step 4 above. It will ask to change the password so change the password once.

Procedure 87. Install NetBackup Client Using platcfg

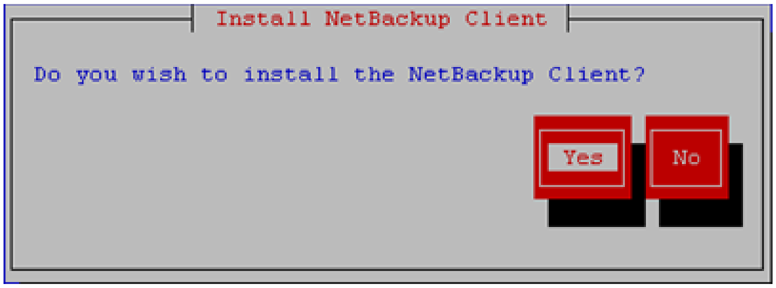
```
$ ./sftp_to_client <application IP> netbackup
Connecting to 192.168.176.31
NetBackup@192.168.176.31's password:
Enter application server NetBackup user password; the
following NetBackup software output is expected,
observe the sftp completed successfully:
File "/usr/openv/NetBackup/client/Linux/6.5/.sizes"
not found.
Couldn't rename file "/tmp/bp.6211/sizes" to
"/tmp/bp.6211/.sizes": No such file or directory
File "/usr/openv/NB-Java.tar.Z" not found.
./sftp_to_client: line 793: [: : integer expression expected
./sftp_to_client: line 793: [: : integer expression expected
./sftp_to_client: line 793: [: : integer expression expected
./sftp_to_client: line 793: [: : integer expression expected
./sftp_to_client: line 793: [: : integer expression expected
./sftp_to_client: line 793: [: : integer expression expected
./sftp_to_client: line 793: [: : integer expression expected
./sftp_to_client: line 793: [: : integer expression expected
./sftp_to_client: line 793: [: : integer expression expected
./sftp_to_client: line 793: [: : integer expression expected
./sftp_to_client: line 793: [: : integer expression expected
sftp completed successfully.
```

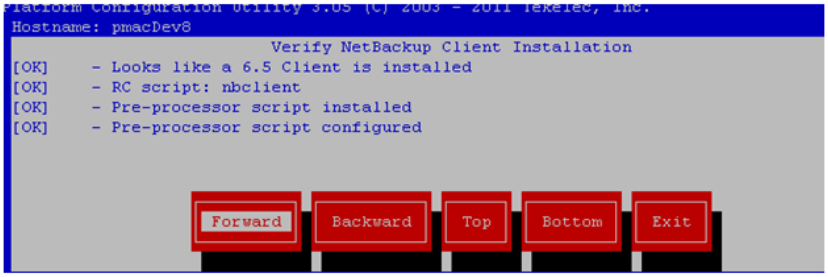
Notes:

- Although the command executed above instructs you to execute the client_config command, DO NOT execute that command since it is executed by platcfg in the next step.
- The optional argument, **-L**, is used to avoid modification of the client's current **bp.conf** file.

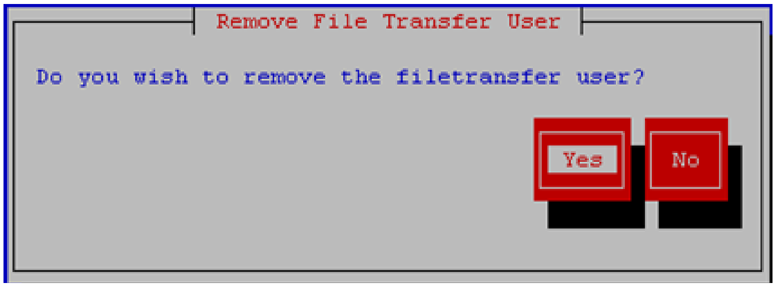
7.	**Set exec Permission**	1. Change the group ownership of init.d directory using below command:
		`sudo chgrp sys /etc/rc.d/init.d/`
		2. Change the permissions of /tmp using below commands:
		`sudo mount -o remount,exec /tmp`
		3. To verify that the "exec" permission is allotted to /tmp execute below command:
		`mount | grep "/tmp"`
		Above command should display, /tmp with exec permissions

Procedure 87. Install NetBackup Client Using platcfg

8.
☐
	Application server iLO: Install NetBackup client software on application server	1. Execute the command.
		`$ sudo chmod 555 /var/TKLC/home/rssh/tmp/bp.6211/client_config`
		where **NETBACKUP_BIN** is the temporary directory where the NetBackup client install programs were copied in step 5. The directory should look similar to **/tmp/bp.XXXX/**.
		2. Navigate to **NetBackup Configuration > Install NetBackup Client**.
		
		`Install NetBackup Client`
		`Do you wish to install the NetBackup Client?`
		
		3. Verify list entries indicate OK for NetBackup client software installation.
		4. Click **Exit** to return to NetBackup Configuration menu.

9.
☐
	Application Server iLO: Verify NetBackup client software installation on the application server	1. Navigate to **NetBackup Configuration > Verify NetBackup Client Installation**.
		
		`Platform Configuration Utility 3.05 (C) 2003 - 2011 Tekelec, Inc.`
		`Hostname: pmacDev8`
		`Verify NetBackup Client Installation`
		`[OK]     - Looks like a 6.5 Client is installed`
		`[OK]     - RC script: nbclient`
		`[OK]     - Pre-processor script installed`
		`[OK]     - Pre-processor script configured`
		
		2. Verify list entries indicate OK for NetBackup Client software installation.
		3. Click **Exit** to return to NetBackup Configuration menu.
		4. Modify the /tmp permissions back to "no exec" using below command:
		`sudo mount -o remount,noexec /tmp`
		5. Verify the permission using below command and check, /tmp has no exec permissions:
		`mount | grep "/tmp"`

Procedure 87. Install NetBackup Client Using platcfg

10. ☐	**Application Server iLO**: Disable NetBackup client software transfer to the application server	1. Navigate to **NetBackup Configuration > Remove File Transfer User**.  Remove File Transfer User Do you wish to remove the filetransfer user? 2. Click **Yes** to remove the NetBackup file transfer user from the application server.
11. ☐	**Application Server iLO**: Exit platform configuration utility (platcfg)	Exit out of platcfg by selecting **Exit**.

12.
☐
	Application Server iLO: Verify server **bp.conf** file	Verify the server has been added to the **/usr/openv/netbackup/bp.conf** file.
		`$ sudo cat /usr/openv/netbackup/bp.conf`
		`SERVER = NB71server`
		`CLIENT_NAME = 10.240.34.10`
		`CONNECT_OPTIONS = localhost 1 0 2`

13. ☐	**Application Server iLO**: Use platform configuration utility (platcfg) to modify hosts file with NetBackup server alias	See below

Note: After the successful transfer and installation of the NetBackup client software the NetBackup servers hostname can be found in the NetBackup **/usr/openv/netbackup/bp.conf** file, identified by the SERVER configuration parameter.

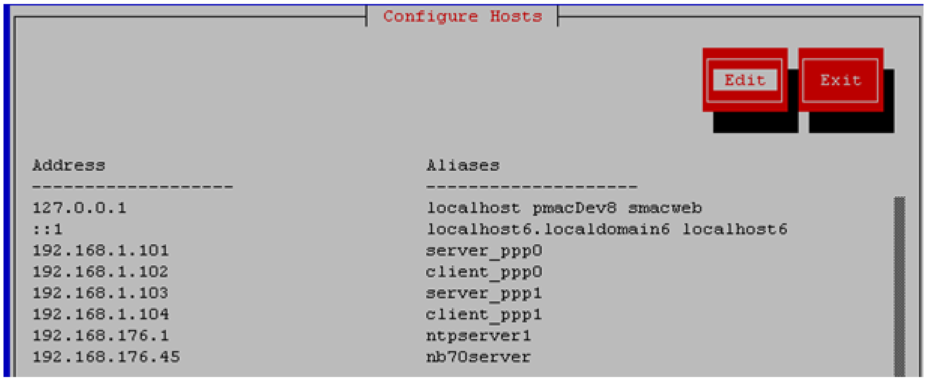
1. The NetBackup server hostname and IP address must be added to the application server's host's file. List the NetBackup server's hostname.

```
$ sudo cat /usr/openv/netbackup/bp.conf
SERVER = NB70server
CLIENT_NAME = pmacDev8
CONNECT_OPTIONS = localhost 1 0 2
```

2. Enter the platcfg menu to update application hosts file with the NetBackup Server alias.

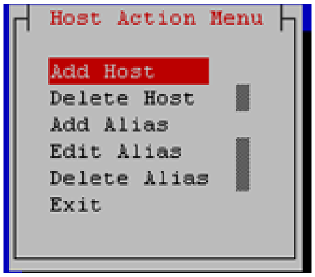
```
$ sudo su - platcfg
```

3. Navigate to **Network Configuration > Modify Hosts File**.
4. Click **Edit**.

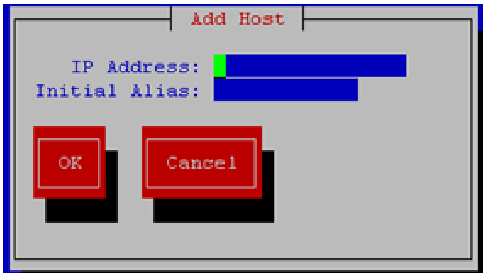

Configure Hosts
Edit
Exit

```
Address                                   Aliases
-------------------                       --------------------
127.0.0.1                                 localhost pmacDev8 smacweb
::1                                       localhost6.localdomain6 localhost6
192.168.1.101                             server_ppp0
192.168.1.102                             client_ppp0
192.168.1.103                             server_ppp1
192.168.1.104                             client_ppp1
192.168.176.1                             ntpserver1
192.168.176.45                            nb70server
```

5. **Click Add Host**.


Host Action Menu
Add Host
Delete Host
Add Alias
Edit Alias
Delete Alias
Exit

6. Enter the appropriate data and click **OK**.


Add Host
IP Address:
Initial Alias:
OK
Cancel

7. Confirm the host alias addition and exit the Platform Configuration Utility.

Procedure 87. Install NetBackup Client Using platcfg

14.
☐
	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.
		`$ sudo ln -s <path>/bpstart_notify /usr/openv/netbackup/bin/bpstart_notify`
		`$ sudo  ln -s <path>/bpend_notify /usr/openv/netbackup/bin/bpend_notify`
		An example of <path> is **/usr/TKLC/appworks/sbin**.

Appendix I.2 Install NetBackup Client Using NBAutoInstall

Execute this procedure to switch/migrate NetBackup installation using NBAutoInstall (push configuration), instead of manual installation using platcfg.

Notes:

- Skip this procedure for DSR 8.4 VE DSR Deployment on X7-2.
- This procedure enables TPD to automatically detect when a NetBackup Client is installed and then completes TPD related tasks needed for an effective NetBackup Client operation. With this procedure, the NetBackup Client installation (pushing the client and performing the installation) is the responsibility of the customer and is not covered in this procedure

Procedure 88. Install NetBackup Client Using NBAutoInstall

STEP #	This procedure installs NetBackup using NBAutoInstall. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**Application Server iLO**: Login	1. Login and launch the integrated remote console. 2. 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	`$ sudo /usr/TKLC/plat/bin/nbAutoInstall –-enable`

3.
☐
	Application Server iLO: Create links to NetBackup client notify scripts on the application server where NetBackup expects to find them	`$ 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`
		An example of <path> is **/usr/TKLC/appworks/sbin**.

Procedure 88. Install NetBackup Client Using NBAutoInstall

4.
☐
	Application Server iLO: Verify NetBackup configuration file	1. Open **/usr/openv/netbackup/bp.conf** and make sure it points to the NetBackup server.
		`$ sudo vi /usr/openv/netbackup/bp.conf`
		`SERVER = nb75server`
		`CLIENT_NAME = 10.240.10.185`
		`CONNECT_OPTIONS = localhost 1 0 2`
		Note: Verify the server name matches the NetBackup server, and verify the CLIENT_NAME matches the hostname or IP of the local client machine. If they do not, update them as necessary.
		2. Edit **/etc/hosts** and add the NetBackup server.
		`$ sudo vi /etc/hosts`
		`e.g.: 192.168.176.45      nb75server`
		Note: The server now periodically checks for a new version of the NetBackup client and performs necessary TPD configuration accordingly.
		3. At any time, you can push and install a new version of the NetBackup client.

Appendix I.3 Create NetBackup Client Configuration File

Procedure 89. Create NetBackup Client Configuration File

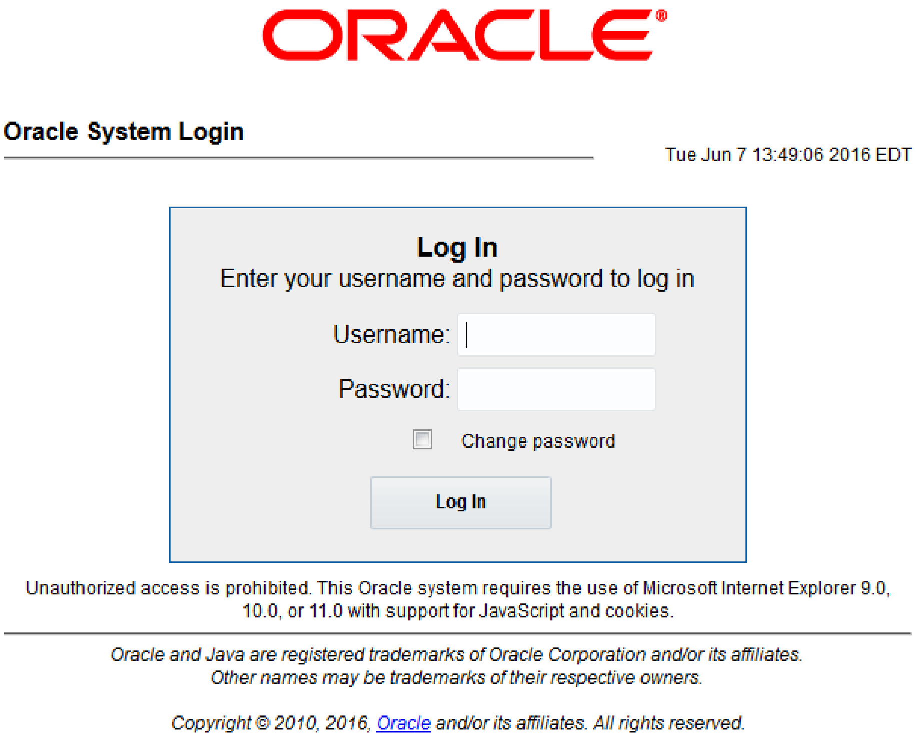
S T E P #	This procedure copies a NetBackup Client config file into the appropriate location on the TPD based application server. This config file installs previously unsupported versions of NetBackup Client by providing necessary information to TPD. ***Note:*** Skip this procedure for DSR 8.4 VE deployments. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	**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 **/usr/TKLC/plat/etc/netbackup/profiles** directory and should follow this naming convention: 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: /usr/TKLC/plat/etc/netbackup/profiles/NB75.conf ***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.

Procedure 89. Create NetBackup Client Configuration File

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 **/usr/TKLC/plat/etc/NetBackup/scripts** 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: **NetBackup Client config**: /usr/TKLC/plat/etc/netbackup/profiles/NB75.conf **NetBackup Client config script**: /usr/TKLC/plat/etc/netbackup/scripts/NB75

Appendix I.4 Configure PMAC Application NetBackup Virtual Disk

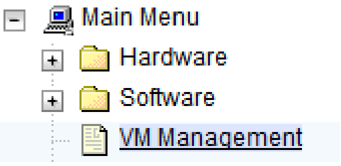
Procedure 90. Configure PMAC Application NetBackup Virtual Disk

This procedure configures 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**: Login	1. Open the web browser and navigate to the PMAC GUI: `http://<PMAC_network_IP>` 2. Login as the **guiadmin** user.  ORACLE Oracle System Login Log In Username: Password: ☐ Change password Log In Tue Jun 7 13:49:06 2016 EDT Enter your username and password to log in Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

Procedure 90. Configure PMAC Application NetBackup Virtual Disk

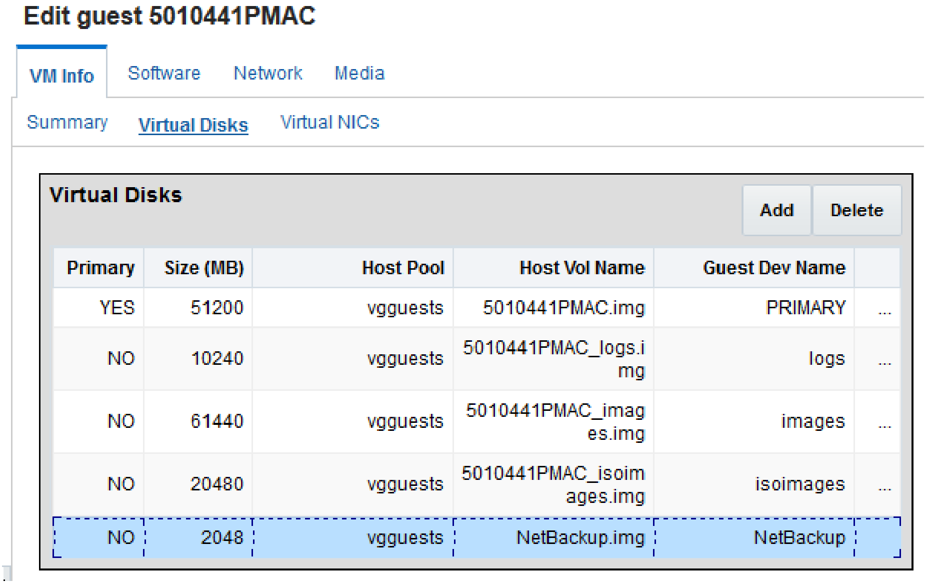
2. ☐ **PMAC GUI**: Create NetBackup virtual disk

1. Navigate to **VM Management**.


Main Menu
Hardware
Software
VM Management

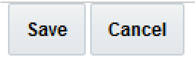
2. Click **Edit** and enter this data for the new NetBackup virtual disk.

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

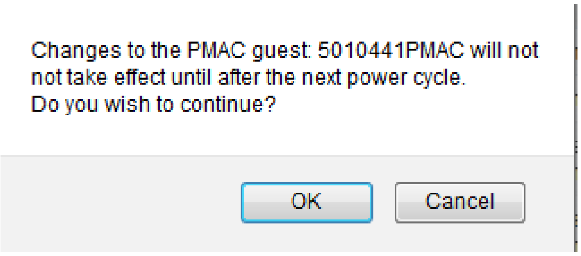

Edit guest 5010441PMAC
VM Info
Software
Network
Media
Summary
Virtual Disks
Virtual NICs
Virtual Disks
Add
Delete

Primary	Size (MB)	Host Pool	Host Vol Name	Guest Dev Name	
YES	51200	vgguests	5010441PMAC.img	PRIMARY	...
NO	10240	vgguests	5010441PMAC_logs.img	logs	...
NO	61440	vgguests	5010441PMAC_images.img	images	...
NO	20480	vgguests	5010441PMAC_isoimages.img	isoimages	...
NO	2048	vgguests	NetBackup.img	NetBackup	

3. Click **Save** to continue.


Save
Cancel

4. Click **OK** to confirm.



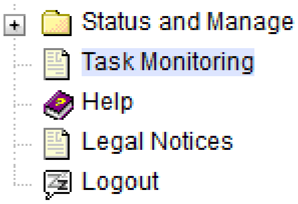
Changes to the PMAC guest: 5010441PMAC will not not take effect until after the next power cycle.
Do you wish to continue?

Procedure 90. Configure PMAC Application NetBackup Virtual Disk

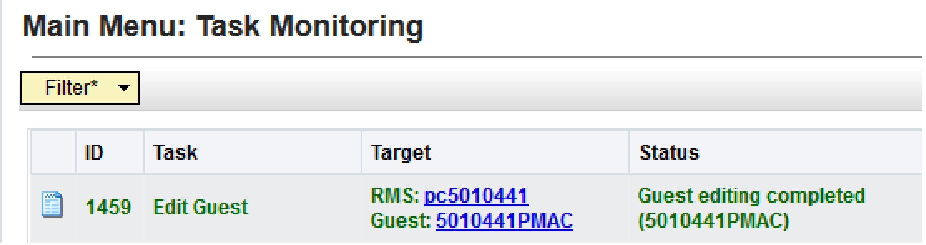
<table>
<tr>
<td>3.
☐</td>
<td>PMAC GUI:
Verify NetBackup virtual disk</td>
<td>

Confirm the **Edit VM Guest** task has completed successfully.

1. Navigate to **Task Monitoring**.


Status and Manage
Task Monitoring
Help
Legal Notices
Logout

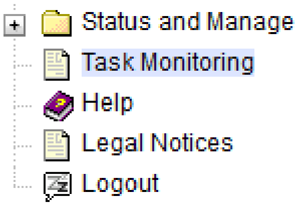
2. Confirm the guest edit task has completed successfully.


Main Menu: Task Monitoring
Filter*

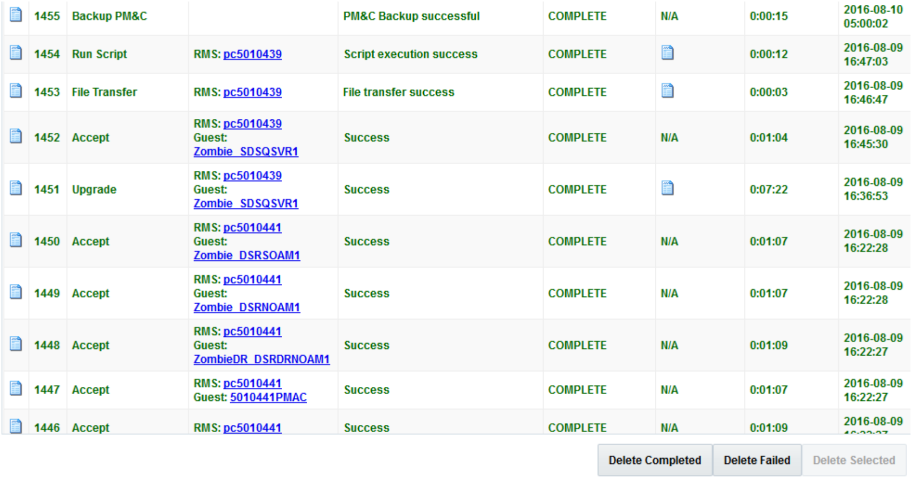
	ID	Task	Target	Status
	1459	Edit Guest	RMS: pc5010441 Guest: 5010441PMAC	Guest editing completed (5010441PMAC)

</td>
</tr>
<tr>
<td>4.
☐</td>
<td>PMAC GUI:
Verify In-Progress tasks</td>
<td>

1. Navigate to **Task Monitoring**.


Status and Manage
Task Monitoring
Help
Legal Notices
Logout

2. If any tasks show as in-progress (blue), then wait for the task to complete before 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_DSRSOAM1	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

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 leaves only the in-progress tasks.

</td>
</tr>
</table>

Procedure 90. Configure PMAC Application NetBackup Virtual Disk

5. ☐ **Management Server TVOE iLO/iLOM**: SSH into the management server

3. Using an SSH client such as putty, ssh to the TVOE host as **admusr**.
4. Login using **virsh** and wait until you see the login prompt:

```
$ sudo /usr/bin/virsh list

Id  Name  State
----------------------------------
1  myTPD  running
2  PM&C   running
```

```
$ 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.
PM&Cdev7 login:
```

6. ☐ **PMAC**: Shut down the PMAC guest

Assuming no in-progress tasks exist, it is safe to shut down the PMAC guest.

Execute this command.

```
[admusr@pmac ~]$ sudo /usr/bin/halt -p
Broadcast message from root@pmacDev901
(/dev/ttyS0) at 11:20 ...
The system is going down for power off NOW!
```

Eventually the virsh console session is closed and you are returned to the TVOE host command prompt.

```
Halting system...
Power down.
[admusr@tvoe ~]$
```

7. ☐ **Management Server TVOE iLO/iLOM**: Verify PMAC guest is shut down

1. From the TVOE host command prompt, execute this command.

```
[admusr@tvoe ~]$ sudo /usr/bin/virsh list --all
Id  Name  State
----------------------------------
-   pmac  shut off
```

This displays the guest state as **shut off**.

2. Make sure all guests are in the shut off state.

Procedure 90. Configure PMAC Application NetBackup Virtual Disk

8. ☐ **Management Server TVOE iLO/iLOM**: Start the PMAC guest

```
$ sudo /usr/bin/virsh
virsh # list --all
Id  Name       State
----------------------------------
20  pmacU14-1  shut off

virsh # start pmacU14-1
Domain pmacU14-1 started

virsh # list --all
Id  Name       State
----------------------------------
20  pmacU14-1  running
```

Appendix J. List of Frequently Used Time Zones

This table lists several valid time zone strings that can be used for the time zone setting in a CSV file, or as the time zone parameter when manually setting a DSR blade time zone. For an exhaustive list of **ALL** time zones, log into the PMAC server console and view the **/usr/share/zoneinfo/zone.tab** text file.

Table 5. List of Selected Time Zone Values

Time Zone Value	Description	Universal Time Code (UTC) Offset
UTC	Universal Time Coordinated	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

Time Zone Value	Description	Universal Time Code (UTC) Offset
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 & west Saskatchewan	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

Procedure 91. Configure PMAC Application NetBackup Virtual Disk

This procedure upgrades 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, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**Virtual PMA**C: Verify PROM image is on the system	Determine if the PROM image for the 4948E-F is on the system. Execute this command. `$ ls /var/TKLC/smac/image/<PROM_image_file>` ***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 [1] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes (Min 2.2.12).
2. ☐	**Virtual PMAC**: Attach to switch console	1. Connect serially to the switch by issuing this command as **admusr** on the server.

```
$ 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
```

2. If the switch is not already in enable mode (**switch#** prompt), then issue the **enable** command; otherwise, continue with the next step.

```
Switch> enable
Switch#
```

Procedure 91. Configure PMAC Application NetBackup Virtual Disk

3. ☐ **4948E-F**: Configure ports on the switch on the 4948E-F switch

1. To ensure connectivity, ping the management server's management VLAN IP <pmac_mgmt_ip_address> address from the switch.
2. Execute these commands.

```
Switch# conf t
Switch(config-if)# switchport mode trunk
Switch(config-if)# spanning-tree portfast trunk
Switch(config-if)# end
Switch# write memory
```

3. Issue **ping** command.

```
Switch# ping <pmac_mgmtVLAN_ip_address>
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 My Oracle Support (MOS).

4. ☐ **4948E-F**: Upgrade PROM

```
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#
```

5. ☐ **4948E-F**: Reload the switch

```
Switch# reload
System configuration has been modified. Save? [yes/no]:
no
Proceed with reload? [confirm] [Enter]
=== Boot messages removed ===
```

Note: Press **Ctrl+C** when the **Type control-C to prevent autobooting** message displays.

Procedure 91. Configure PMAC Application NetBackup Virtual Disk

6. ☐ **4948E-F**: Initiate the PROM upgrade

```
rommon 1 > boot bootflash:<PROM_image_file>
=== PROM upgrade messages removed ===
System will reset itself and reboot within few
seconds....
```

The switch reboots when the firmware upgrade completes.

1. Allow it to boot up.
2. Wait for this line to display.

```
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
```

3. Review the output and look for the ROM version.
4. Verify the version is the desired new version.

   If the switch does not boot properly or has the wrong ROM version, contact My Oracle Support (MOS).

7. ☐ **4948E-F**: Reset switch factory defaults

```
Switch# write erase
Switch# reload
```

Notes:

- Wait until the switch reloads, then exit from console, press **<ctrl-e><c><.>** to return to the server prompt.
- If asked to confirm, press **Enter**. If asked yes or no, type **no** and press **Enter**.

Appendix L. Sample Network Element

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 create different network names accidentally for the NOAMP and SOAM network elements and then the mapping of services to networks is not possible.

Note: In Figure 3. Example Network Element XML File, IP values are network ID IPs and not host IPs.

```
<?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>
```

Figure 3. Example Network Element XML File

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 is performed during server creation.

Appendix M. Configure IDIH Fast Deployment

The fdc.cfg file contains sections. This table lists 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

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-8.2.1.0.0-82.23.0-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 cannot 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 these 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:

Notes:

- 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 (for example, 64).
- 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, 2016,2018 Oracle and/or its affiliates. All rights
reserved.
-->

<fdc>
  <infrastructures>
    <infrastructure name="localPMAC">
      <software>
        <image id="ora">
          <name>oracleGuest-8.2.1.0.0-82.23.0-x86_64</name>
        </image>
        <image id="med">
          <name>mediation-8.2.1.0.0-82.23.0-x86_64</name>
        </image>
        <image id="app">
          <name>apps-8.2.1.0.0-82.23.0-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>
          <rmspassword>changeme</rmspassword>
        </rms>
        <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="mgmtsrvrtvoe1">
        <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>mgmtsrvrtvoe1</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>
      </vdisks>
      <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/utils/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>
      <vdisks>
        <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>
        <vnic>
          <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. Create a Bootable USB Drive on Linux

Procedure 92. Configure PMAC Application NetBackup Virtual Disk

This procedure upgrades the Cisco 4948 PROM.

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

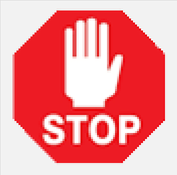
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.

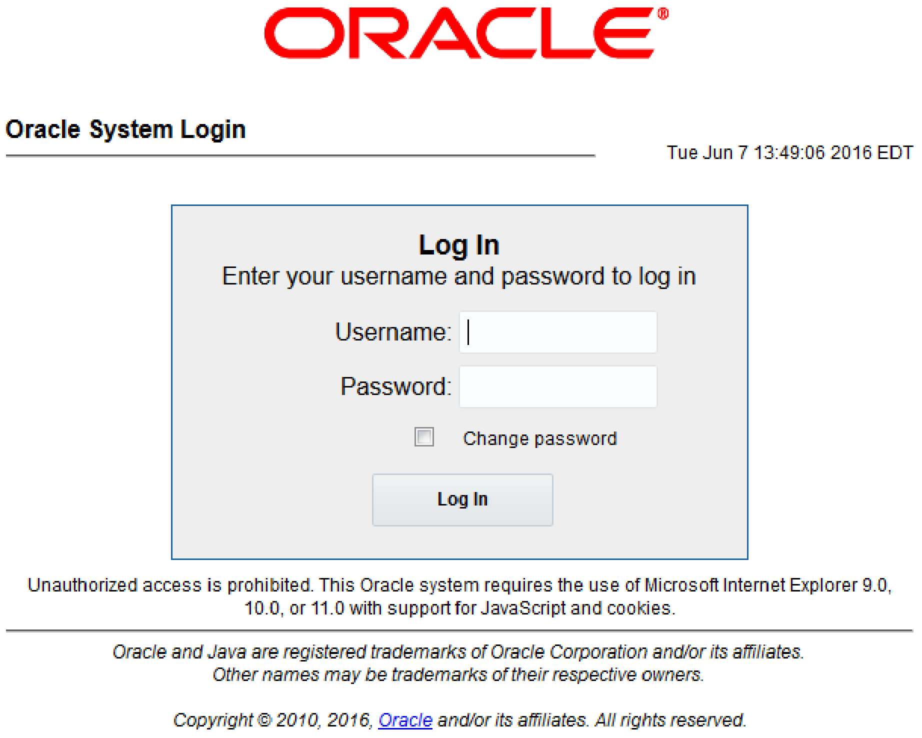
1. ☐	Insert USB Media	1. Insert the USB media into the USB port. It should automatically be mounted under /media 2. Obtain the path of the USB drive by running. `$ ls /media` The output should be similar to this: sdb1 3. Note the path without the partition number (in this case, it would be /dev/sdb).
2. ☐	Linux Machine	Obtain the TVOE .iso file and copy it onto the local Linux computer (for example, 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. Remove IDIH External Drive

Run this procedure only if you intend to do a fresh installation on an existing IDIH.

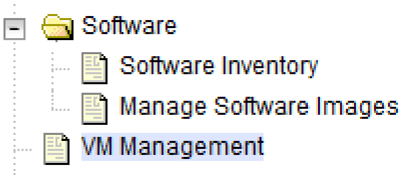
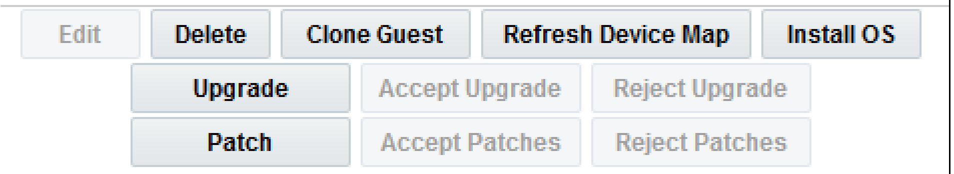
Procedure 93. Remove the IDIH External Drive

<table>
<tr><td colspan="3">This procedure destroys all data in the Oracle database.


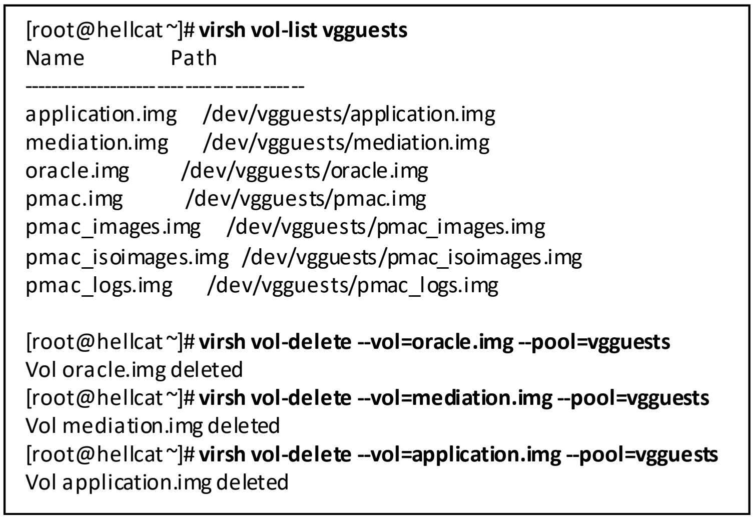
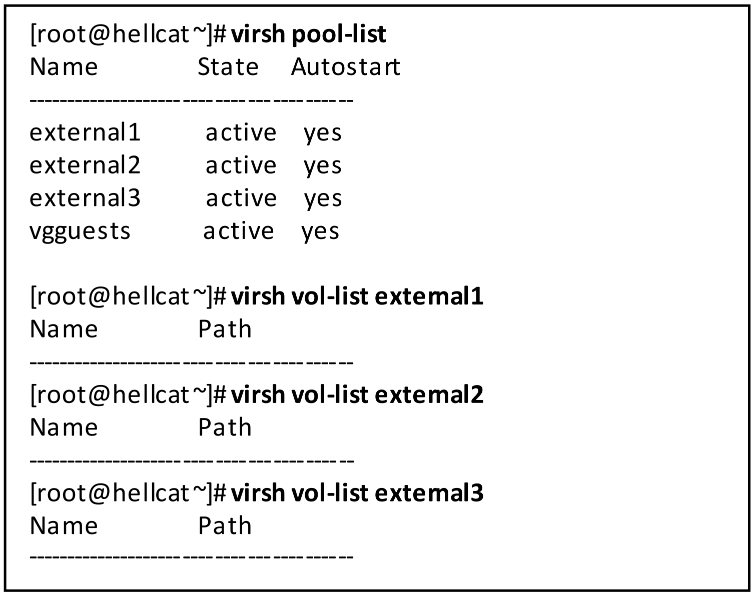
Warning
Do not perform this procedure on an IDIH system unless your intent is to do a fresh TVO installation.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.
If this procedure fails, it is recommended to contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>**PMAC GUI**: Login</td><td>1. Open the web browser and navigate to the PMAC GUI:
`http://<PMAC_network_IP>`
2. Login as the **guiadmin** user.

Oracle System Login
Tue Jun 7 13:49:06 2016 EDT
Log In
Enter your username and password to log in
Username:
Password:
☐ Change password

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.</td></tr>
</table>

Procedure 93. Remove the IDIH External Drive

2. ☐	**PMAC GUI**: Delete VMs, if Needed	Before a re-installation can be performed, the IDIH VMs must be removed first. 1. Navigate to **VM Management**.  Software Software Inventory Manage Software Images VM Management 2. Select each of the IDIH VMs and click **Delete**.  Edit Delete Clone Guest Refresh Device Map Install OS Upgrade Accept Upgrade Reject Upgrade Patch Accept Patches Reject Patches
3. ☐	**IDIH TVOE Host**: Login	Establish an SSH session to the TVOE host and login as **admusr**.
4. ☐	**IDIH TVOE HOST**: Verify external drive exists	**HP DL380** `$ sudo hpssacli ctrl slot=2 Id all show`

Procedure 93. Remove the IDIH External Drive

5. ☐	**IDIH TVOE Host**: Remove the external drive and volume group	**HP DL380** `$ sudo /usr/TKLC/plat/sbin/storageClean hpdisk --slot=2` **Oracle X5-2/Netra X5-2/X6-2** Log into the TVOE host as root user and execute the virsh commands to delete the image files manually. Make sure the storage pool, other than vgguests, is also cleaned.  

```
[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
```

```
[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
----------------------------------------
```

Appendix P. Growth/De-Growth/Re-Shuffle (Oracle X5-2/Netra X5-2/X6-2/X7-2/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. For more information, refer to the following sections in the C-Class Software Installation and Configuration Procedure 2/2:

- Appendix L.1 explains how to add individual VMs and add various DSR/SDS servers.
- Appendix L.2 explains how to delete individual VMs and move or remove various DSR/SDS servers.

Appendix P.1 Growth (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 (10Gbps) Only)

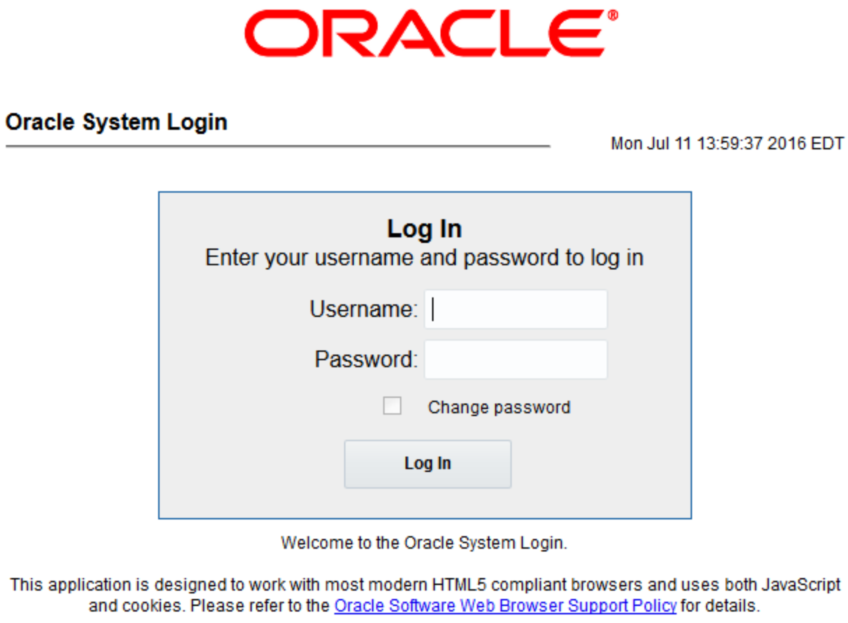
For growth scenarios where it is necessary to add DSR servers, follow these procedures.

Step	Procedure(s)
Perform backups	Procedure 94 Perform Backups
Perform system health check	Procedure 95 Perform Health Check
Identify servers affected by growth: • DR NOAM • SOAM Spares • MP (IPFE, SBR, SS7-MP)/SDS DP • Query Server	
Add new servers Create and configure the VMs on new servers (SOAM spare and DR NOAMs only)	Procedure 96 Add a New TVOE Server/VMs
Configure servers in new VM locations	**NOAM/DR NOAM (DSR/SDS)**: Procedure 97 Growth: DR NOAM **SOAM (DSR/SDS)**: Procedure 98 Growth: SOAM Spare (DSR/PCA Only) **MP/DP (DSR/SDS)**: Procedure 99 Growth: MP or Procedure 100 Growth: MP (For 7.x to 8.x Upgraded System) **Query Server**: Procedure 101 Growth: Query Server (SDS Only)
Post growth health check	Procedure 102 Post Growth Health Check
Post growth backups	Procedure 103 Post Growth Backups

Procedure 94. Perform Backups

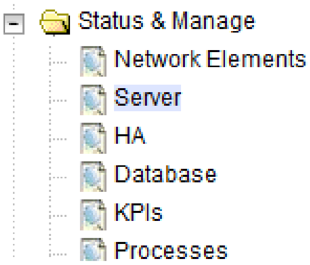
This procedure backs up all necessary items before a growth scenario. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Backup TVOE	Back up all TVOE host configurations by executing section 3.17.6 Back Up TVOE Configuration.
2. ☐	Backup PMAC	Back up the PMAC application by executing section 3.17.7 Back Up PMAC Application.
3. ☐	Backup NOAM/SOAM databases	Back up the NOAM and SOAM databases by executing sections 3.17.8 Back Up NOAM Database and 3.17.9 Back Up SOAM Database. ***Note:*** Database backup on SDS SOAMs is not required.

Procedure 95. Perform Health Check

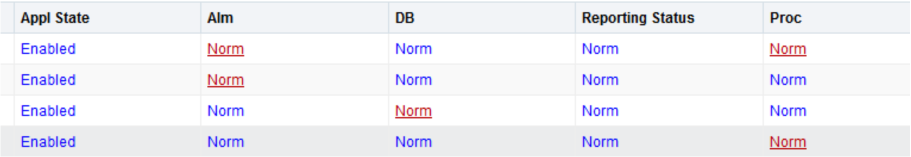
This procedure verifies system status and logs all alarms. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  ORACLE **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.

Procedure 95. Perform Health Check

<table>
<tr>
<td>2.
☐</td>
<td>NOAM VIP GUI: Verify server status</td>
<td>
1. Navigate to Status & Manage > Server.

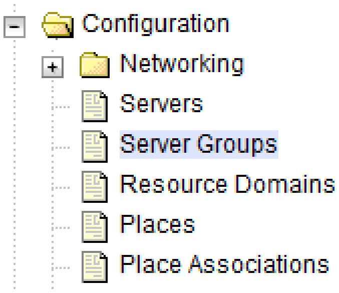

Status & Manage
Network Elements
Server
HA
Database
KPIs
Processes

2. 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>

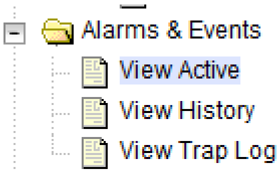
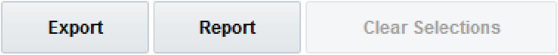
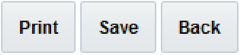
Do not proceed with Growth/De-Growth if any of the above states are not Norm. If any of these are not Norm, corrective action should be taken to restore the non-Norm status to Norm before proceeding with the feature activation.

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.
</td>
</tr>
<tr>
<td>3.
☐</td>
<td>NOAM VIP GUI: Verify server configuration</td>
<td>
1. Navigate to Configuration > Server Groups.


Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Verify the configuration data is correct for your network.
</td>
</tr>
</table>

Procedure 95. Perform Health Check

4. ☐	**NOAM VIP GUI**: Log current alarms	1. Navigate to **Alarms & Events > View Active**.  Alarms & Events View Active View History View Trap Log 2. Click **Report**.  3. **Save** or **Print** this report, keep copies for future reference. 
5. ☐	**SOAM VIP GUI**: Repeat for SOAM	Repeat this procedure for the SOAM.

Procedure 96. Add a New TVOE Server/VMs

This procedure adds 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 My Oracle Support (MOS) and ask for assistance.

1. ☐	Add/Configure additional servers	Follow these sections to install and configure TVOE on additional rack mount servers: 1. Section 3.7 Add a Rack Mount Server to PMAC 2. Section 3.8 Install TVOE on Additional Rack Mount Servers 3. Section 3.9 Configure TVOE on Additional Rack Mount Servers
2. ☐	Add/Configure new VMs	1. Determine CPU placement and pinning information by referring to section 3.10 Determine VM Placement. 2. Create new virtual machines by following section 3.12 Virtual Machine/Network Fast Deployment. 3. Perform CPU pinning by following section 3.13 CPU Pinning.

Procedure 97. Growth: DR NOAM

This procedure configures 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 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 these procedures: **DSR DR NOAM**: Section 3.14.3 Disaster Recovery NOAM (Optional) **SDS DR NOAM**: Section 3.15.3 Disaster Recovery NOAM (Optional)
2. ☐	**DR NOAM**: Activate optional features. DSR only. If SDS DR NOAM, then skip this step.	If there are any optional features currently activated, the feature activation procedures need to be run again. Refer to section 1.5 Optional Features.
3. ☐	**DR NOAM VIP**: Login	Establish an SSH to the DR NOAM VIP address and login as **admusr**.

4.
☐
	DR NOAM VIP: Transfer optimization script from the primary NOAM	Execute these commands to transfer and set permissions of the optimization script from the primary NOAM.
		`$ sudo scp -r admusr@<Primary NOAM XMI VIP>:/usr/TKLC/dsr/bin/rmsNoamConfig.sh /usr/TKLC/dsr/bin`
		`$ sudo chmod 777 /usr/TKLC/dsr/bin/rmsNoamConfig.sh`

5.
☐
	NOAM VIP: Execute the optimization script on the active NOAM	Execute these commands for the performance optimization script on the active NOAM server.
		`$ cd /usr/TKLC/dsr/bin/`
		`$ sudo ./rmsNoamConfig.sh`
		Note: Configuration successful output should display.

6.
☐
	NOAM VIP: Execute the key revocation script on the active NOAM server (RADIUS only) to copy key file to new NOAM server created	**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).**
		`$ cd /usr/TKLC/dsr/bin/`
		`$ ./sharedKrevo -synchronize –server <new_NOAM_hostname>`
		Note: Key transfer successful output should display.

Procedure 98. Growth: SOAM Spare (DSR/PCA Only)

This procedure configures 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 My Oracle Support (MOS) and ask for assistance.

1. ☐	**NOAM VIP GUI**: Configure the SOAM spare	Configure the SOAM spare by executing these procedures: • Procedure 24 Configure DSR SOAM NE • Procedure 25 Configure DSR SOAM Server • Procedure 26 Configure the DSR SOAM Server Group (steps 1. , 4. , 6. , and 9.)
2. ☐	**NOAM GUI**: Activate optional features	If there are any optional features currently activated, the feature activation procedures need to be run again. Refer to section 1.5 Optional Features.

3.
☐
	NOAM VIP: Execute the key revocation script on the active NOAM server (RADIUS) to copy key file to new SOAM server created	**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).**
		`$ cd /usr/TKLC/dsr/bin/`
		`$ ./sharedKrevo -synchronize –server <new_SOAM_hostname>`
		Note: Key transfer successful output should be given.

Procedure 99. Growth: MP/DP

This procedure configures 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 My Oracle Support (MOS) and ask for assistance.

1. ☐	**NOAM VIP GUI**: Configure the MP	Configure the MP/DP by executing the steps referenced in these procedures: **DSR MP** • To configure MP blade servers (IPFE, SBR, DA-MP), refer to the procedure Configure MP Blade Servers in the C-Class Software Installation and Configuration Procedure 2/2. • To configure Places and Assign MP servers to Places (PCA and DCA), refer to the procedure Configure Places and Assign MP Servers to Places (PCA/DCA Only) in the C-Class Software Installation and Configuration Procedure 2/2. • To configure DAMP Server Groups and Profiles, refer to the procedure Configure the MP Server Group(s) and Profile(s) in the C-Class Software Installation and Configuration Procedure 2/2. • Procedure 61 Back Up the Upgrade and Disaster Recovery FDC File (Optional) **SDS DP** • Procedure 47 Pair SDS Query Server with SDS NOAMs • Procedure 48 Configure SDS DP SOAM NE • Procedure 61 Back Up the Upgrade and Disaster Recovery FDC File (Optional)

2.
☐
	NOAM VIP: Execute the key revocation script on the active NOAM server (RADIUS) to copy key file to new MP server created	**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.**
		`$ cd /usr/TKLC/dsr/bin/`
		`$ ./sharedKrevo -synchronize –server <new_MP_hostname>`
		Note: Key transfer successful output should be given.

Procedure 100. Growth: MP (For 7.x to 8.x Upgraded System)

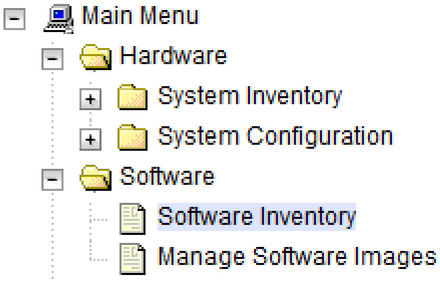
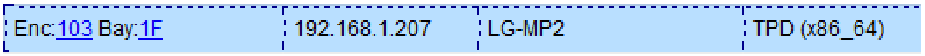
This procedure should be executed **ONLY** to configure an MP on the new virtual machine for growth scenarios for 7.x to 8.x upgraded system.

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 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. 1. From the MP site's PMAC GUI, navigate to **Software** > **Software Inventory**.  Main Menu Hardware System Inventory System Configuration Software Software Inventory Manage Software Images 2. Note the IP address for an MP server. Enc:103 Bay:1F 192.168.1.207 LG-MP2 TPD (x86_64) 3. Obtain a terminal session to the MP site's PMAC and login as **admusr**. 4. Exchange SSH keys for admusr between the PMAC and the MP blade server using the keyexchange utility and the control network IP address for the MP blade server. `$ keyexchange admusr@<MP_Control_Blade_IP Address>` 5. When asked for the password, type the password for the **admusr** of the MP server.

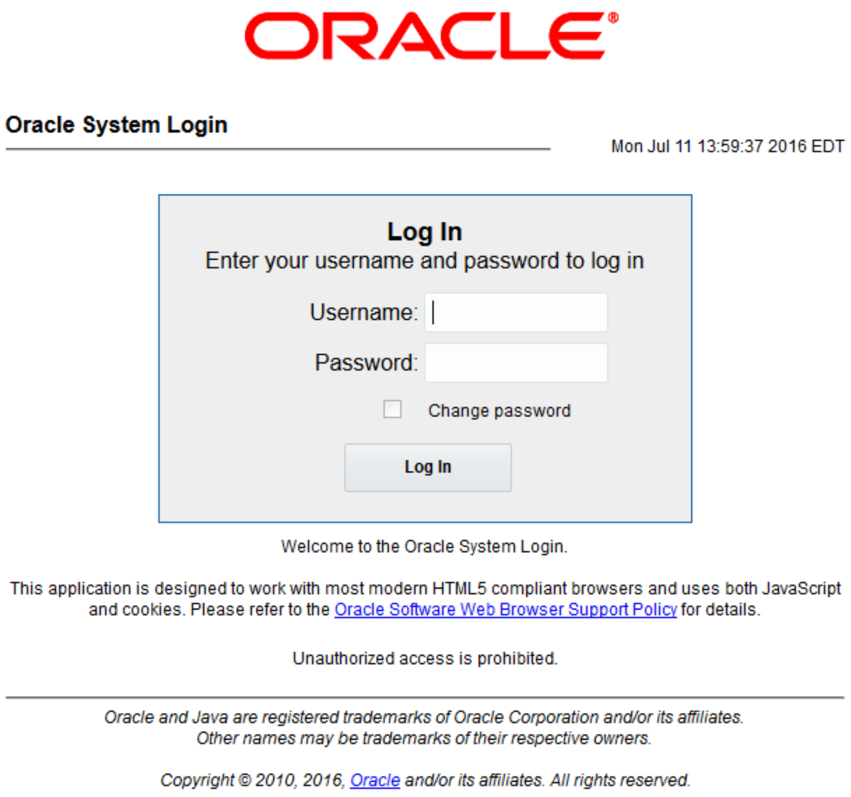
Procedure 100. Growth: MP (For 7.x to 8.x Upgraded System)

<table>
<tr>
<td>2.
☐</td>
<td>NOAM VIP GUI:
Login</td>
<td>

1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:

```
https://<Primary_NOAM_XMI_VIP_IP_Address>
```

2. Login as the **guiadmin** user.



Oracle System Login

Mon Jul 11 13:59:37 2016 EDT

Log In

Enter your username and password to log in

Username:

Password:

☐ Change password

Log In

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

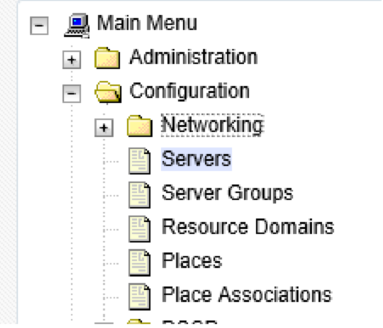
Unauthorized access is prohibited.

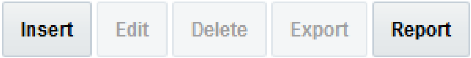
Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

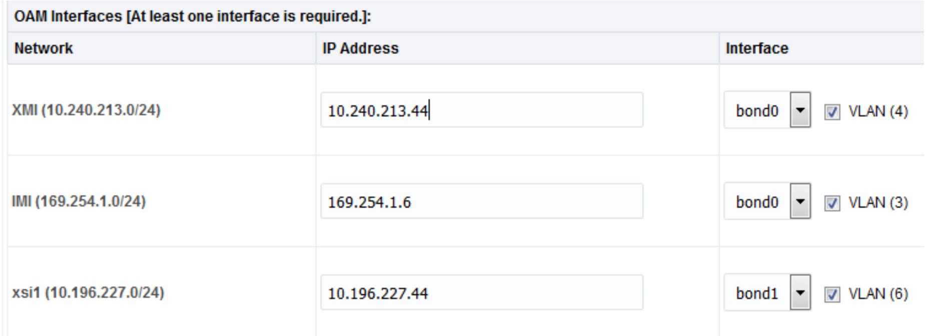
Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.

</td>
</tr>
</table>

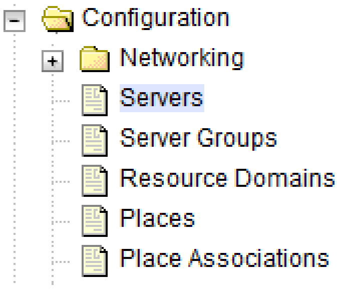
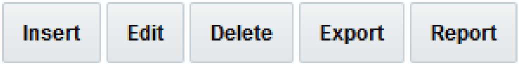
Procedure 100. Growth: MP (For 7.x to 8.x Upgraded System)

<table>
<tr>
<td>3.
☐</td>
<td>**NOAM VIP GUI**: Insert the MP server</td>
<td>
1. Navigate to **Configuration > Servers**.

Main Menu
Administration
Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Click **Insert** to insert the new MP server into servers table.

Insert
Edit
Delete
Export
Report

3. Enter these values:
<table>
<tr><td>**Hostname**:</td><td><Hostname></td></tr>
<tr><td>**Role**:</td><td>MP</td></tr>
<tr><td>**Network Element**:</td><td>[Choose Network Element]</td></tr>
<tr><td>**Hardware Profile**:</td><td>DSR TVOE Guest</td></tr>
<tr><td>**Location**:</td><td><Enter an optional location description></td></tr>
</table>
4. For the **XMI** network, type the MP's XMI IP address and select the **xmi** interface.
5. For the **IMI** network, type the MP's IMI IP address and select the **imi** interface.

OAM Interfaces [At least one interface is required.]:
<table>
<tr><th>Network</th><th>IP Address</th><th>Interface</th></tr>
<tr><td>XMI (10.240.213.0/24)</td><td>10.240.213.44</td><td>bond0 ☑ VLAN (4)</td></tr>
<tr><td>IMI (169.254.1.0/24)</td><td>169.254.1.6</td><td>bond0 ☑ VLAN (3)</td></tr>
<tr><td>xsi1 (10.196.227.0/24)</td><td>10.196.227.44</td><td>bond1 ☑ VLAN (6)</td></tr>
</table>
6. Add the NTP server.
<table>
<tr><th>NTP Server</th><th>Preferred?</th></tr>
<tr><td><MP_RMS_TVOE_IP_Address></td><td>Yes</td></tr>
</table>
7. Click **OK** when all fields are entered to finish MP server insertion.
</td>
</tr>
</table>

Procedure 100. Growth: MP (For 7.x to 8.x Upgraded System)

4. ☐	**NOAM VIP GUI**: Export the configuration	1. Navigate to **Configuration > Servers**.  Configuration Networking Servers Server Groups Resource Domains Places Place Associations 2. From the GUI screen, select the MP server and click **Export** to generate the initial configuration data for that server.  Insert Edit Delete Export Report
5. ☐	**NOAM VIP**: Copy the configuration file to MP server	1. Obtain a terminal session to the NOAM VIP as the **admusr** user. 2. 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 has a filename like **TKLCConfigData.<hostname>.sh**. `$ sudo awpushcfg` The awpushcfg utility is interactive, so the user is asked 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 3.

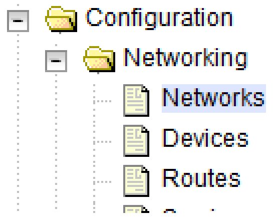
Procedure 100. Growth: MP (For 7.x to 8.x Upgraded System)

6.
☐
	MP Server: Verify awpushcfg was called and reboot the configured server	1. Obtain a terminal session to the MP server console by establishing an ssh session from the NOAM VIP terminal console.
		`$ ssh admusr@<MP_Control_IP>`
		2. Login as **admusr**.
		3. Verify awpushcfg was called by checking the log file.
		`$ sudo cat /var/TKLC/appw/logs/Process/install.log`
		Verify this message displays:
		`[SUCCESS] script completed successfully!`
		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.
		4. Reboot the server.
		`$ sudo init 6`
		5. Proceed to the next step once the server finishes rebooting. The server is done rebooting once the login prompt is displayed.

7. ☐	**MP Server**: Verify server health	Login as **admusr** to the MP server and make sure no errors are returned.

```
$ 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
```

Procedure 100. Growth: MP (For 7.x to 8.x Upgraded System)

8. ☐	**MP Server**: Delete auto-configured default route on MP and replace it with a network route via the XMI network — Part 1 (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 means a default route is not configurable on this MP and you have to create separate network routes for each signaling network destination. 1. Log into the site's PMAC and SSH to the MP's control address. Alternatively, log into the TVOE host and access the MP using the **virsh console <MP VM>**. 2. Determine <XMI_Gateway_IP> from your SO site network element information. 3. Gather this information: - <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 **Configuration > Networking > Networks** screen.  Configuration Networking Networks Devices Routes

Procedure 100. Growth: MP (For 7.x to 8.x Upgraded System)

9. ☐ **MP Server**: Delete auto-configured default route on MP and replace it with a network route via the XMI network — Part 2 (optional)

1. Establish a connection to the MP server and login as **admusr**.
2. 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.

```
$ 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>
```

3. Create network routes to the DR NO’s XMI (OAM) network.

```
$ 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>
```

4. Create network routes to the management server TVOE XMI (OAM) network for NTP.

```
$ sudo /usr/TKLC/plat/bin/netAdm add -route=net
--address=<TVOE_Mgmt_Network_Address>
--netmask=<TVOE_Mgmt_Network_Netmask>
--gateway=<MP_XMI_Gateway_IP_Address> --
device=<MP_XMI_Interface>
```

5. (Optional) If sending SNMP traps from individual servers, create host routes to customer SNMP trap destinations on the XMI network.

```
$ sudo /usr/TKLC/plat/bin/netAdm add -route=host
--address=<Customer_NMS_IP> --
gateway=<MP_XMI_Gateway_IP_Address>
--device=<MP_XMI_Interface>
```

6. Repeat for any existing customer NMS stations.
7. Delete the existing default route:
   a. Log into primary NOAM VIP GUI.
   b. Navigate to **Configuration > Networking > Networks**.
   c. Select the respective SOAM tab.
   d. Select the XMI network and click **Unlock**. Click **OK** to confirm.
   e. Navigate to **Configuration > Networking > Routes**.
   f. Select the XMI route and click **Delete**.
   g. Click **OK** to confirm.
   h. Repeat steps 1 through 7 for all required MPs to delete the XMI routes.
   i. Navigate to **Configuration > Networking > Networks**.
   j. Select the respective SOAM tab.
   k. Select the XMI network and click **Lock**.
   l. Click **OK** to confirm.

Procedure 100. Growth: MP (For 7.x to 8.x Upgraded System)

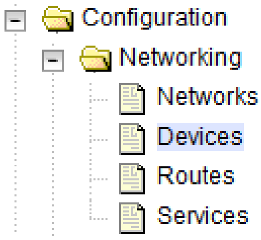
10.
☐
	MP Server: Verify connectivity	1. Establish a connection to the MP server and login as **admusr**.
		2. Ping active NO XMI IP address to verify connectivity.
		`$ ping <ACTIVE_NO_XMI_IP_Address>`
		`PING 10.240.108.6 (10.240.108.6) 56(84) bytes of data.`
		`64 bytes from 10.240.108.6: icmp_seq=1 ttl=64 time=0.342 ms`
		`64 bytes from 10.240.108.6: icmp_seq=2 ttl=64 time=0.247 ms`
		3. (Optional) Ping Customer NMS Station(s).
		`$ ping <Customer_NMS_IP>`
		`PING 172.4.116.8 (172.4.118.8) 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`
		4. If you do not get a response, then verify your network configuration. If you continue to get failures, then stop the installation and contact Oracle customer support.

11. ☐	Repeat for remaining MPs at all sites	Repeat this entire procedure for all remaining MPs (SS7-MP, DA-MP, SBR, and IPFE).
12. ☐	**Configure MP**	Execute these procedures: 1. Procedure 30 Configure Places and Assign MP Servers to Places (PCA and DCA Only) 2. Procedure 31 Configure DAMP Server Groups and Profiles
Steps (13. through 16.) configure the signaling interfaces for the newly added MPs.		

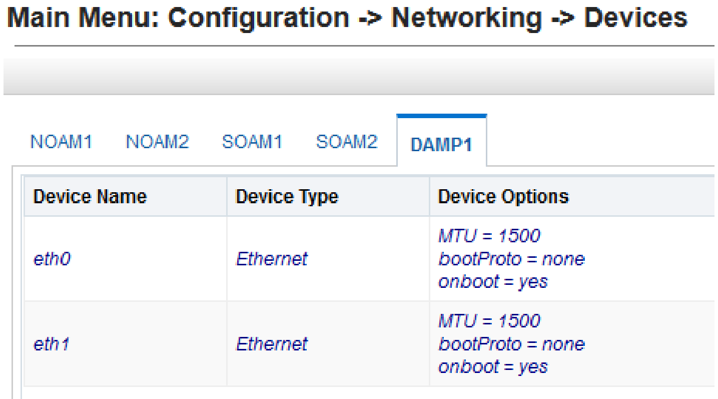
13.
☐
	Newly Created MP Server Console: Manually configure signaling interface	1. Log into iLO/iLOM and follow Appendix D TVOE iLO/iLOM GUI Access to access the iLO/iLOM GUI.
		`https://<management_server_iLO_ip>`
		2. Log into the newly added MP console.
		3. Execute this command to configure the signaling interfaces.
		`$ sudo /usr/TKLC/plat/bin/netAdm add --onboot=yes --netmask=<netmask> --device=xsi1 --address=<IP address>`
		`Interface xsi1 added.`
		4. Repeat to configure the required number of signaling interfaces.
		5. Reboot the VM.
		`$ sudo init 6`
		It takes approximately five minutes for the VM to complete rebooting.

Procedure 100. Growth: MP (For 7.x to 8.x Upgraded System)

<table>
<tr><td>14.
☐</td><td>**NOAM VIP GUI**: Take ownership of the signaling interfaces and make it deployed</td><td>
1. Navigate to **Configuration > Network > Devices**.

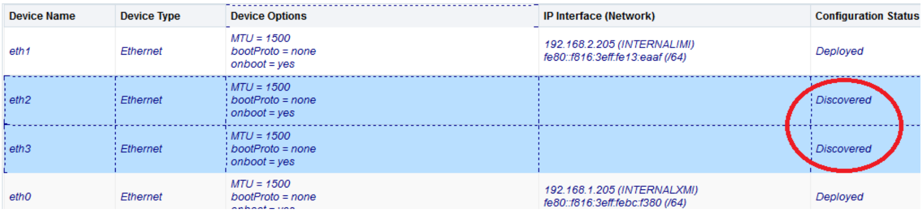

Configuration
Networking
Networks
Devices
Routes
Services

2. Click on the tab representing the newly added MP blade.


Main Menu: Configuration -> Networking -> Devices
NOAM1
NOAM2
SOAM1
SOAM2
DAMP1

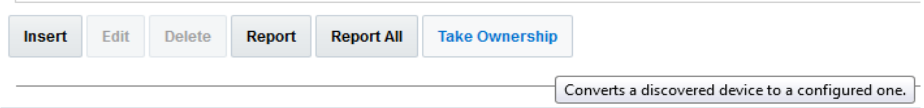
<table>
<tr><th>Device Name</th><th>Device Type</th><th>Device Options</th></tr>
<tr><td>eth0</td><td>Ethernet</td><td>MTU = 1500
bootProto = none
onboot = yes</td></tr>
<tr><td>eth1</td><td>Ethernet</td><td>MTU = 1500
bootProto = none
onboot = yes</td></tr>
</table>

3. Select all newly configured signaling ethernet devices that have **Discovered** as their Configuration Status.



<table>
<tr><th>Device Name</th><th>Device Type</th><th>Device Options</th><th>IP Interface (Network)</th><th>Configuration Status</th></tr>
<tr><td>eth1</td><td>Ethernet</td><td>MTU = 1500
bootProto = none
onboot = yes</td><td>192.168.2.205 (INTERNALIMI)
fe80::f816:3eff:fe13:eaaf (/64)</td><td>Deployed</td></tr>
<tr><td>eth2</td><td>Ethernet</td><td>MTU = 1500
bootProto = none
onboot = yes</td><td></td><td>Discovered</td></tr>
<tr><td>eth3</td><td>Ethernet</td><td>MTU = 1500
bootProto = none
onboot = yes</td><td></td><td>Discovered</td></tr>
<tr><td>eth0</td><td>Ethernet</td><td>MTU = 1500
bootProto = none</td><td>192.168.1.205 (INTERNALXMI)
fe80::f816:3eff:febc:f380 (/64)</td><td>Deployed</td></tr>
</table>

4. Click **Take Ownership**.

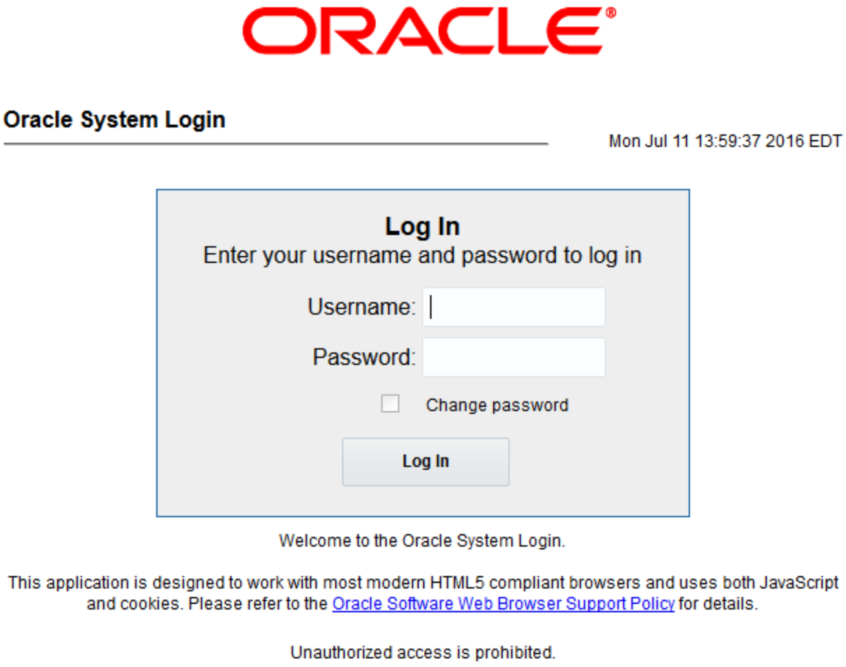

Insert
Edit
Delete
Report
Report All
Take Ownership
Converts a discovered device to a configured one.

The selected devices change their Configuration Status to **Configured**.
</td></tr>
<tr><td>15.
☐</td><td>Repeat for remaining MPs and IPFEs</td><td>Repeat steps 13. through 14. for any newly created remaining MP servers.</td></tr>
<tr><td>16.
☐</td><td>Configure ComAgent connection</td><td>Execute section 3.17.2 Configure ComAgent Connections (DSR and SDS Only).</td></tr>
</table>

Procedure 101. Growth: Query Server (SDS Only)

This procedure configures 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**SDS NOAM VIP GUI**: Configure the query server	Configure the query server by executing section 3.15.4 Query Server Configuration.

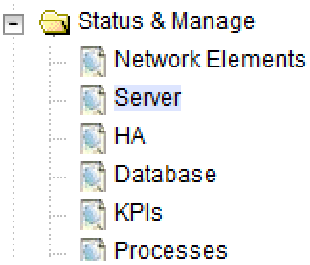
Procedure 102. Post Growth Health Check

This procedure verifies system status and logs all alarms after 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  ORACLE® **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.

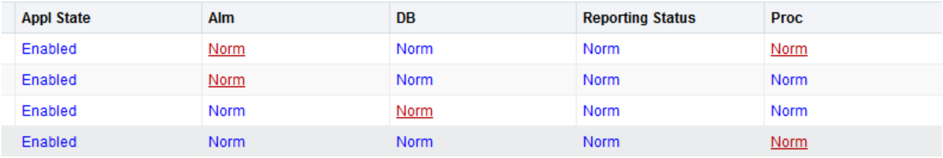
Procedure 102. Post Growth Health Check

<table>
<tr>
<td>2.
☐</td>
<td>NOAM VIP GUI: Verify server status</td>
<td>

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


Status & Manage
Network Elements
Server
HA
Database
KPIs
Processes

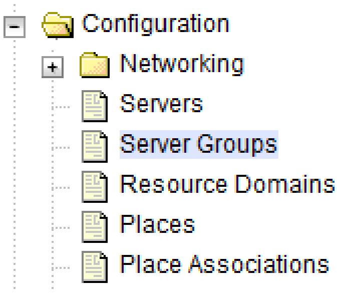
2. Verify all server status is Normal (Norm) for Alarm (Alm), Database (DB), Replication Status, and Processes (Proc).



<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>

</td>
</tr>
<tr>
<td>3.
☐</td>
<td>NOAM VIP GUI: Verify server configuration</td>
<td>

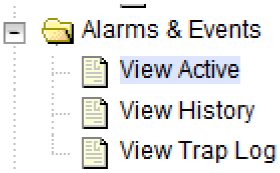
1. Navigate to **Configuration > Server Groups**.


Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

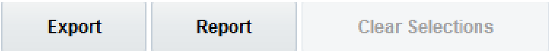
2. Verify the configuration data is correct for your network.

</td>
</tr>
<tr>
<td>4.
☐</td>
<td>NOAM VIP GUI: Log current alarms</td>
<td>

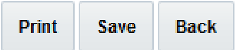
1. Navigate to **Alarms & Events > View Active**.


Alarms & Events
View Active
View History
View Trap Log

2. Click **Report**.


Export
Report
Clear Selections

3. **Save** or **Print** this report and keep copies for future reference.


Print
Save
Back

4. Compare this alarm report with those gathered in Procedure 95 Perform Health Check.

</td>
</tr>
<tr>
<td>5.
☐</td>
<td>SOAM VIP GUI: Repeat</td>
<td>Repeat steps 1. through 3. for the SOAM.</td>
</tr>
</table>

Procedure 103. Post Growth Backups

This procedure backs up 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	Backup TVOE	Back up all TVOE host configurations by executing section 3.17.6 Back Up TVOE Configuration.
2. ☐	Backup PMAC	Back up the PMAC application by executing section 3.17.7 Back Up PMAC Application.
3. ☐	Backup NOAM/SOAM databases	Back up the NOAM and SOAM databases by executing sections 3.17.8 Back Up NOAM Database and 3.17.9 Back Up SOAM Database. ***Note:*** Database backup on SDS SOAMs is not required.

Appendix P.2 De-Growth (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 (10Gbps) Only)

For de-growth scenarios where it is necessary to remove/delete DSR/SDS MP (IPFE, SBR, SS7-MP) servers, follow these procedures.

Step	Procedure(s)
Perform backups	Procedure 104 Perform Backups
Perform system health check	Procedure 105 Perform Health Check
Identify servers affected by de-growth: DSR MP (IPFE, SBR, SS7-MP)/SDS DP	
Remove identified servers from server group	Procedure 106 Remove Server from Server Group and Procedure 107 Delete Server/Server Group
Shut down and remove the identified server’s VM	Procedure 108 Delete Server VM
Post de-growth health check	Procedure 109 Post De-Growth Health Check
Post de-growth backups	Procedure 110 Post De-Growth Backups

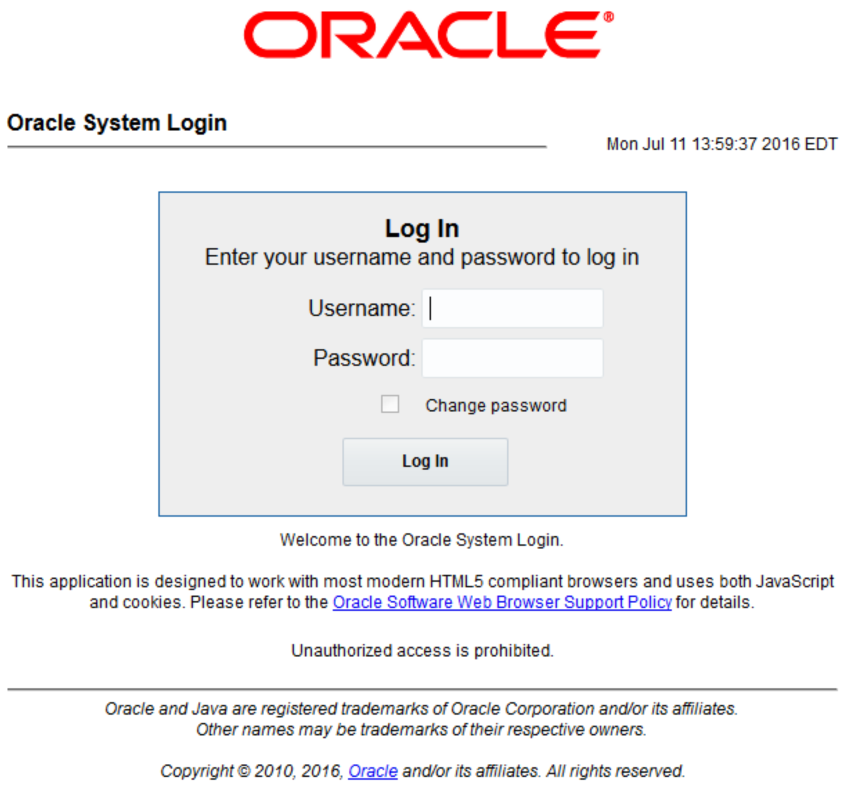
Procedure 104. Perform Backups

This procedure backs up all necessary items before 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	Backup TVOE	Back up all TVOE host configurations by executing section 3.17.6 Back Up TVOE Configuration.
2. ☐	Backup PMAC	Back up the PMAC application by executing section 3.17.7 Back Up PMAC Application.

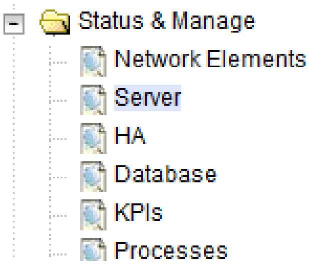
Procedure 104. Perform Backups

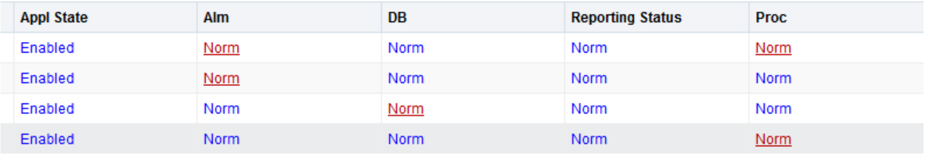
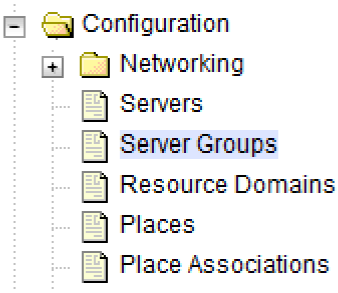
3. ☐	Backup NOAM/SOAM databases	Back up the NOAM and SOAM databases by executing sections 3.17.8 Back Up NOAM Database and 3.17.9 Back Up SOAM Database. ***Note:*** Database backup on SDS SOAMs is not required.

Procedure 105. Perform Health Check

<table>
<tr><td colspan="3">This procedure verifies system status and logs 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 My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>NOAM VIP GUI: Login</td><td>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:
<code>https://<Primary_NOAM_VIP_IP_Address></code>
2. Login as the guiadmin user.

Oracle System Login
Mon Jul 11 13:59:37 2016 EDT
Log In
Enter your username and password to log in
Username:
Password:
☐ Change password
Log In
Welcome to the Oracle System Login.
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.
Unauthorized access is prohibited.
Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.</td></tr>
</table>

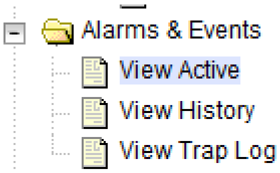
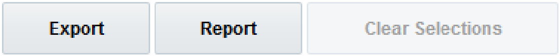
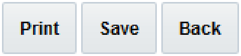
Procedure 105. Perform Health Check

<table>
<tr>
<td>2.
☐</td>
<td>NOAM VIP GUI: Verify server status</td>
<td>
1. Navigate to Status & Manage > Server.

Status & Manage
Network Elements
Server
HA
Database
KPIs
Processes

2. 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
</td>
</tr>
<tr>
<td>3.
☐</td>
<td>NOAM VIP GUI: Verify server configuration</td>
<td>
1. Navigate to Configuration > Server Groups.

Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Verify the configuration data is correct for your network.
</td>
</tr>
</table>

Procedure 105. Perform Health Check

4. ☐	**NOAM VIP GUI**: Log current alarms	1. Navigate to **Alarms & Events > View Active**.  Alarms & Events View Active View History View Trap Log 2. Click Report.  Export Report Clear Selections 3. **Save** or **Print** this report and keep copies for future reference.  Print Save Back
5. ☐	**SOAM VIP GUI**: Repeat for SOAM	Repeat this procedure for the SOAM.

Procedure 106. Remove Server from Server Group

Once the server that will be deleted has been identified, the server first needs to be removed from its server group.

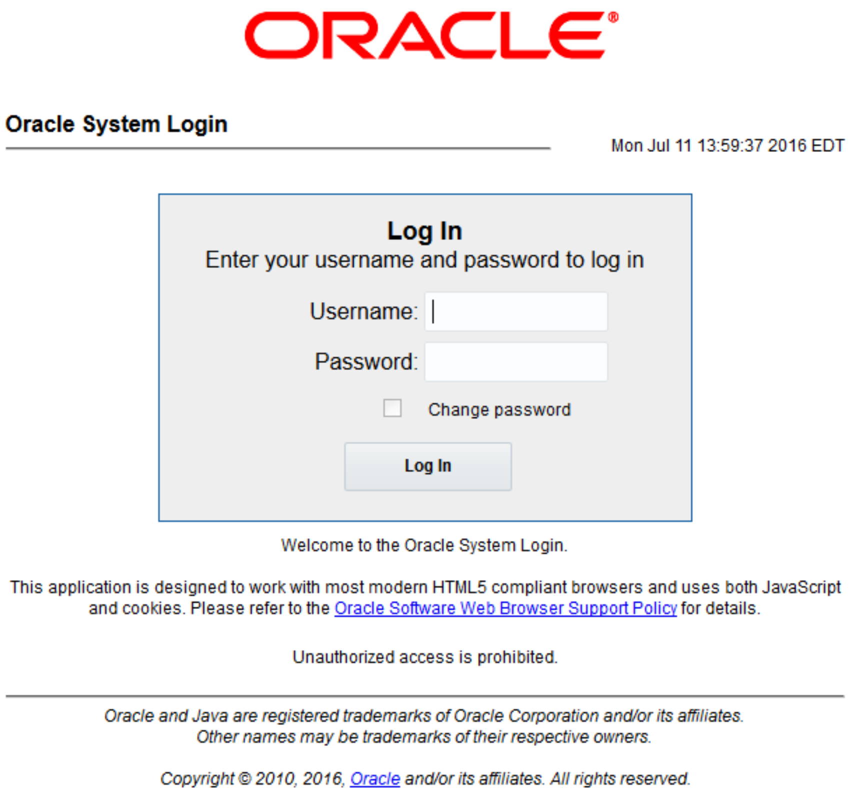
This procedure removes a server from a server group.

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.

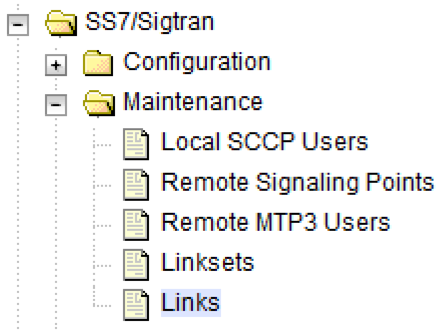
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**SOAM VIP GUI**: Login	Execute this step if removing SS7-MP, otherwise skip to step 10. 1. 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>` 2. Login as the **guiadmin** user.  **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details. Unauthorized access is prohibited. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*

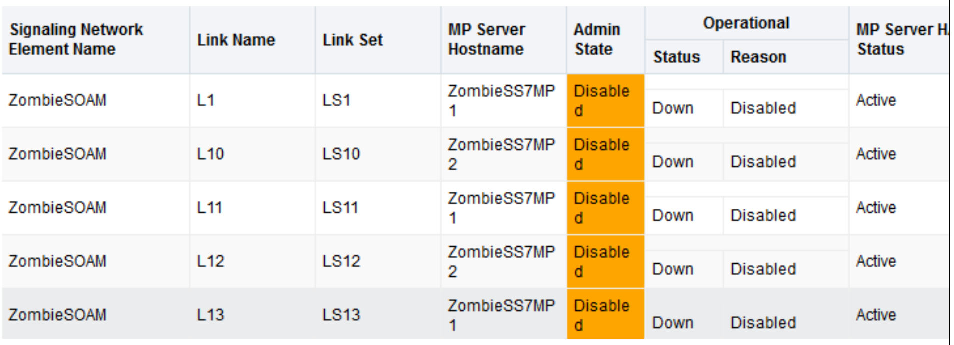
Procedure 106. Remove Server from Server Group

<table>
<tr>
<td>2.
☐</td>
<td>SOAM VIP GUI: Disable SS7-MP links</td>
<td>
Execute this step if removing SS7-MP, otherwise skip to step 10.

1. Navigate to **SS7/Sigtran > Maintenance > Links**.

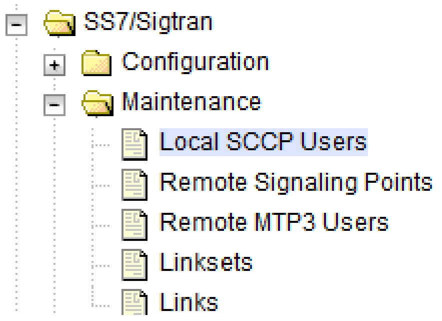

SS7/Sigtran
Configuration
Maintenance
Local SCCP Users
Remote Signaling Points
Remote MTP3 Users
Linksets
Links

2. Disable the associated links of the identified SS7-MP.

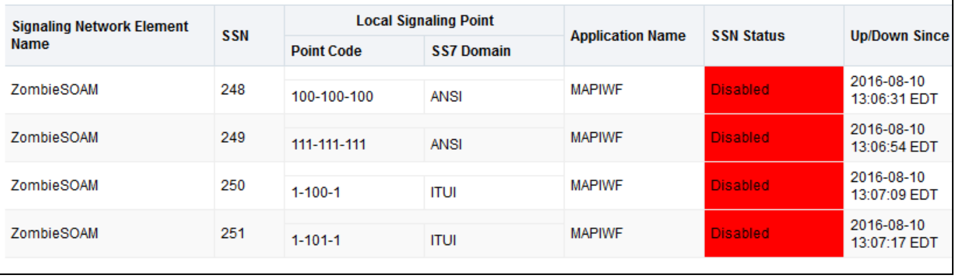


<table>
<tr><th rowspan="2">Signaling Network Element Name</th><th rowspan="2">Link Name</th><th rowspan="2">Link Set</th><th rowspan="2">MP Server Hostname</th><th rowspan="2">Admin State</th><th colspan="2">Operational</th><th rowspan="2">MP Server H Status</th></tr>
<tr><th>Status</th><th>Reason</th></tr>
<tr><td>ZombieSOAM</td><td>L1</td><td>LS1</td><td>ZombieSS7MP1</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>ZombieSS7MP2</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>ZombieSS7MP1</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>ZombieSS7MP2</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>ZombieSS7MP1</td><td>Disabled</td><td>Down</td><td>Disabled</td><td>Active</td></tr>
</table>
</td>
</tr>
<tr>
<td>3.
☐</td>
<td>SOAM VIP GUI: Disable SS7-MP SCCP users</td>
<td>
Execute this step if removing SS7-MP, otherwise skip to step 10.

1. Navigate to **SS7/Sigtran > Maintenance > Local SCCP Users**.

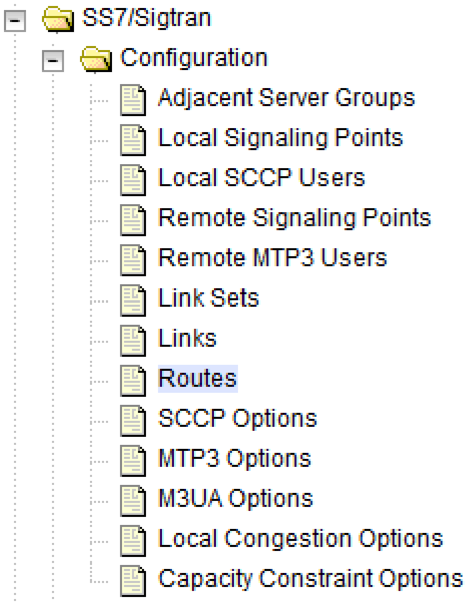

SS7/Sigtran
Configuration
Maintenance
Local SCCP Users
Remote Signaling Points
Remote MTP3 Users
Linksets
Links

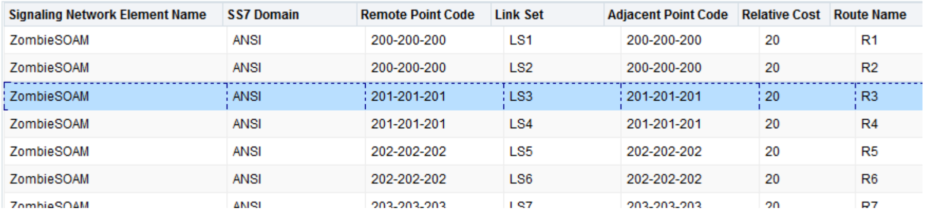
2. Disable the associated local SCCP users of the identified SS7-MP.



<table>
<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><th rowspan="2">SSN Status</th><th rowspan="2">Up/Down Since</th></tr>
<tr><th>Point Code</th><th>SS7 Domain</th></tr>
<tr><td>ZombieSOAM</td><td>248</td><td>100-100-100</td><td>ANSI</td><td>MAPIWF</td><td>Disabled</td><td>2016-08-10 13:06:31 EDT</td></tr>
<tr><td>ZombieSOAM</td><td>249</td><td>111-111-111</td><td>ANSI</td><td>MAPIWF</td><td>Disabled</td><td>2016-08-10 13:06:54 EDT</td></tr>
<tr><td>ZombieSOAM</td><td>250</td><td>1-100-1</td><td>ITUI</td><td>MAPIWF</td><td>Disabled</td><td>2016-08-10 13:07:09 EDT</td></tr>
<tr><td>ZombieSOAM</td><td>251</td><td>1-101-1</td><td>ITUI</td><td>MAPIWF</td><td>Disabled</td><td>2016-08-10 13:07:17 EDT</td></tr>
</table>
</td>
</tr>
</table>

Procedure 106. Remove Server from Server Group

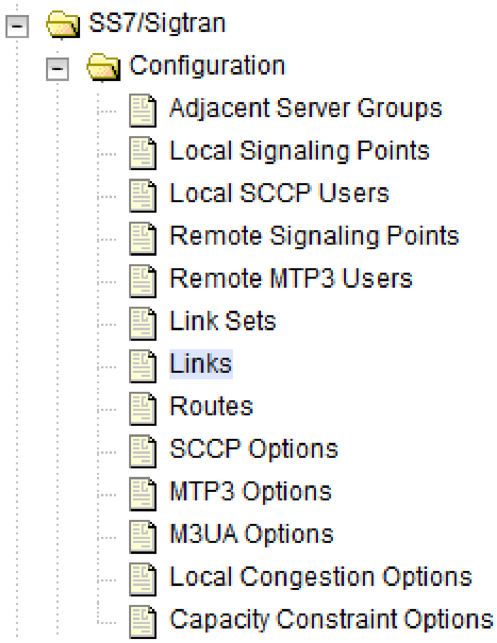
<table>
<tr>
<td>4.
☐</td>
<td>SOAM VIP GUI:
Delete SS7-MP routes</td>
<td>
Execute this step if removing SS7-MP, otherwise skip to step 10.
1. Navigate to SS7/Sigtran > Configuration > Routes.

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

2. Delete the associated routes of the identified SS7-MP.

<table>
<tr><th>Signaling Network Element Name</th><th>SS7 Domain</th><th>Remote Point Code</th><th>Link Set</th><th>Adjacent Point Code</th><th>Relative Cost</th><th>Route Name</th></tr>
<tr><td>ZombieSOAM</td><td>ANSI</td><td>200-200-200</td><td>LS1</td><td>200-200-200</td><td>20</td><td>R1</td></tr>
<tr><td>ZombieSOAM</td><td>ANSI</td><td>200-200-200</td><td>LS2</td><td>200-200-200</td><td>20</td><td>R2</td></tr>
<tr><td>ZombieSOAM</td><td>ANSI</td><td>201-201-201</td><td>LS3</td><td>201-201-201</td><td>20</td><td>R3</td></tr>
<tr><td>ZombieSOAM</td><td>ANSI</td><td>201-201-201</td><td>LS4</td><td>201-201-201</td><td>20</td><td>R4</td></tr>
<tr><td>ZombieSOAM</td><td>ANSI</td><td>202-202-202</td><td>LS5</td><td>202-202-202</td><td>20</td><td>R5</td></tr>
<tr><td>ZombieSOAM</td><td>ANSI</td><td>202-202-202</td><td>LS6</td><td>202-202-202</td><td>20</td><td>R6</td></tr>
<tr><td>ZombieSOAM</td><td>ANSI</td><td>203-203-203</td><td>LS7</td><td>203-203-203</td><td>20</td><td>R7</td></tr>
</table>
</td>
</tr>
</table>

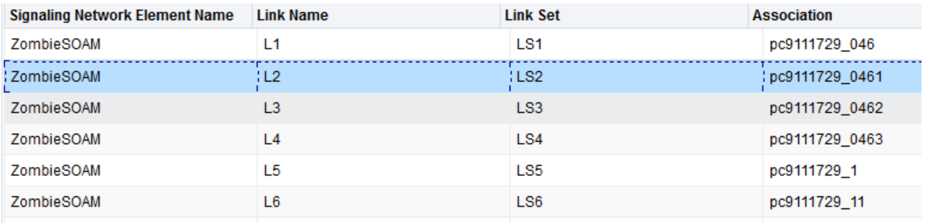
Procedure 106. Remove Server from Server Group

<table>
<tr>
<td>5.
☐</td>
<td>SOAM VIP GUI: Delete SS7-MP links</td>
<td>
Execute this step if removing SS7-MP, otherwise skip to step 10.

1. Navigate to **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

2. Delete the associated links of the identified SS7-MP.

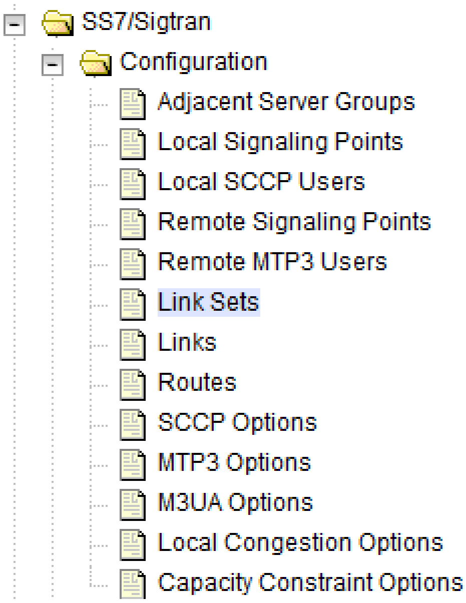


<table>
<tr><th>Signaling Network Element Name</th><th>Link Name</th><th>Link Set</th><th>Association</th></tr>
<tr><td>ZombieSOAM</td><td>L1</td><td>LS1</td><td>pc9111729_046</td></tr>
<tr><td>ZombieSOAM</td><td>L2</td><td>LS2</td><td>pc9111729_0461</td></tr>
<tr><td>ZombieSOAM</td><td>L3</td><td>LS3</td><td>pc9111729_0462</td></tr>
<tr><td>ZombieSOAM</td><td>L4</td><td>LS4</td><td>pc9111729_0463</td></tr>
<tr><td>ZombieSOAM</td><td>L5</td><td>LS5</td><td>pc9111729_1</td></tr>
<tr><td>ZombieSOAM</td><td>L6</td><td>LS6</td><td>pc9111729_11</td></tr>
</table>
</td>
</tr>
</table>

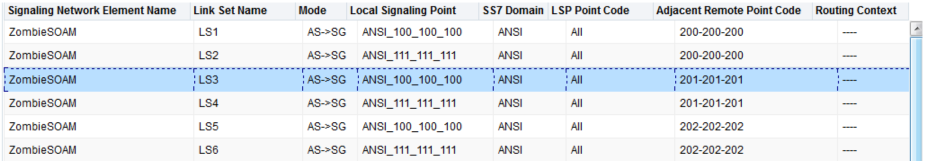
Procedure 106. Remove Server from Server Group

<table>
<tr>
<td>6.
☐</td>
<td>SOAM VIP GUI: Delete SS7-MP link sets</td>
<td>
Execute this step if removing SS7-MP, otherwise skip to step 10.

1. Navigate to **SS7/Sigtran > Configuration > Link Sets**.

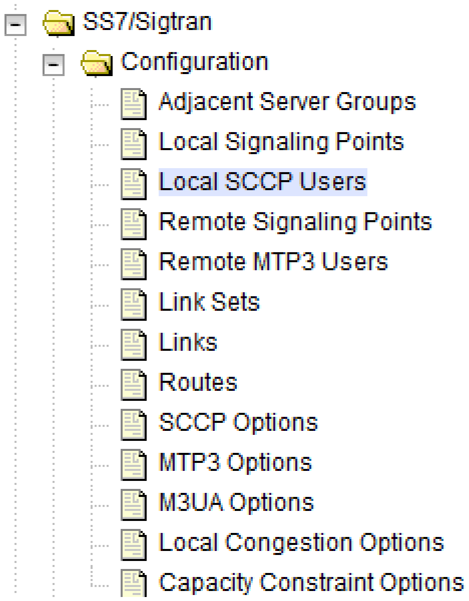

SS7/Sigtran
Configuration
Adjacent Server Groups
Local Signaling Points
Local SCCP Users
Remote Signaling Points
Remote MTP3 Users
Link Sets
Links
Routes
SCCP Options
MTP3 Options
M3UA Options
Local Congestion Options
Capacity Constraint Options

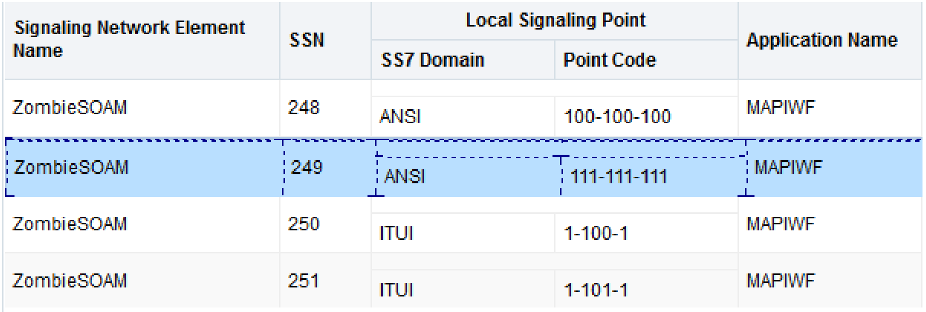
2. Delete the associated link sets of the identified SS7-MP.



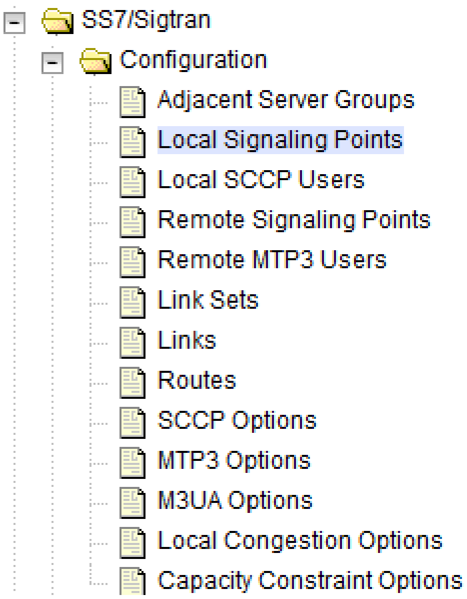
<table>
<tr><th>Signaling Network Element Name</th><th>Link Set Name</th><th>Mode</th><th>Local Signaling Point</th><th>SS7 Domain</th><th>LSP Point Code</th><th>Adjacent Remote Point Code</th><th>Routing Context</th></tr>
<tr><td>ZombieSOAM</td><td>LS1</td><td>AS->SG</td><td>ANSI_100_100_100</td><td>ANSI</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>
</table>
</td>
</tr>
</table>

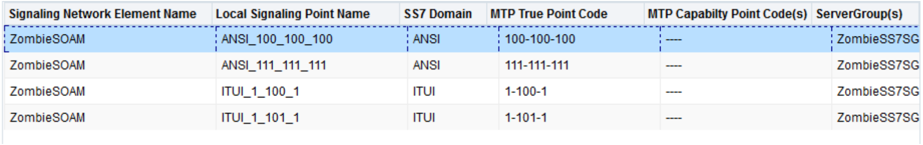
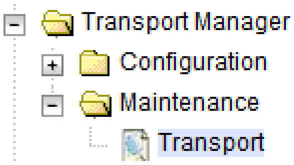
Procedure 106. Remove Server from Server Group

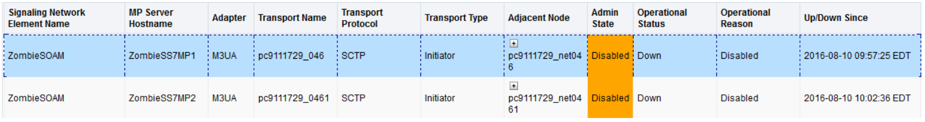
<table>
<tr>
<td>7.
☐</td>
<td>SOAM VIP GUI: Delete SS7-MP local SCCP users</td>
<td>
Execute this step if removing SS7-MP, otherwise skip to step 10.
1. Navigate to SS7/Sigtran > Configuration > Local SCCP Users.

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

2. Delete the associated Local SCCP Users from the identified SS7-MP.

<table>
<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>
<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>
</table>
</td>
</tr>
</table>

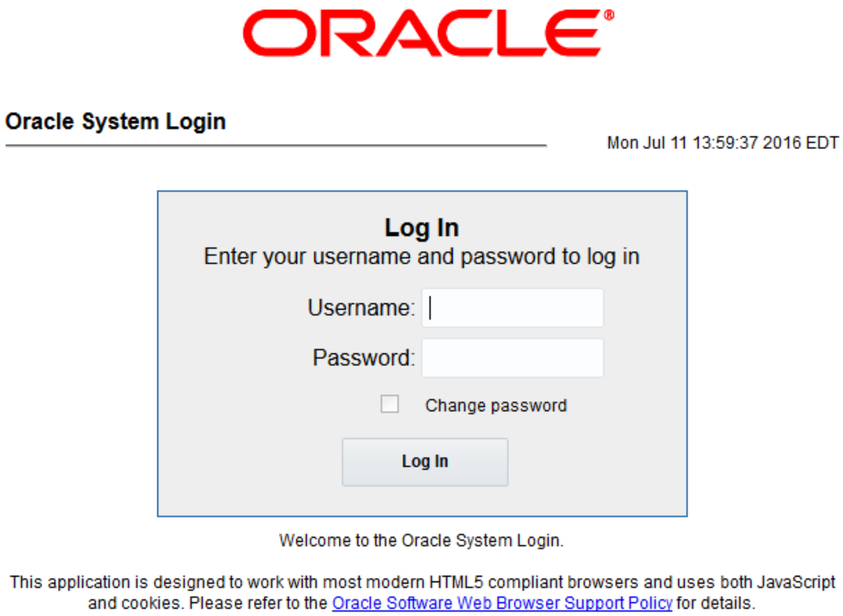
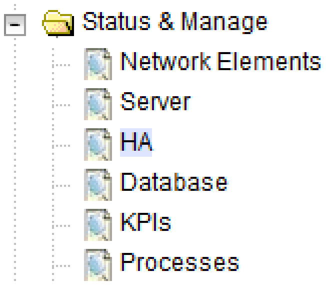
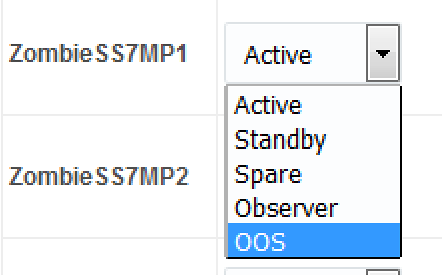
Procedure 106. Remove Server from Server Group

<table>
<tr>
<td>8.
☐</td>
<td>SOAM VIP GUI: Delete SS7-MP local signaling points</td>
<td>
Execute this step if removing SS7-MP, otherwise skip to step 10.
1. Navigate to 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

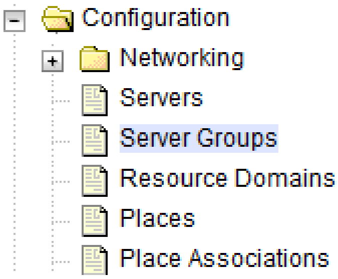
2. Delete the associated Local signaling points from the identified SS7-MP.

<table>
<tr><th>Signaling Network Element Name</th><th>Local Signaling Point Name</th><th>SS7 Domain</th><th>MTP True Point Code</th><th>MTP Capabilty Point Code(s)</th><th>ServerGroup(s)</th></tr>
<tr><td>ZombieSOAM</td><td>ANSI_100_100_100</td><td>ANSI</td><td>100-100-100</td><td>----</td><td>ZombieSS7SG</td></tr>
<tr><td>ZombieSOAM</td><td>ANSI_111_111_111</td><td>ANSI</td><td>111-111-111</td><td>----</td><td>ZombieSS7SG</td></tr>
<tr><td>ZombieSOAM</td><td>ITUI_1_100_1</td><td>ITUI</td><td>1-100-1</td><td>----</td><td>ZombieSS7SG</td></tr>
<tr><td>ZombieSOAM</td><td>ITUI_1_101_1</td><td>ITUI</td><td>1-101-1</td><td>----</td><td>ZombieSS7SG</td></tr>
</table>
</td>
</tr>
<tr>
<td>9.
☐</td>
<td>SOAM VIP GUI: Disable SS7-MP transports</td>
<td>
Execute this step if removing SS7-MP, otherwise skip to step 10.
1. Navigate to Transport Manager > Maintenance > Transport.

Transport Manager
Configuration
Maintenance
Transport

2. Disable the associated transports from the identified SS7-MP.

<table>
<tr><th>Signaling Network Element Name</th><th>MP Server Hostname</th><th>Adapter</th><th>Transport Name</th><th>Transport Protocol</th><th>Transport Type</th><th>Adjacent Node</th><th>Admin State</th><th>Operational Status</th><th>Operational Reason</th><th>Up/Down Since</th></tr>
<tr><td>ZombieSOAM</td><td>ZombieSS7MP1</td><td>M3UA</td><td>pc9111729_046</td><td>SCTP</td><td>Initiator</td><td>pc9111729_net046</td><td>Disabled</td><td>Down</td><td>Disabled</td><td>2016-08-10 09:57:25 EDT</td></tr>
<tr><td>ZombieSOAM</td><td>ZombieSS7MP2</td><td>M3UA</td><td>pc9111729_0461</td><td>SCTP</td><td>Initiator</td><td>pc9111729_net0461</td><td>Disabled</td><td>Down</td><td>Disabled</td><td>2016-08-10 10:02:36 EDT</td></tr>
</table>
</td>
</tr>
</table>

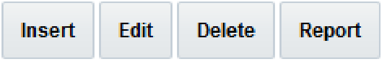
Procedure 106. Remove Server from Server Group

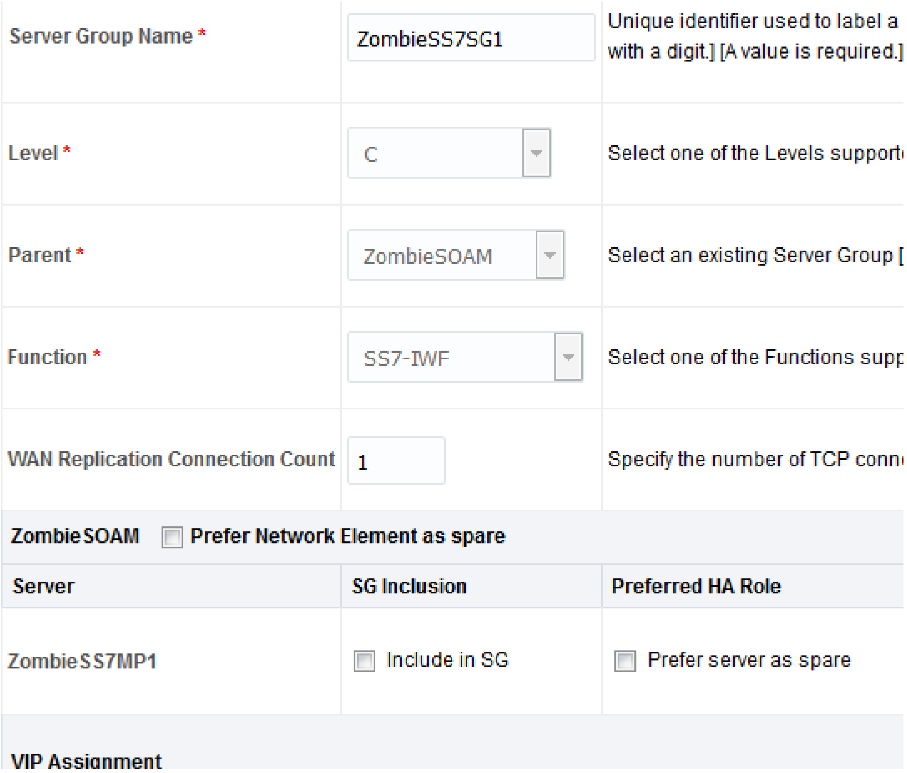
10. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user. Oracle System Login Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.
11. ☐	**NOAM VIP GUI**: Set server to OOS	1. Navigate to **Status & Manage > HA**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Click **Edit**. 3. Set the server's Max Allowed HA Role to **OOS**.  ZombieSS7MP1 Active Active Standby Spare Observer OOS ZombieSS7MP2 4. Click **OK**.

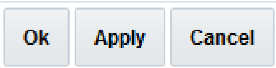
Procedure 106. Remove Server from Server Group

<table>
<tr><td>12.
☐</td><td>NOAM VIP GUI: Delete server from server group</td><td>
1. Navigate to Configuration > Server Groups.

Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Select the server group for which the server from step 2 that was placed OOS.

3. Click Edit.

Insert
Edit
Delete
Report

4. Unmark the Include in SG checkbox next to the server from step 2.

<table>
<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 Assignment</td></tr>
</table>

5. Click OK.

Ok
Apply
Cancel
</td></tr>
</table>

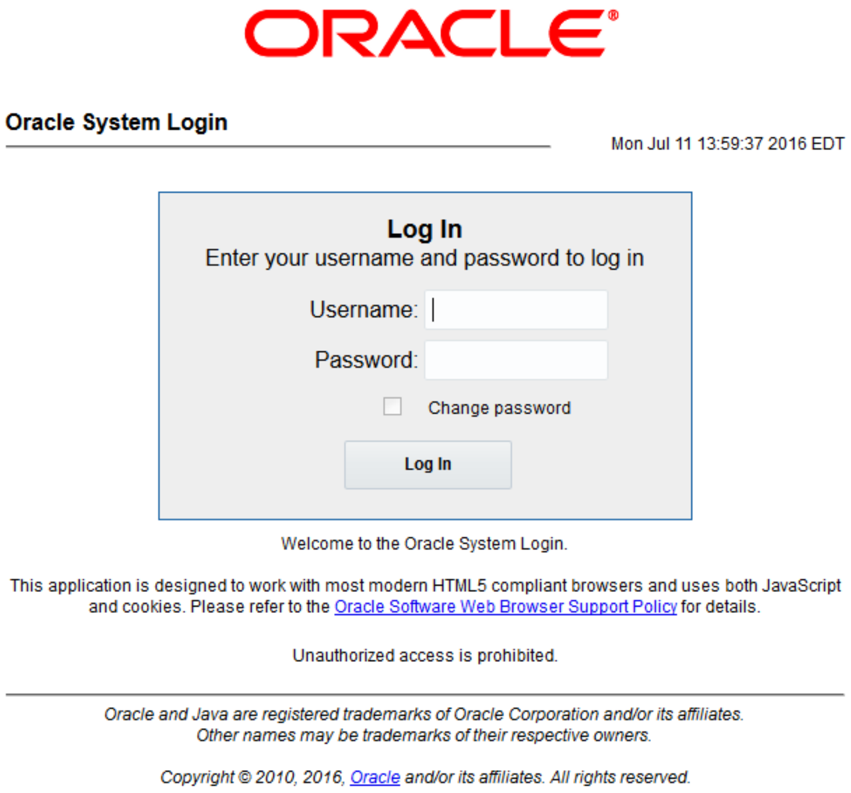
Procedure 107. Delete Server/Server Group

Once the server has been removed from the server group, it is safe to delete the server. The server group can also be deleted, if there are no more servers associated with it.

This procedure deletes a server and a server group.

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

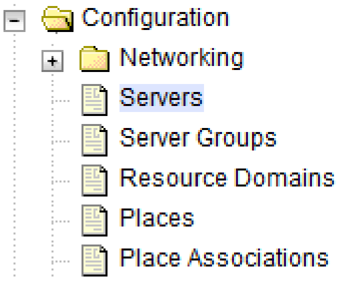
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  ORACLE® Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Username: Password: ☐ Change password Log In Enter your username and password to 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.*

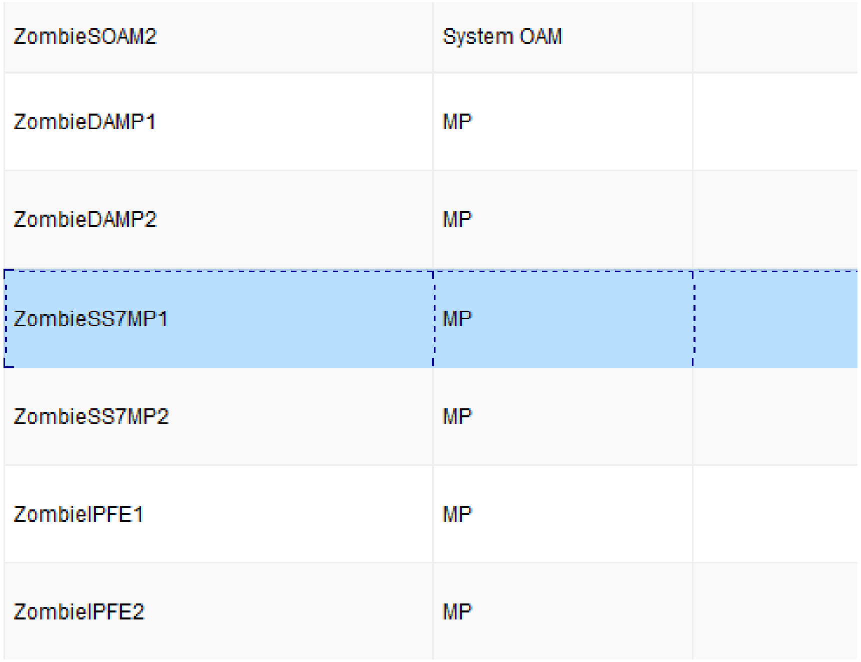
Procedure 107. Delete Server/Server Group

<table>
<tr>
<td>2.
☐</td>
<td>NOAM VIP GUI: Delete the server</td>
<td>

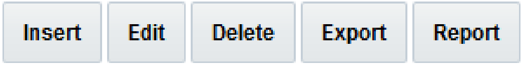
1. Navigate to **Configuration > Servers**.


Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

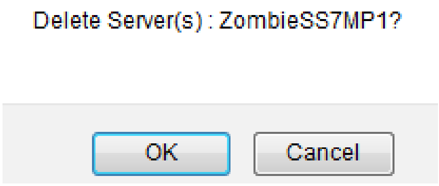
2. Select the server that has been previously removed from the server group and click **Delete**.



<table>
<tr><td>ZombieSOAM2</td><td>System OAM</td><td></td></tr>
<tr><td>ZombieDAMP1</td><td>MP</td><td></td></tr>
<tr><td>ZombieDAMP2</td><td>MP</td><td></td></tr>
<tr><td>ZombieSS7MP1</td><td>MP</td><td></td></tr>
<tr><td>ZombieSS7MP2</td><td>MP</td><td></td></tr>
<tr><td>ZombieIPFE1</td><td>MP</td><td></td></tr>
<tr><td>ZombieIPFE2</td><td>MP</td><td></td></tr>
</table>


Insert
Edit
Delete
Export
Report

3. Click **OK** to confirm.



Delete Server(s) : ZombieSS7MP1?

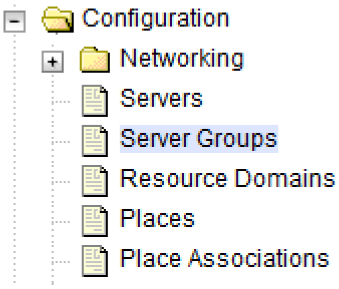
</td>
</tr>
</table>

Procedure 107. Delete Server/Server Group

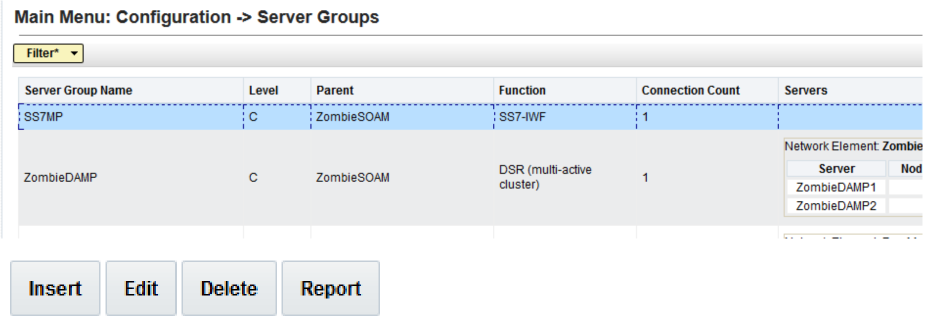
<table>
<tr>
<td>3.
☐</td>
<td>NOAM VIP GUI: Delete server group</td>
<td>

If all servers have been removed from a server group, it is now safe to delete the server group.

1. Navigate to **Configuration > Server Groups**.


Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Select the empty server group and click **Delete**.

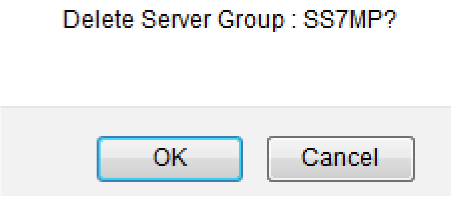


Main Menu: Configuration -> Server Groups

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 Server Nod ZombieDAMP1 ZombieDAMP2

Filter*
Insert
Edit
Delete
Report

3. Click **OK** to confirm.



Delete Server Group : SS7MP?

</td>
</tr>
</table>

Procedure 108. Delete Server VM

Once the servers being deleted have been identified, placed in OOS, and removed the from the server group, it is safe to shut down and delete the VM for the server.

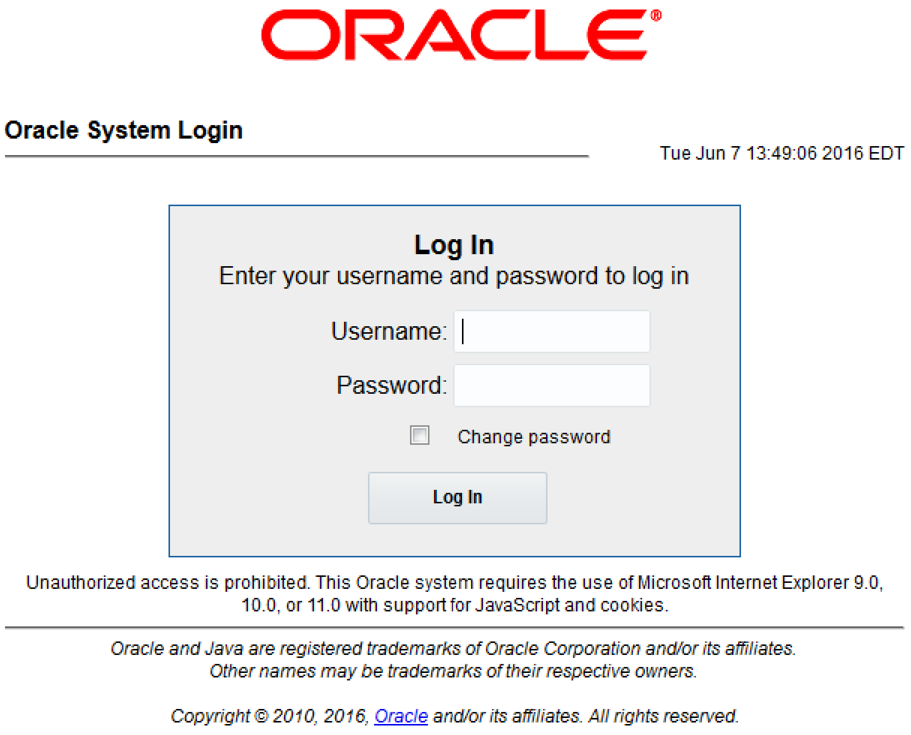
This procedure removes a VM from a TVOE host.

WARNING

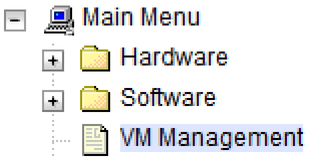
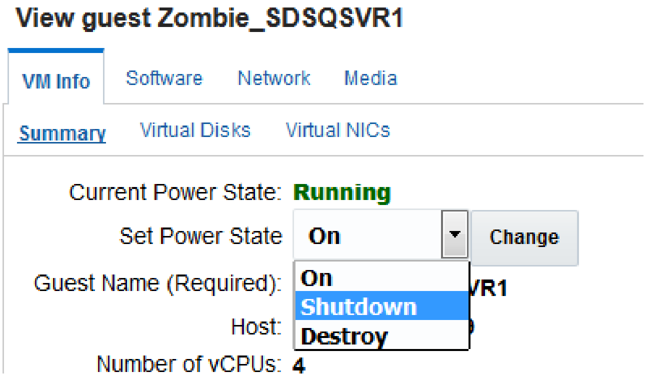
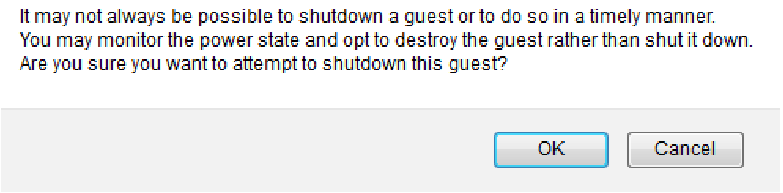
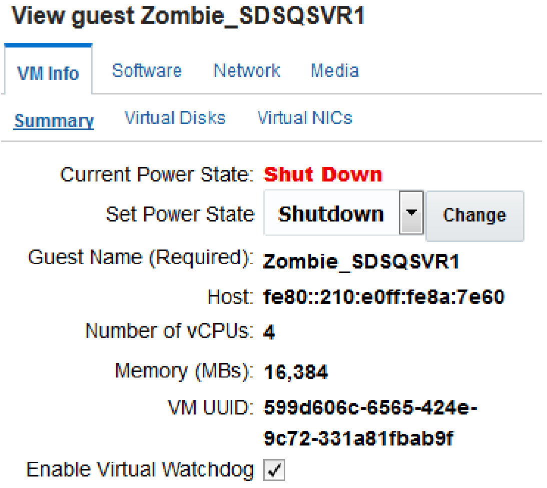
Confirm the server to VM mapping before proceeding.

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

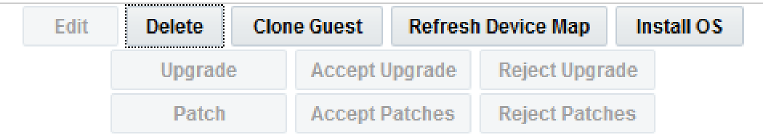
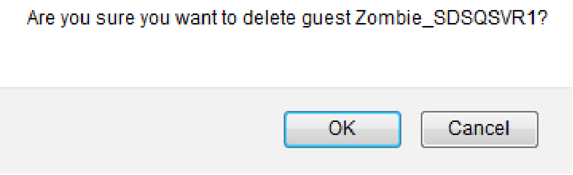
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

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

Procedure 108. Delete Server VM

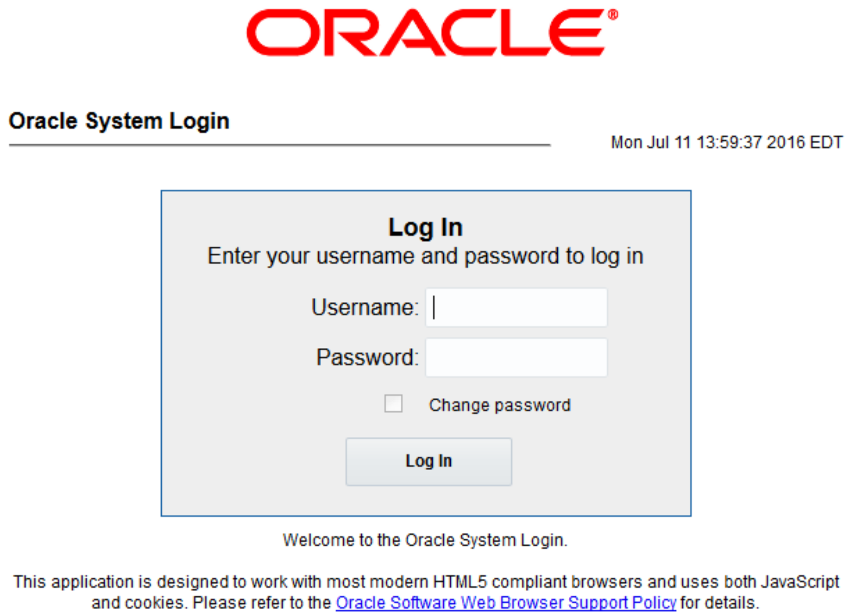
2. ☐	**NOAM VIP GUI**: Shut down the VM	1. Navigate to **VM Management**.  Main Menu Hardware Software VM Management 2. Expand the view of the rack mount server, if needed. 3. Shut down the VM by setting the Current Power State to **Shutdown**.  View guest Zombie_SDSQSVR1 VM Info Software Network Media Summary Virtual Disks Virtual NICs Change On Shutdown Destroy Current Power State: Running Set Power State: On Guest Name (Required): VR1 Host: Number of vCPUs: 4 4. Click **Change**. 5. Click **OK**.  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 Current Power State displays as **Shutdown**.  View guest Zombie_SDSQSVR1 VM Info Software Network Media Summary Virtual Disks Virtual NICs Change Current Power State: Shut Down Set Power State: Shutdown Guest Name (Required): Zombie_SDSQSVR1 Host: fe80::210:e0ff:fe8a:7e60 Number of vCPUs: 4 Memory (MBs): 16,384 VM UUID: 599d606c-6565-424e-9c72-331a81fbab9f Enable Virtual Watchdog ☑

Procedure 108. Delete Server VM

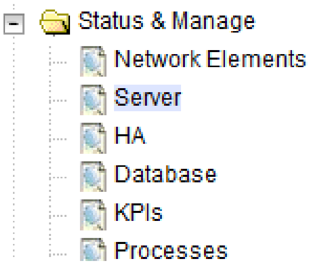
3. ☐	**PMAC GUI**: Delete the VM	1. Once the server has been shut down, select the VM. 2. Verify the current power state is **Shutdown** and click **Delete**.  Edit Delete Clone Guest Refresh Device Map Install OS Upgrade Accept Upgrade Reject Upgrade Patch Accept Patches Reject Patches 3. Click **OK** to confirm. Are you sure you want to delete guest Zombie_SDSQSVR1?

Procedure 109. Post De-Growth Health Check

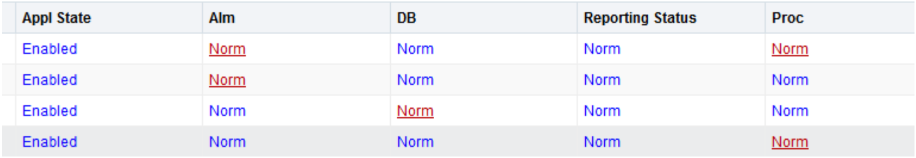
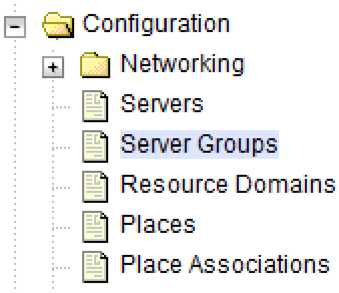
This procedure verifies system status and logs all alarms after de-growth. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  ORACLE 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.

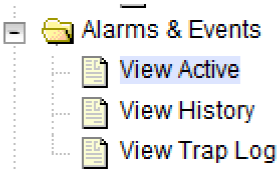
Procedure 109. Post De-Growth Health Check

<table>
<tr><td>2.
☐</td><td>NOAM VIP GUI: Verify server status</td><td>1. Navigate to Status & Manage > Server.


Status & Manage
Network Elements
Server
HA
Database
KPIs
Processes

2. 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></td></tr>
<tr><td>3.
☐</td><td>NOAM VIP GUI: Verify server configuration</td><td>1. Navigate to Configuration > Server Groups.


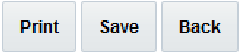
Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Verify the configuration data is correct for your network.</td></tr>
<tr><td>4.
☐</td><td>NOAM VIP GUI: Log current alarms</td><td>1. Navigate to Alarms & Events > View Active.


Alarms & Events
View Active
View History
View Trap Log

2. Click Report.

Export
Report
Clear Selections

3. Save or Print this report, keep copies for future reference.


Print
Save
Back

4. Compare this alarm report with those gathered in Procedure 105 Perform Health Check.</td></tr>
<tr><td>5.
☐</td><td>SOAM VIP GUI: Repeat</td><td>Repeat this procedure the SOAM.</td></tr>
</table>

Procedure 110. Post De-Growth Backups

This procedure backs up 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	Back up TVOE	Back up all TVOE host configurations by executing section 3.17.6 Back Up TVOE Configuration.
2. ☐	Back up PMAC	Back up the PMAC application by executing section 3.17.7 Back Up PMAC Application.
3. ☐	Back up NOAM/SOAM databases	Back up the NOAM and SOAM databases by executing sections 3.17.8 Back Up NOAM Database and 3.17.9 Back Up SOAM Database. ***Note:*** Database backup on SDS SOAMs is not required.

Appendix P.3 Re-Shuffle (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 (10Gbps) Only)

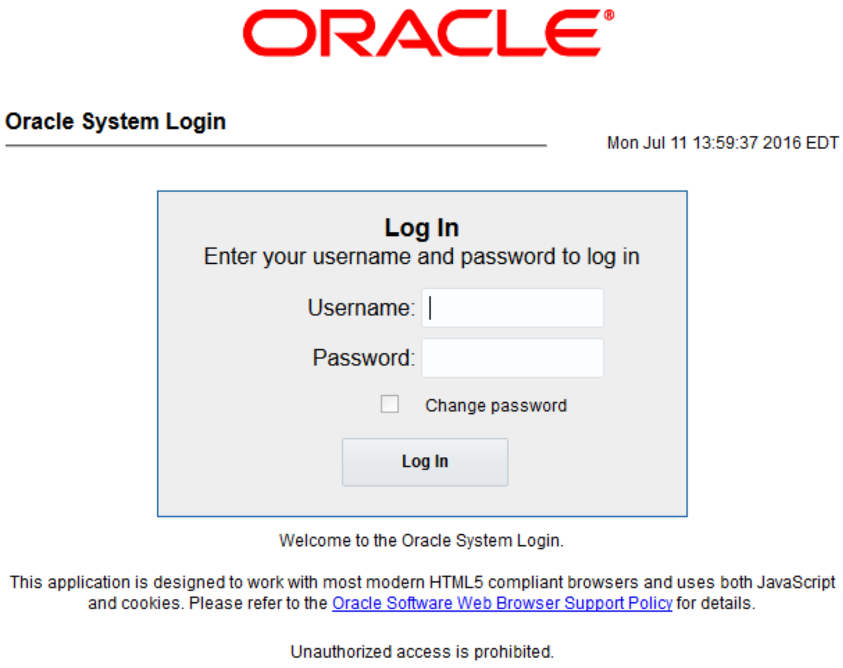
For growth/de-growth scenarios where you need to move or re-shuffle DSR/SDS servers to different TVOE hosts, follow these procedures.

Step	Procedure(s)
Perform backups	Procedure 104 Perform Backups
Perform system health check	Procedure 105 Perform Health Check
Add new rack mount server, if necessary	
Identify servers affected by growth: • NOAM • SOAM • DSR MP (SBR, SS7MP, IPFE)/SDS DP • Query Server • PMAC	
Remove identified servers from server group	Procedure 106 Remove Server from Server Group and Procedure 107 Delete Server/Server Group
Shut down and remove the identified server’s VM	Procedure 108 Delete Server VM
Identify new rack mount server	
Create and configure VMs on new rack mount server	
Configure servers in new VM locations	
Post move/re-shuffle health check	Procedure 109 Post De-Growth Health Check
Post move/re-shuffle backups	Procedure 110 Post De-Growth Backups

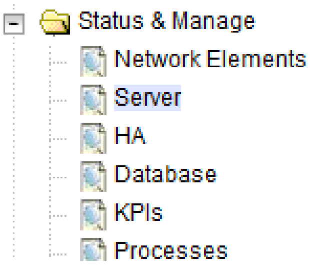
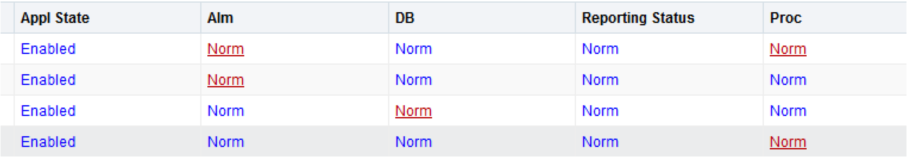
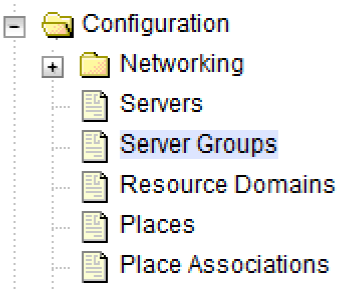
Procedure 111. Perform Backups

<table>
<tr><td colspan="3">This procedure backs up 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 My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>Backup TVOE</td><td>Back up all TVOE host configurations by executing section 3.17.6 Back Up TVOE Configuration.</td></tr>
<tr><td>2.
☐</td><td>Backup PMAC</td><td>Back up the PMAC application by executing section 3.17.7 Back Up PMAC Application.</td></tr>
<tr><td>3.
☐</td><td>Backup NOAM/SOAM databases</td><td>Back up the NOAM and SOAM databases by executing sections 3.17.8 Back Up NOAM Database and 3.17.9 Back Up SOAM Database.
Note: Database backup on SDS SOAMs is not required.</td></tr>
</table>

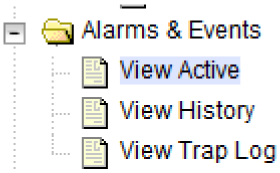
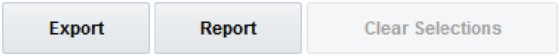
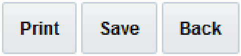
Procedure 112. Perform Health Check

<table>
<tr><td colspan="3">This procedure verifies system status and logs 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 My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>**NOAM VIP GUI**: Login</td><td>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:
`https://<Primary_NOAM_VIP_IP_Address>`
2. Login as the **guiadmin** user.

Oracle System Login
Mon Jul 11 13:59:37 2016 EDT
Log In
Enter your username and password to log in
Username:
Password:
☐ Change password
Log In
Welcome to the Oracle System Login.
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.
Unauthorized access is prohibited.</td></tr>
</table>

Procedure 112. Perform Health Check

<table>
<tr>
<td>2.
☐</td>
<td>**NOAM VIP GUI**: Verify server status</td>
<td>
1. Navigate to **Status & Manage > Server**.

Status & Manage
Network Elements
Server
HA
Database
KPIs
Processes
2. 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 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.
</td>
</tr>
<tr>
<td>3.
☐</td>
<td>**NOAM VIP GUI**: Verify server configuration</td>
<td>
1. Navigate to **Configuration > Server Groups**.

Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations
2. Verify the configuration data is correct for your network.
</td>
</tr>
</table>

Procedure 112. Perform Health Check

4. ☐	**NOAM VIP GUI**: Log current alarms	1. Navigate to **Alarms & Events > View Active**.  Alarms & Events View Active View History View Trap Log 2. Click **Report**.  Export Report Clear Selections 3. **Save** or **Print** this report, keep copies for future reference.  Print Save Back
5. ☐	**SOAM VIP GUI**: Repeat for SOAM	Repeat this procedure for the SOAM.

Procedure 113. Add a New TVOE Server

This procedure adds 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 My Oracle Support (MOS) and ask for assistance.

1. ☐	Add/Configure additional servers	Follow these sections to install and configure TVOE on additional rack mount servers: 1. Section 3.8 Install TVOE on Additional Rack Mount Servers 2. Section 3.9 Configure TVOE on Additional Rack Mount Servers

Procedure 114. Place Server in OOS

Once the server that will be moved has been identified, the server first needs to be placed in HA OOS.

This procedure places the server in OOS HA state.

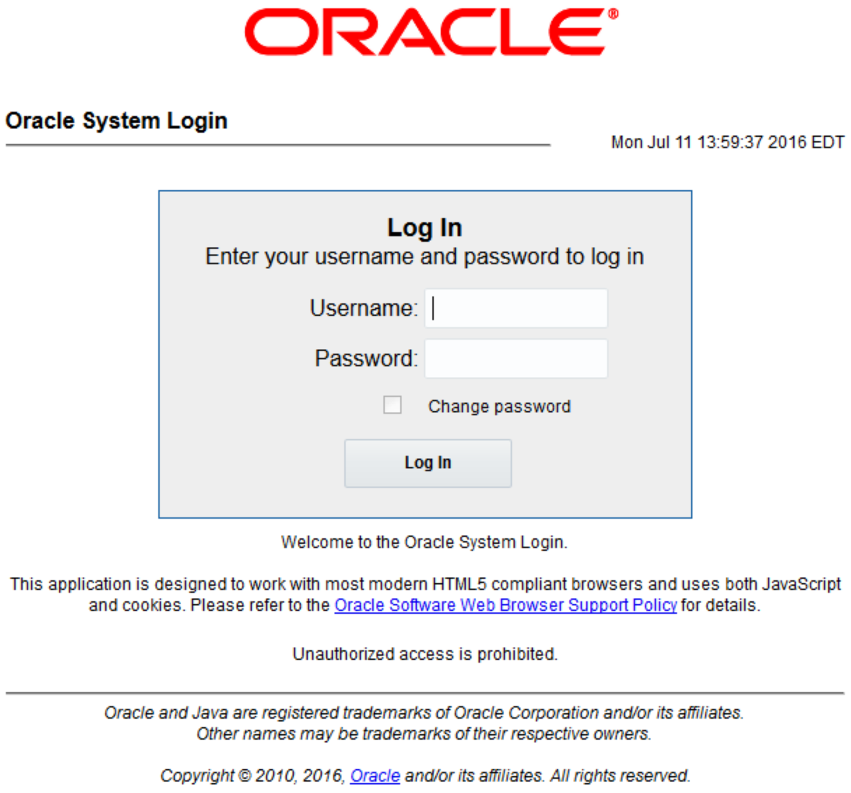
WARNING

No more than one server from each server should be placed in OOS at one time.

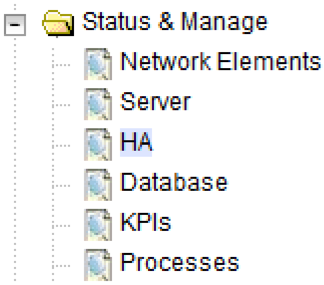
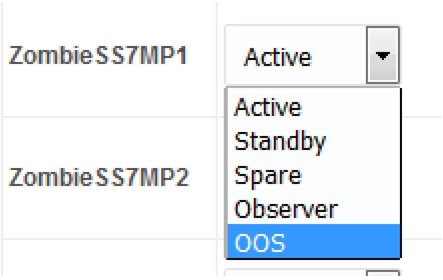
For NOAM and SOAM servers, move/re-shuffle the servers one at a time.

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

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

1. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in 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 114. Place Server in OOS

2. ☐	**NOAM VIP GUI**: Set server to OOS	1. Navigate to **Status & Manage > HA**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Click **Edit**. 3. Set the server's Max Allowed HA Role to **OOS**.  ZombieSS7MP1 Active Active Standby Spare Observer OOS ZombieSS7MP2 4. Click **OK**.

Procedure 115. Delete Server VM

Once the servers being deleted have been identified, placed in OOS, and removed the from the server group, it is safe to shut down and delete the VM for the server.

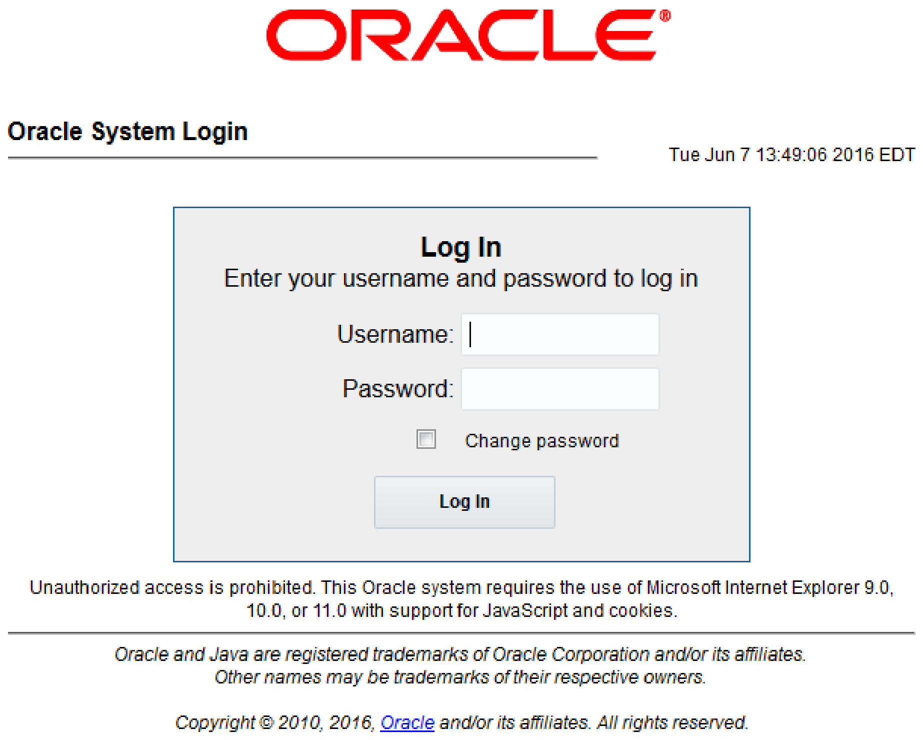
This procedure removes a VM from a TVOE host.

WARNING

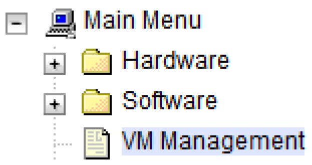
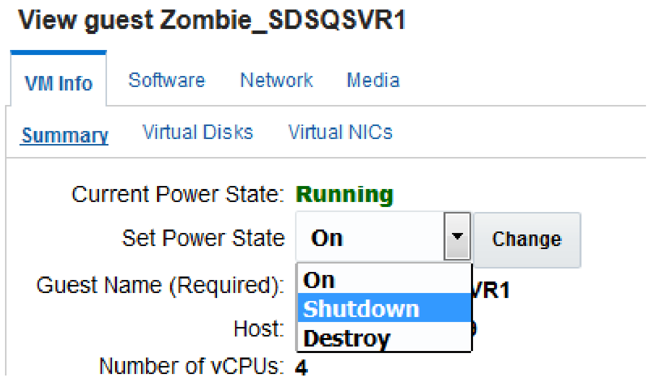
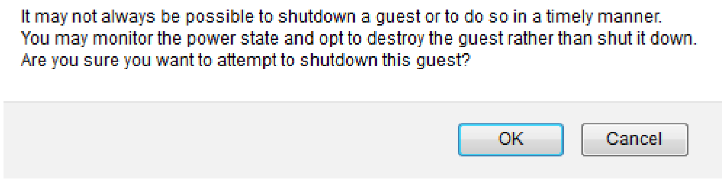
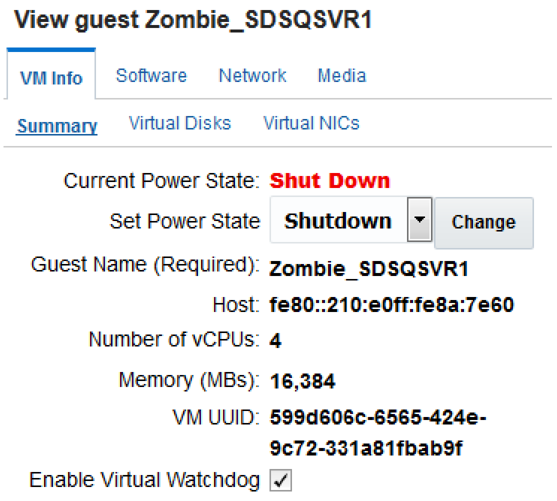
Confirm the server to VM mapping before proceeding.

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

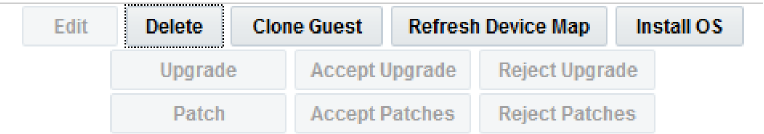
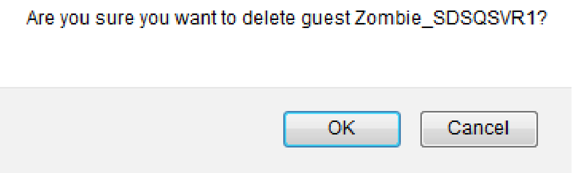
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

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

Procedure 115. Delete Server VM

2. ☐	**NOAM VIP GUI**: Shut down the VM	1. Navigate to **VM Management**.  Main Menu Hardware Software VM Management 2. Expand the view of the rack mount server, if needed. 3. Shut down the VM by setting the Current Power State to **Shutdown**.  View guest Zombie_SDSQSVR1 VM Info Software Network Media Summary Virtual Disks Virtual NICs Change On Shutdown Destroy Current Power State: **Running** Set Power State **On** Guest Name (Required): **VR1** Host: Number of vCPUs: **4** 4. Click **Change**. 5. Click **OK**.  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 Current Power State displays as **Shutdown**.  View guest Zombie_SDSQSVR1 VM Info Software Network Media Summary Virtual Disks Virtual NICs Change Current Power State: **Shut Down** Set Power State **Shutdown** Guest Name (Required): **Zombie_SDSQSVR1** Host: **fe80::210:e0ff:fe8a:7e60** Number of vCPUs: **4** Memory (MBs): **16,384** VM UUID: **599d606c-6565-424e-9c72-331a81fbab9f** Enable Virtual Watchdog ☑

Procedure 115. Delete Server VM

3. ☐	**PMAC GUI**: Delete the VM	1. Once the server has been shut down, select the VM. 2. Verify the current power state is **Shutdown** and click **Delete**.  Edit Delete Clone Guest Refresh Device Map Install OS Upgrade Accept Upgrade Reject Upgrade Patch Accept Patches Reject Patches 3. Click **OK** to confirm. Are you sure you want to delete guest Zombie_SDSQSVR1?

Procedure 116. Move/Re-Shuffle: Create/Configure VMs

This procedure creates the new VM, loads, the software, and configures the server.

Prerequisites:

- Server has been identifies placed in OOS, and its corresponding VM has been deleted.
- Proper VM mapping has been determined to maintain performance efficiency. See section 3.10 Determine VM Placement.
- PMAC contains TPD, DSR, and SDS ISO software. See Procedure 14 Load DSR, SDS, and TPD ISOs onto the PMAC 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 My Oracle Support (MOS) and ask for assistance.

1. ☐	**PMAC GUI**: Create virtual machine	To create a virtual machine for all applicable servers, follow section 3.12 Virtual Machine/Network Fast Deployment.
2. ☐	**TVOE Host**: Execute CPU pinning	Execute section 3.13 CPU Pinning to allocate CPU resources on each new VM.

Procedure 117. Move/Re-Shuffle: NOAM/DR NOAM

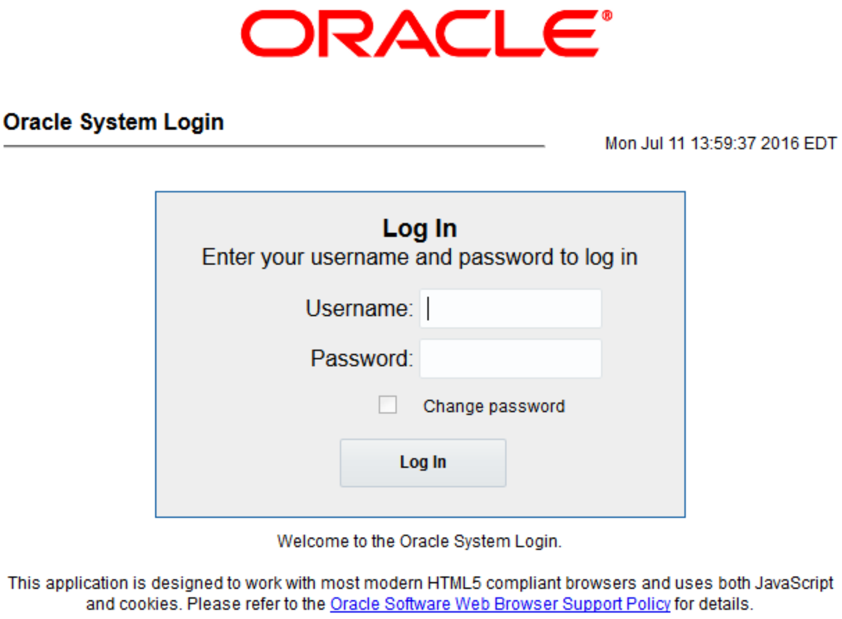
This procedure configures the NOAM/DR NOAM on the new VM for VM re-shuffling scenarios.

Prerequisites:

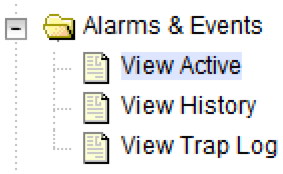
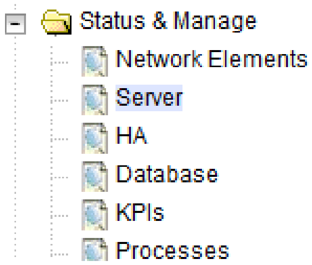
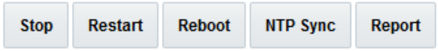
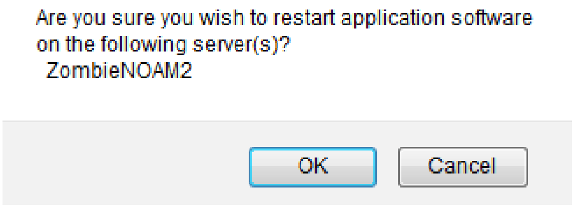
- NOAM/DR NOAM has been Identified
- Placed in OOS
- Old VM deleted
- New VM created
- TPD/DSR software installed

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

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

1. ☐	**NOAM VIP GUI**: Configure the 2nd NOAM/DR NOAM	Configure the second NOAM/DR NOAM by following these sections: • **DSR NOAM**: Procedure 17 Configure First DSR NOAM NE and Server, steps 1. through 2. , 4. through 7. , 8. (optional for NetBackup), and 9. • **DSR DR NOAM**: Procedure 22 Configure DSR NOAM for DR Site (Optional), steps • **SDS NOAM**: Procedure 39 Configure First SDS NOAM NE and Server, steps 1. through 2. , 4. through 5. , 6. (optional for NetBackup), and 7. • **SDS DR NOAM**: Procedure 44 Configure SDS NOAM for DR Site (Optional)
2. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  Oracle System Login Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in Username: Password: ☐ Change password Log In Welcome to the Oracle System Login. This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

Procedure 117. Move/Re-Shuffle: NOAM/DR NOAM

3. ☐	**NOAM VIP**: Wait for remote database alarm to clear	Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding. Monitor progress by navigating to **Alarms & Events > View Active**.  Alarms & Events View Active View History View Trap Log
4. ☐	**NOAM GUI**: Restart 2nd NOAM/DR NOAM server	1. Navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the second NOAM/DR NOAM server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm. Are you sure you wish to restart application software on the following server(s)? ZombieNOAM2
5. ☐	**NOAM GUI**: Activate optional features	If there are any optional features currently activated, the feature activation procedures need to be run again. Refer to section 1.5 Optional Features.

Procedure 118. Move/Re-Shuffle: SOAM

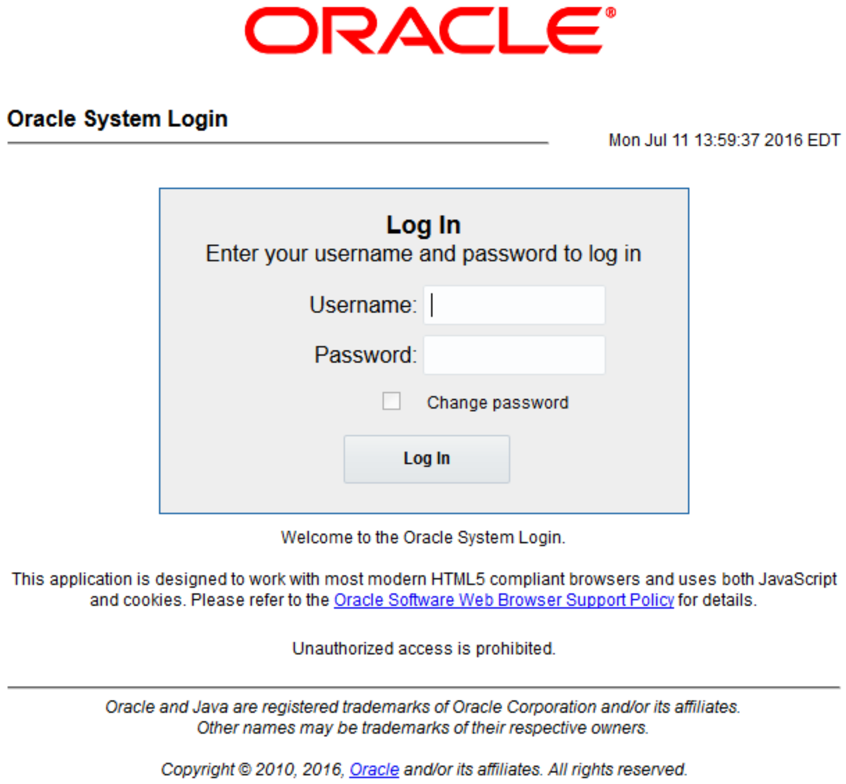
This procedure configures the SOAM on the new VM for VM re-shuffling scenarios.

Prerequisites:

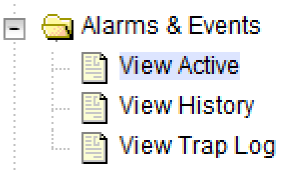
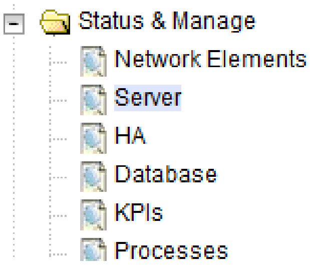
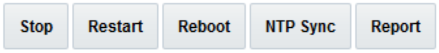
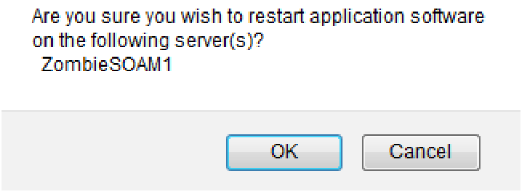
- SOAM has been Identified
- Placed in OOS
- Old VM deleted
- New VM created
- TPD/DSR software installed

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

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

1. ☐	**NOAM VIP GUI**: Configure the SOAM	Configure the SOAM by following these sections: • **DSR SOAM**: Procedure 25 Configure DSR SOAM Server, steps 1. through 3. , 5. through 9. , 11. (optional for NetBackup) • **SDS DP SOAM**: Procedure 49 Configure SDS DP SOAM Server, steps 1. through 3. , 5. through 9.
2. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  Oracle System Login Mon Jul 11 13:59:37 2016 EDT Log In Enter your username and password to log in Username: Password: ☐ Change password 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 118. Move/Re-Shuffle: SOAM

3. ☐	**NOAM VIP**: Wait for remote database alarm to clear	Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding. Monitor progress by navigating to **Alarms & Events > View Active**.  Alarms & Events View Active View History View Trap Log
4. ☐	**NOAM GUI**: Restart SOAM server	1. Navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the SOAM server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm.  Are you sure you wish to restart application software on the following server(s)? ZombieSOAM1
5. ☐	**NOAM GUI**: Activate optional features	If there are any optional features currently activated, the feature activation procedures need to be run again. Refer to section 1.5 Optional Features.

Procedure 119. Move/Re-Shuffle: MP/DP

This procedure configures MP/DP on the new VM for VM re-shuffling scenarios.

Prerequisites:

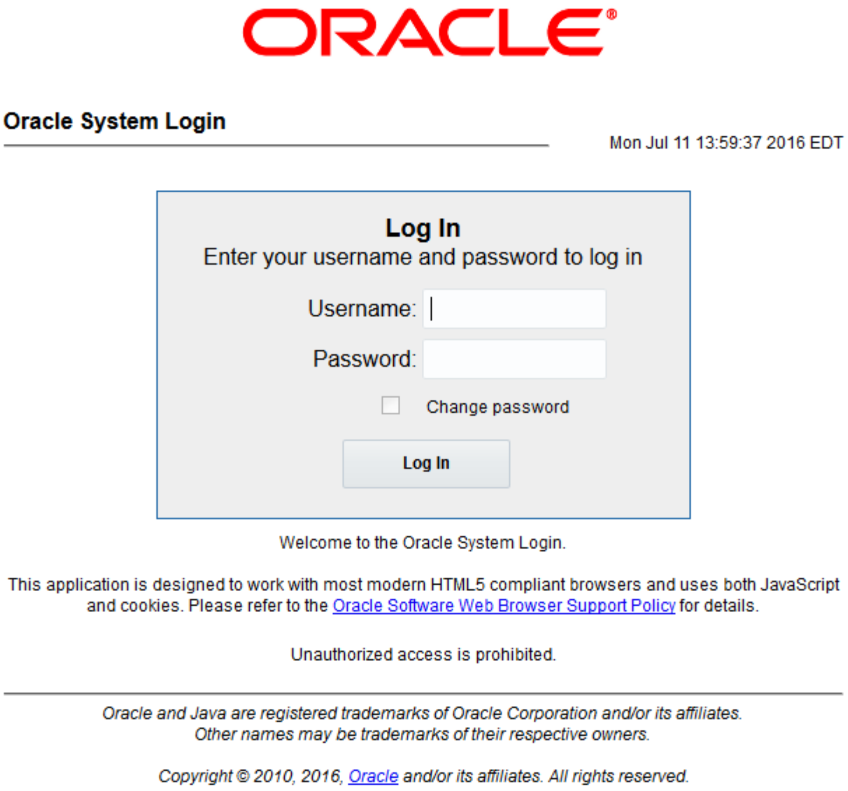
- MP/DP has been Identified
- Placed in OOS
- Old VM deleted
- New VM created
- TPD/DSR software installed

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

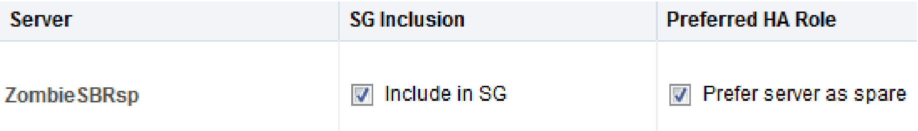
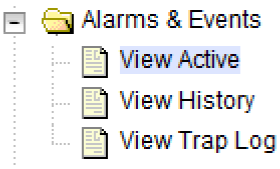
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**NOAM VIP GUI**: Configure the MP/DP	Configure the MP/DP by following these sections: • **DSR MP**: To configure MP blade servers (IPFE, SBR, DA-MP), refer to the procedure Configure MP Blade Servers in the C-Class Software Installation and Configuration Procedure 2/2. • **SDS DP**: To install the Data Processor (DP) blade, refer to the procedure DP Installation (All SOAM sites) in the DSR Initial Installation and Configuration Guide.

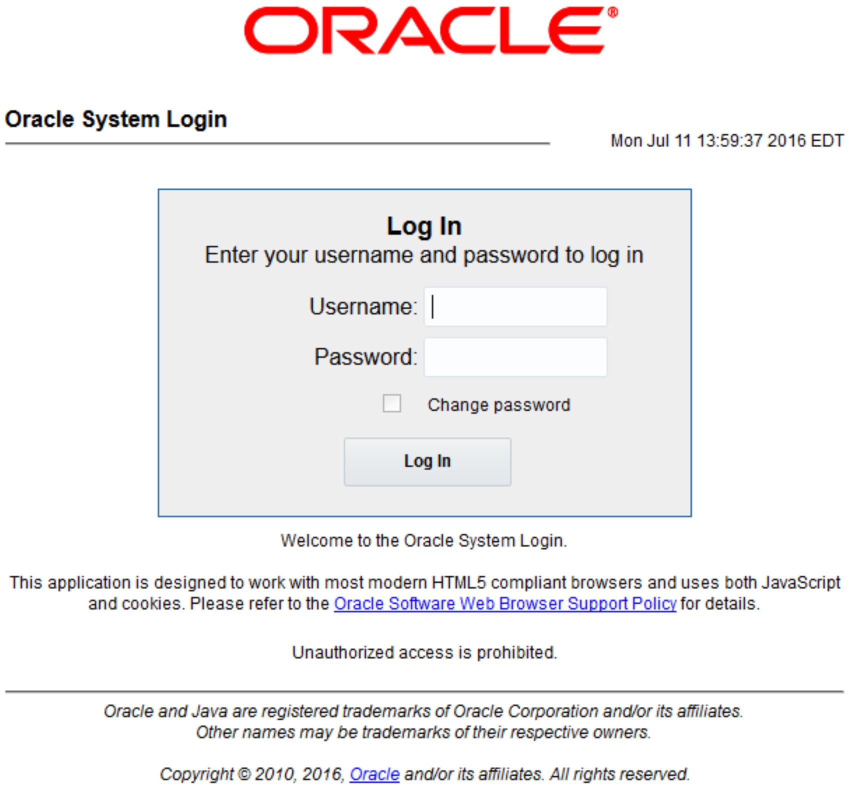
Procedure 119. Move/Re-Shuffle: MP/DP

2. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  ORACLE 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 119. Move/Re-Shuffle: MP/DP

<table>
<tr>
<td>3.
☐</td>
<td>NOAM VIP GUI: Edit the MP server group and add preferred spares for site redundancy (optional)
PCA/DCA Only</td>
<td>If Two Site Redundancy feature for the Policy and Charging SBR server group OR Session Binding Repository is wanted, add an MP server that is physically located in a separate site (location) to the server group by marking the Include in SG checkbox. Also, mark the Preferred Spare checkbox.

<table>
<tr><th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr>
<tr><td>ZombieSBRsp</td><td>☑ Include in SG</td><td>☑ Prefer server as spare</td></tr>
</table>
If Three Site Redundancy feature for the SBR MP server group is wanted, add two SBR MP servers that are both physically located in separate sites (location) to the server group by marking the Include in SG checkbox. Also, mark the Preferred Spare checkbox for both servers.
<i>Notes</i>:
• 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).
• There must first be non-preferred spare available in 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 section 1.3 Terminology.
Click OK to save.</td>
</tr>
<tr>
<td>4.
☐</td>
<td>NOAM VIP: Wait for remote database alarm to clear</td>
<td>Wait for the Remote Database re-initialization in progress alarm to clear before proceeding.
Monitor progress by navigating to Alarms & Events > View Active.

</td>
</tr>
</table>

Procedure 119. Move/Re-Shuffle: MP/DP

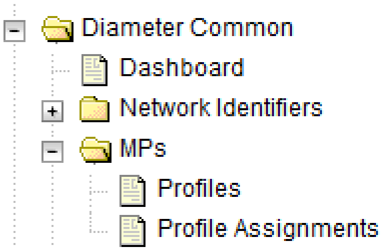
5. ☐	**SOAM VIP GUI**: Login	1. Establish a GUI session on the SOAM server by using the VIP IP address of the SOAM server. Open the web browser and enter a URL of: `https://<Primary_SOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  **Oracle System Login** Mon Jul 11 13:59:37 2016 EDT **Log In** Enter your username and password to log in 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 119. Move/Re-Shuffle: MP/DP

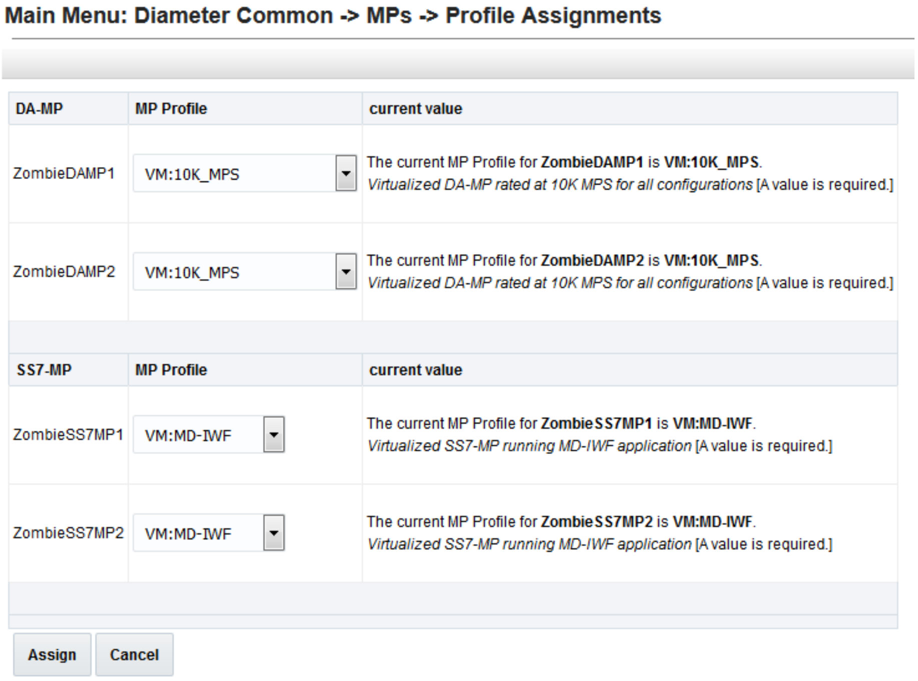
6. ☐

SOAM VIP GUI: Assign profiles to DA-MPs from SOAM GUI

1. Navigate to **Diameter Common > MPs > Profiles Assignments**.



If the site has both DSR and MAP-IWF server groups, both DA-MP and SS7-MP sections display.



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**. *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.]

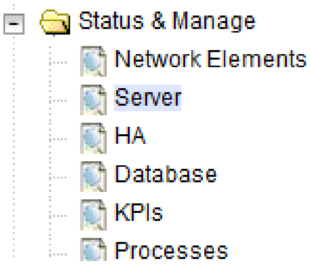
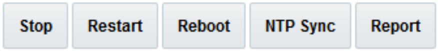
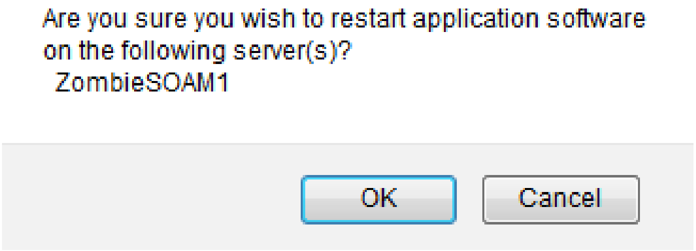
SS7-MP	MP Profile	current value
ZombieSS7MP1	VM:MD-IWF	The current MP Profile for **ZombieSS7MP1** is **VM:MD-IWF**. *Virtualized SS7-MP running MD-IWF application* [A value is required.]
ZombieSS7MP2	VM:MD-IWF	The current MP Profile for **ZombieSS7MP2** is **VM:MD-IWF**. *Virtualized SS7-MP running MD-IWF application* [A value is required.]

2. For each MP, select the proper profile assignment based on the function of each MP.

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

3. Click **Assign**.

Procedure 119. Move/Re-Shuffle: MP/DP

7. ☐	**NOAM GUI**: Restart MP/DP server	1. Navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the MP/DP server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm.  Are you sure you wish to restart application software on the following server(s)? ZombieSOAM1

Procedure 120. Move/Re-Shuffle: Query Server (SDS Only)

This procedure configures the query server on the new VM for VM re-shuffling scenarios.

Prerequisites:

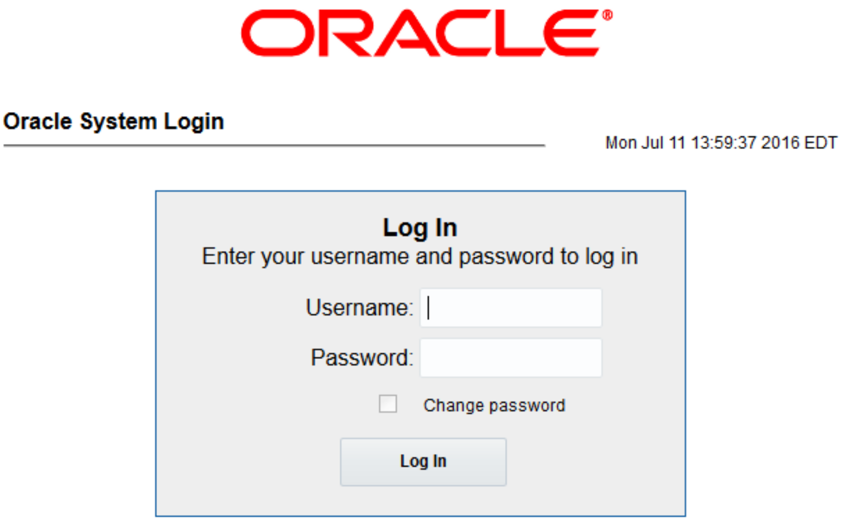
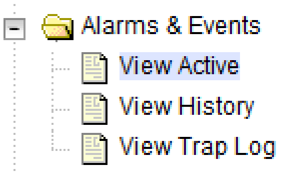
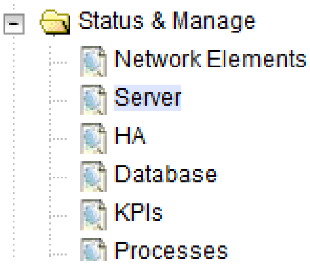
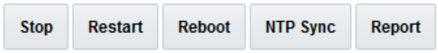
- Query server has been Identified
- Placed in OOS
- Old VM deleted
- New VM created
- TPD/DSR software installed

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

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

1. ☐	**NOAM VIP GUI**: Configure the query server	Configure the query server by following Procedure 46 Configure SDS Query Server.

Procedure 120. Move/Re-Shuffle: Query Server (SDS Only)

2. ☐	**NOAM VIP GUI**: Login	1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of: `https://<Primary_NOAM_VIP_IP_Address>` 2. Login as the **guiadmin** user.  ORACLE 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
3. ☐	**NOAM VIP**: Wait for remote database alarm to clear	Wait for the **Remote Database re-initialization in progress** alarm to clear before proceeding. Monitor progress by navigating to **Alarms & Events > View Active**.  Alarms & Events View Active View History View Trap Log
4. ☐	**NOAM GUI**: Restart SOAM server	1. Navigate to **Status & Manage > Server**.  Status & Manage Network Elements Server HA Database KPIs Processes 2. Select the query server and click **Restart**.  Stop Restart Reboot NTP Sync Report 3. Click **OK** to confirm.

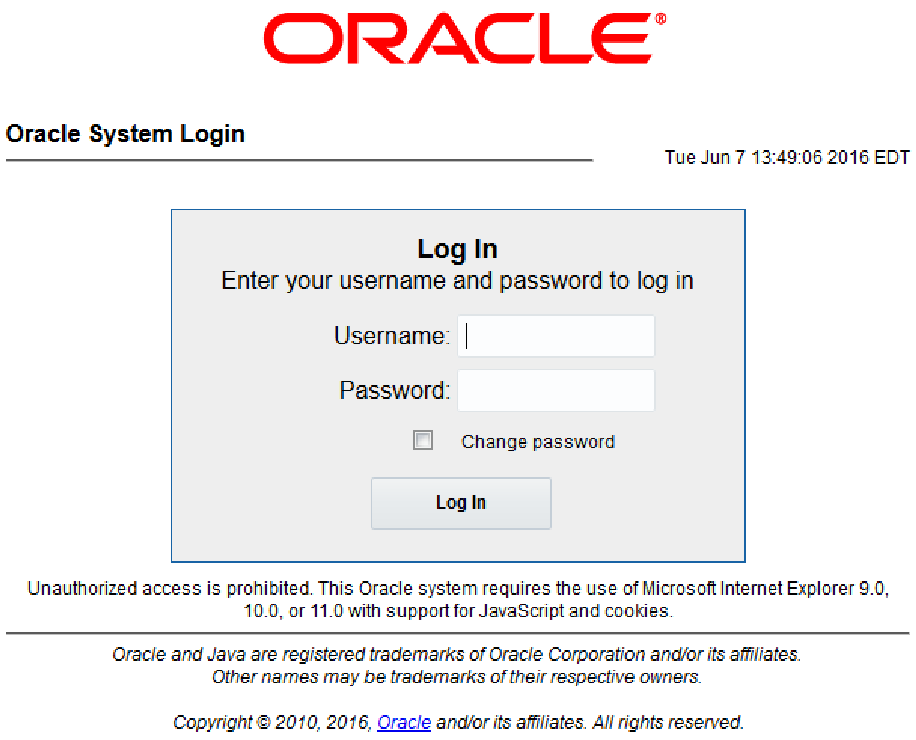
Procedure 121. Move/Re-Shuffle: iDIH

This procedure configures the iDIH server on the new VM for VM re-shuffling scenarios.

Note: If moving/re-shuffling the Oracle VM/server, doing so removes all historical trace data. However, moving/re-shuffling spplication 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.

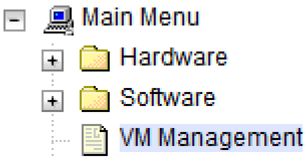
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**PMAC GUI**: Login	1. Open the web browser and navigate to the PMAC GUI: `http://<PMAC_network_IP>` 2. Login as the **guiadmin** user:  **Oracle System Login** Tue Jun 7 13:49:06 2016 EDT **Log In** Enter your username and password to log in 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.*

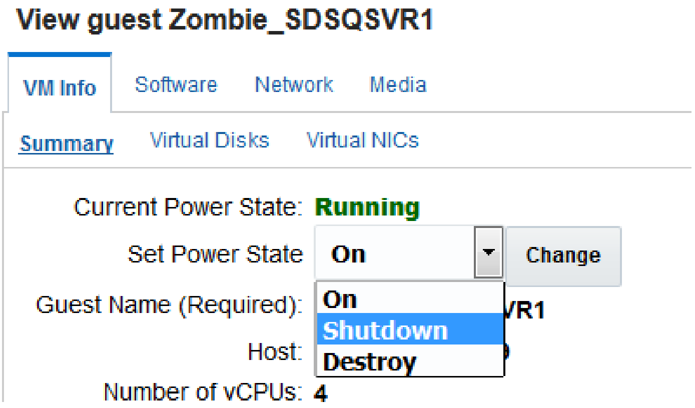
Procedure 121. Move/Re-Shuffle: iDIH

<table>
<tr>
<td>2.
☐</td>
<td>NOAM VIP GUI:
Shut down the VM</td>
<td>

1. Navigate to **VM Management**.


Main Menu
Hardware
Software
VM Management

2. Expand the view of the rack mount server, if needed.
3. Shut down the VM by setting the Current Power State to **Shutdown**.



View guest Zombie_SDSQSVR1

VM Info
Software
Network
Media
Summary
Virtual Disks
Virtual NICs

Current Power State: Running

Set Power State On ▾ Change

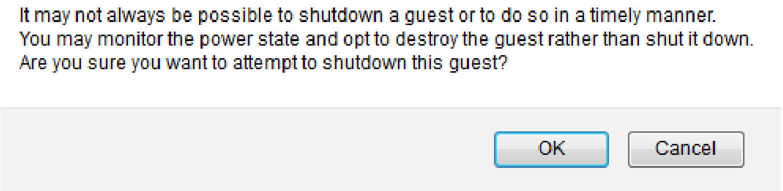
On
Shutdown
Destroy

Guest Name (Required): VR1

Host:

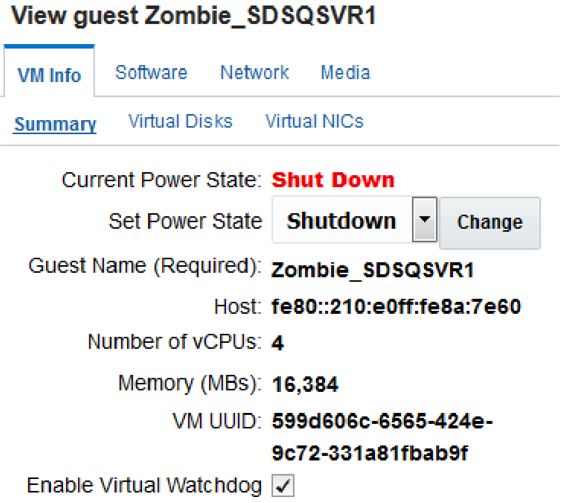
Number of vCPUs: 4

4. Click **Change**.
5. Click **OK**.



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 Current Power State displays as **Shutdown**.



View guest Zombie_SDSQSVR1

VM Info
Software
Network
Media
Summary
Virtual Disks
Virtual NICs
Change

Current Power State: Shut Down

Set Power State Shutdown ▾

Guest Name (Required): Zombie_SDSQSVR1

Host: fe80::210:e0ff:fe8a:7e60

Number of vCPUs: 4

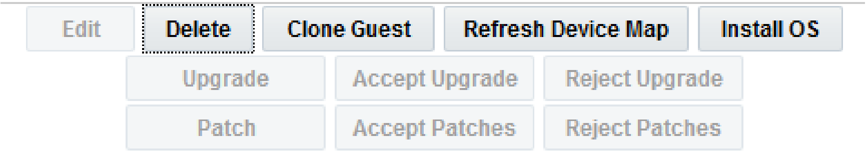
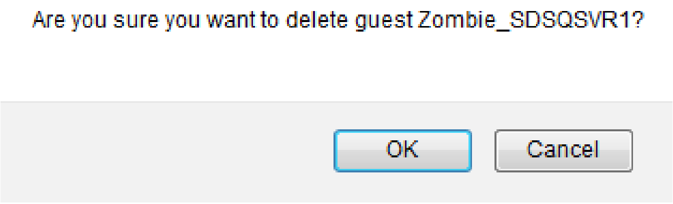
Memory (MBs): 16,384

VM UUID: 599d606c-6565-424e-9c72-331a81fbab9f

Enable Virtual Watchdog ☑

</td>
</tr>
</table>

Procedure 121. Move/Re-Shuffle: iDIH

3. ☐	**PMAC GUI**: Delete the VM	1. Once the server has been shut down, select the VM. 2. Verify the current power state is **Shutdown** and click **Delete**.  Edit Delete Clone Guest Refresh Device Map Install OS Upgrade Accept Upgrade Reject Upgrade Patch Accept Patches Reject Patches 3. Click **OK** to confirm. Are you sure you want to delete guest Zombie_SDSQSVR1?
4. ☐	**PMAC Server**: Navigate to guest-dropin directory	`$ cd /var/TKLC/smac/guest-dropin/`
5. ☐	**PMAC Server**: Edit the IDIH fdc file	Edit the existing **idih_fdc_file_name.xml** (or create a new) file configured in Procedure 54 IDIH Installation, step 7. Changing the rack mount server to the VM being moved/re-shuffled is done 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.

Procedure 122. Move/Re-Shuffle: PMAC

This procedure configures PMAC on the new VM for VM re-shuffling scenarios.

Prerequisite: Database backup of 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 My Oracle Support (MOS) and ask for assistance.

1. ☐	**PMAC**: Back up the PMAC database	Back up the PMAC database by following section 3.17.7 Back Up PMAC Application.
2. ☐	**PMAC TVOE Host**: Login	Establish an SSH session to the PMAC's TVOE host and login as **admusr**.
3. ☐	**PMAC TVOE Host**: Verify PMAC location	Verify the location of the redundant PMAC VM using virsh.

```
$ sudo /usr/bin/virsh list
Id  Name            State
----------------------------------
2   Redundant-PM&C  running
```

Procedure 122. Move/Re-Shuffle: PMAC

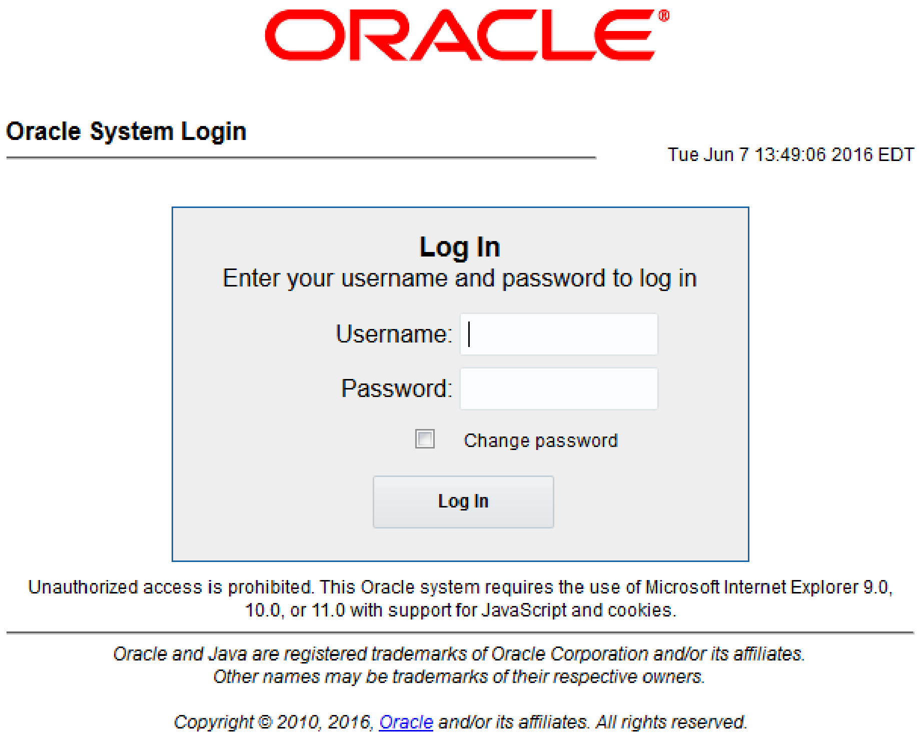
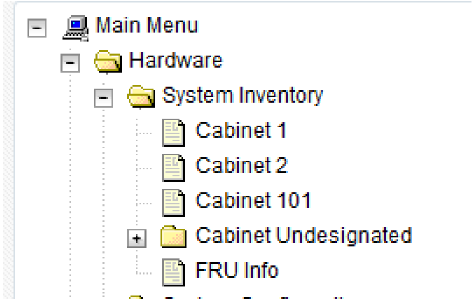
4. ☐	**PMAC TVOE Host**: Remove existing PMAC guest	Delete the PMAC guest. `$ sudo guestMgr –remove <PMAC_Name>`
5. ☐	**New PMAC TVOE Host**: Deploy PMAC on new TVOE host	Once the TVOE host for the new PMAC location has been identified, execute section 3.3 Install PMAC to deploy the new PMAC.
6. ☐	**PMAC**: Login	Establish an SSH session to the PMAC server and login as **admusr**.

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 PMAC backup location. If using IPv6 addresses, command requires shell escapes, for example, **admusr@[<ipV6addr>]:/<file>**
		`$ sudo /usr/bin/scp -p \`
		`admsur@<remoteserver>:/var/TKLC/smac/backup/*.pef \`
		`/var/TKLC/smac/backup/`
		Note: Copy the correct backup file to use in the restore. The latest backup may not be the backup which contains the system data of interest. This could be the case if the automatic backup, which is scheduled in the morning, is performed on the newly installed PMAC before restoring the data.

8. ☐	**PMAC**: Verify no alarms are present	`$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus`

9.
☐
	Restore the PMAC data from backup	`$ sudo /usr/TKLC/smac/bin/pmacadm restore`
		`PM&C Restore been successfully initiated as task ID 1`
		Note: By default, the PMAC restore used the most recent file in **/var/TKLC/smac/backup** folder 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.
		1. To check the status of the background task, issue this command:
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		2. Wait for the **PMAC Restore successful** message.

Procedure 122. Move/Re-Shuffle: PMAC

10. ☐	**PMAC GUI**: Login	1. Open the web browser and navigate to the PMAC GUI: `http://<PMAC_network_IP>` 2. Login as the **guiadmin** user:  ORACLE® Oracle System Login Tue Jun 7 13:49:06 2016 EDT Log In Enter your username and password to log in Username: Password: ☐ Change password Log In Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 9.0, 10.0, or 11.0 with support for JavaScript and cookies. *Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.* *Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.*
11. ☐	**PMAC GUI**: Verify restore task completed	1. Navigate to **Task Monitoring**. 2. Verify the restore background task completed successfully. ***Notes***: • After the restore is complete, **Add Enclosure** tasks start for all previously provisioning servers. Allow these to complete before continuing. • After the restore is complete, some tasks delete ISO images. This is normal behavior, ISO images are added in the next step.
12. ☐	**PMAC GUI**: Verify system inventory	1. Navigate to **Hardware > System Inventory**.  Main Menu Hardware System Inventory Cabinet 1 Cabinet 2 Cabinet 101 Cabinet Undesignated FRU Info 2. Verify previously provisioned enclosures are present.

Procedure 122. Move/Re-Shuffle: PMAC

13.
☐
	PMAC: Verify PMAC	Perform a system health check on the PMAC.
		`$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus`
		Note: Some expected networking alarms may be present.
		This command should return no output on a healthy system.
		`$ sudo /usr/TKLC/smac/bin/sentry status`
		All processes should be running and display output similar to this:
		`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.`

14. ☐	**PMAC**: Add ISO images to the PMAC	Re-add any needed ISO images to the PMAC by executing section 3.8 Install TVOE on Additional Rack Mount Servers.

Procedure 123. Move/Re-Shuffle: Redundant PMAC

This procedure configures the redundant PMAC on the new VM 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Redundant PMAC TVOE Host**: Login	Establish an SSH session to the redundant PMAC's TVOE host and login as **admusr**.

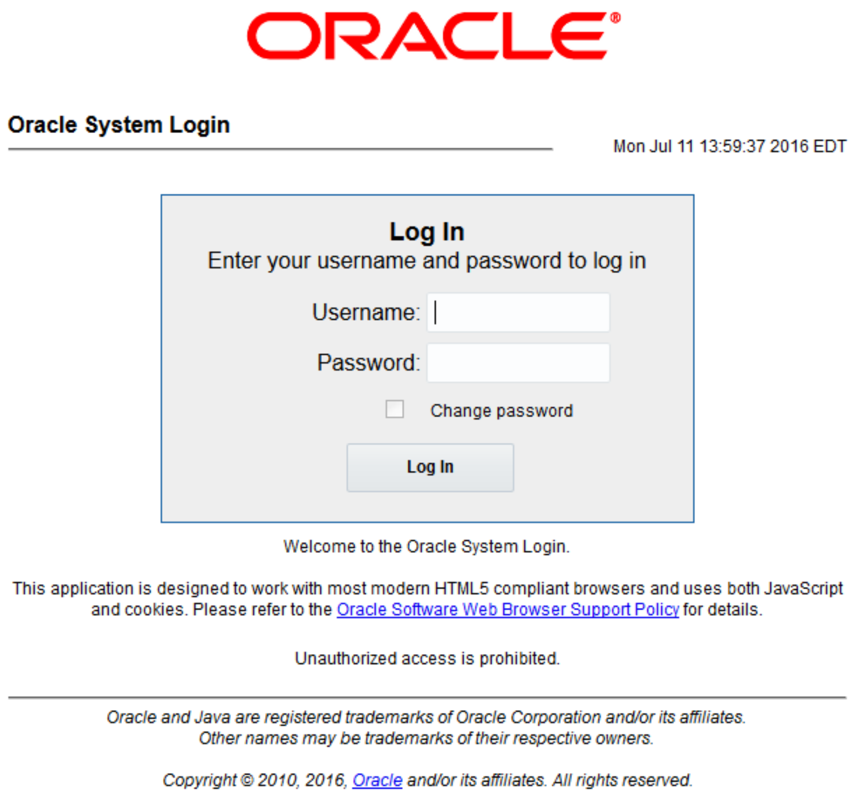
2.
☐
	Redundant PMAC TVOE Host: Verify PMAC location	Verify the location of the redundant PMAC VM using virsh.
		`$ sudo /usr/bin/virsh list`
		`Id  Name            State`
		`----------------------------------`
		`2   Redundant-PM&C  running`

3. ☐	**Redundant PMAC TVOE Host**: Remove existing PMAC guest	If an error was made, use this command to delete the PMAC guest and re-deploy the guest. `$ sudo guestMgr –remove <PMAC_Name>`

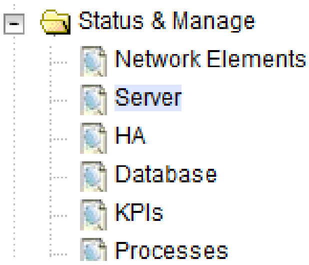
Procedure 123. Move/Re-Shuffle: Redundant PMAC

4. ☐	**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 3.11 Deploy Redundant PMAC (Optional) to deploy the redundant PMAC.

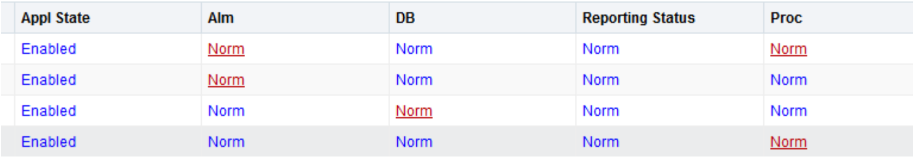
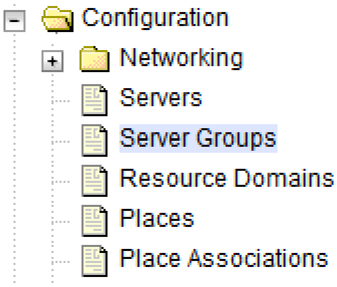
Procedure 124. Post Moving/Re-Shuffling Health Check

<table>
<tr><td colspan="3">This procedure verifies system status and logs all alarms after moving/re-shuffling.
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</td></tr>
<tr><td>1.
☐</td><td>NOAM VIP GUI: Login</td><td>1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and enter a URL of:
<code>https://<Primary_NOAM_VIP_IP_Address></code>
2. Login as the guiadmin user.

Oracle System Login
Mon Jul 11 13:59:37 2016 EDT
Log In
Enter your username and password to log in
Username:
Password:
☐ Change password
Log In
Welcome to the Oracle System Login.
This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.
Unauthorized access is prohibited.
<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></td></tr>
</table>

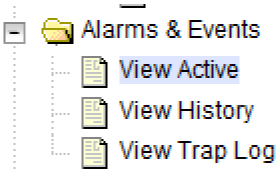
Procedure 124. Post Moving/Re-Shuffling Health Check

<table>
<tr><td>2.
☐</td><td>NOAM VIP GUI: Verify server status</td><td>1. Navigate to Status & Manage > Server.


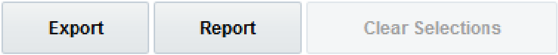
Status & Manage
Network Elements
Server
HA
Database
KPIs
Processes

2. 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></td></tr>
<tr><td>3.
☐</td><td>NOAM VIP GUI: Verify server configuration</td><td>1. Navigate to Configuration > Server Groups.


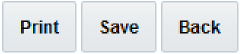
Configuration
Networking
Servers
Server Groups
Resource Domains
Places
Place Associations

2. Verify the configuration data is correct for your network.</td></tr>
<tr><td>4.
☐</td><td>NOAM VIP GUI: Log current alarms</td><td>1. Navigate to Alarms & Events > View Active.


Alarms & Events
View Active
View History
View Trap Log

2. Click Report.


Export
Report
Clear Selections

3. Save or Print this report, keep copies for future reference.


Print
Save
Back

4. Compare this alarm report with those gathered in Procedure 112 Perform Health Check.</td></tr>
<tr><td>5.
☐</td><td>SOAM VIP GUI: Repeat</td><td>Repeat this procedure the SOAM.</td></tr>
</table>

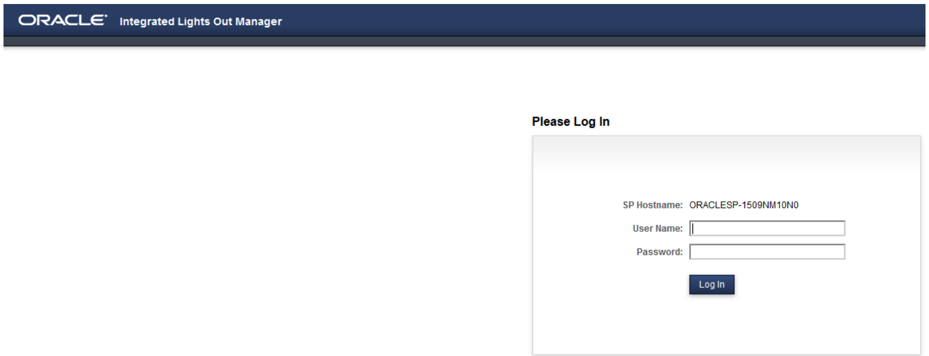
Procedure 125. Post Move/Re-Shuffle Backups

This procedure backs up all necessary items after a move/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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	Backup TVOE	Back up all TVOE host configurations by executing section 3.17.6 Back Up TVOE Configuration.
2. ☐	Backup PMAC	Back up the PMAC application by executing section 3.17.7 Back Up PMAC Application.
3. ☐	Backup NOAM/SOAM databases	Back up the NOAM and SOAM databases by executing sections 3.17.8 Back Up NOAM Database and 3.17.9 Back Up SOAM Database. ***Note:*** Database backup on SDS SOAMs is not required.

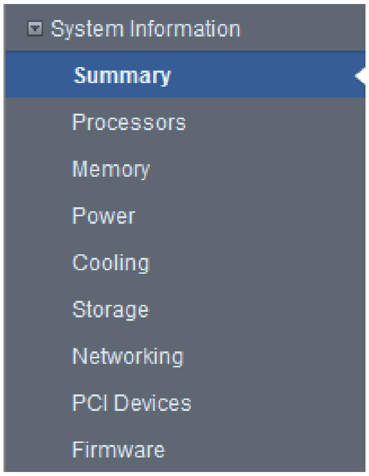
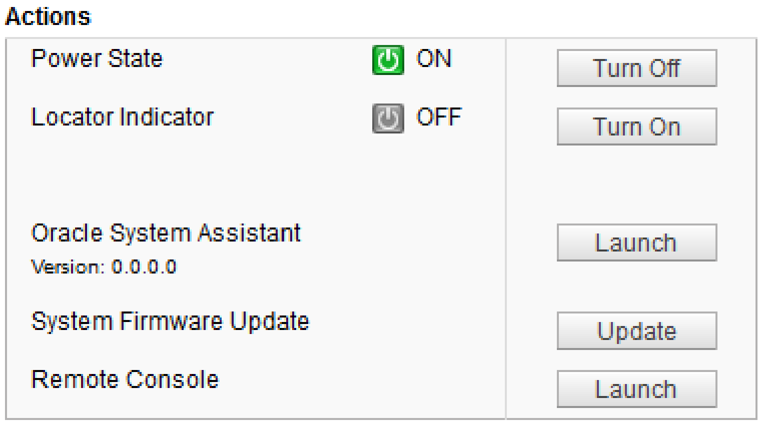
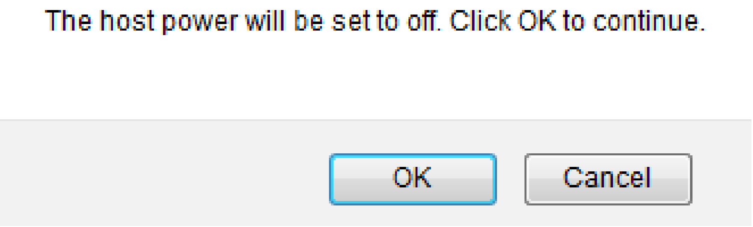
Appendix Q. Non-HA Lab Node Instructions (Oracle X5-2/Netra X5-2/X6-2/X7-2/HP DL380 Gen 9 (10Gbps) Non-HA Lab Node Only)

Appendix Q.1 Non-HA Lab Node Pre-IPM Procedures

Procedure 126. RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X5-2/Netra X5-2)

This procedure creates an HD RAID10 volume by combining multiple HDD on Oracle X5-2/Netra X5-2. ***Prerequisites***: • 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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Oracle X5-2/Netra X5-2**: Login	Log into the Oracle rack mount server ILOM.  ORACLE Integrated Lights Out Manager Please Log In User Name: Password: Log In SP Hostname: ORACLESP-1509NM10N0

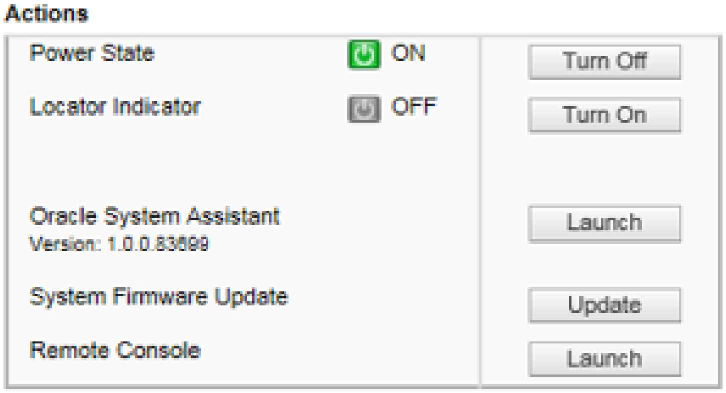
Procedure 126. RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X5-2/Netra X5-2)

2. ☐	**ILOM GUI**: Turn off the power	1. Navigate to **System Information > Summary**.  System Information Summary Processors Memory Power Cooling Storage Networking PCI Devices Firmware 2. From the Actions window, click **Turn Off** for Power State.  Actions Power State ON Turn Off Locator Indicator OFF Turn On Oracle System Assistant Launch Version: 0.0.0.0 System Firmware Update Update Remote Console Launch 3. Click **OK** to confirm  The host power will be set to off. Click OK to continue.

Procedure 126. RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X5-2/Netra X5-2)

<table>
<tr>
<td>3.
☐</td>
<td>ILOM GUI: Launch Oracle system assistant and accept license agreement</td>
<td>

1. Click **Launch** next to Oracle System Assistant to launch a remote console.



Actions

Power State ON

Locator Indicator OFF

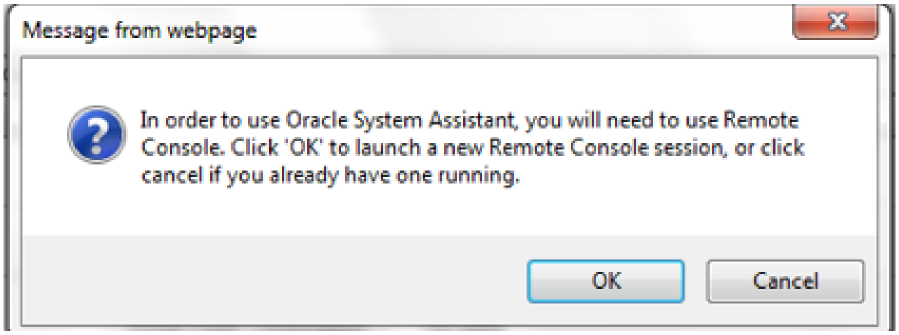
Oracle System Assistant
Version: 1.0.0.83699

System Firmware Update

Remote Console

Turn Off
Turn On
Launch
Update
Launch

2. Click **OK** and wait for Oracle System Assistant to open.



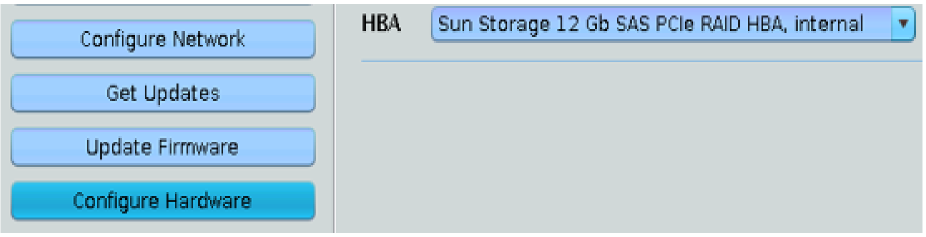
Message from webpage

In order to use Oracle System Assistant, you will need to use Remote Console. Click 'OK' to launch a new Remote Console session, or click cancel if you already have one running.

3. Click **Accept** to accept the license agreement.

</td>
</tr>
<tr>
<td>4.
☐</td>
<td>ILOM GUI: Configure hardware and select HBA</td>
<td>

Click **Configure Hardware** and select the HBA. There should only be one.

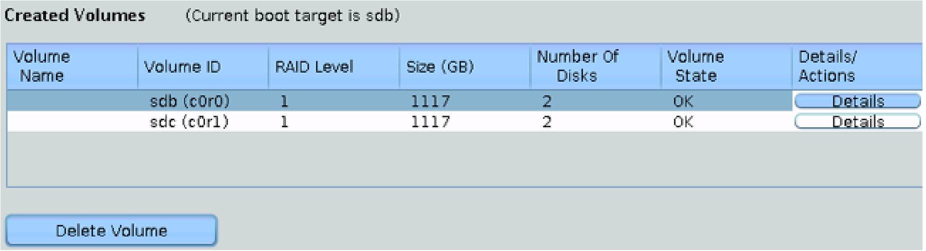
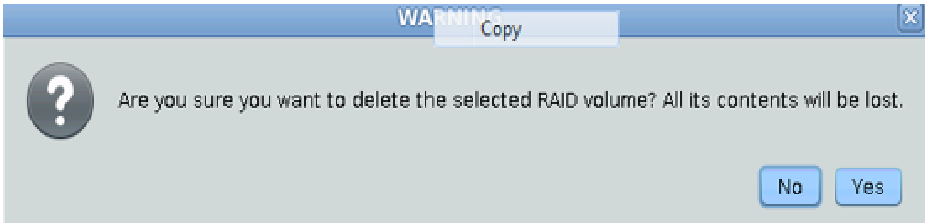
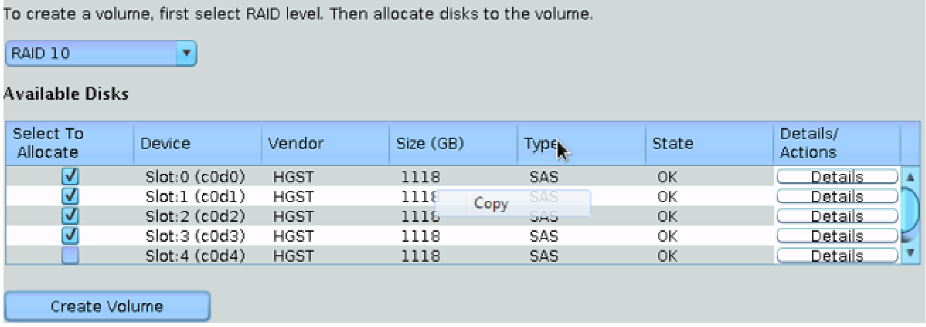


HBA: Sun Storage 12 Gb SAS PCIe RAID HBA, internal

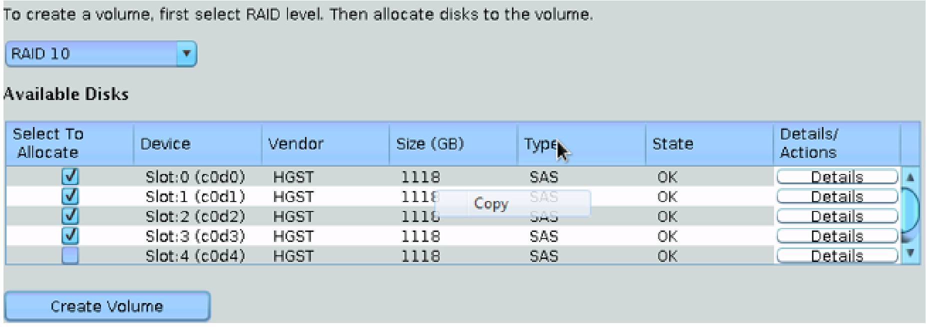
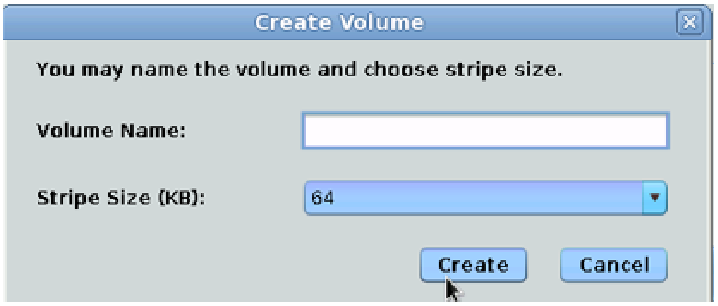
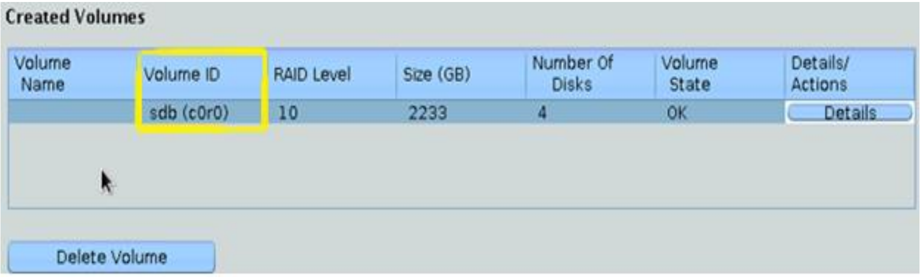
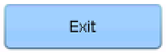
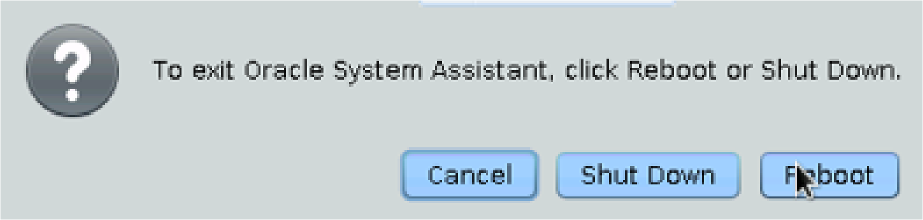
Configure Network
Get Updates
Update Firmware
Configure Hardware

</td>
</tr>
</table>

Procedure 126. RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X5-2/Netra X5-2)

5. ☐	ILOM GUI: Delete the existing volume, if it exists	1. Look under Created Volumes. If there is a volume created that does not match the configuration you want, then complete this step. 2. Click **Delete Volume**.  Created Volumes (Current boot target is sdb) Volume Name Volume ID RAID Level Size (GB) Number Of Disks Volume State Details/ Actions sdb (c0r0) 1 1117 2 OK Details sdc (c0r1) 1 1117 2 OK Details 3. Click **Yes** to confirm.  Are you sure you want to delete the selected RAID volume? All its contents will be lost. 4. Delete all the volumes.
6. ☐	**ILOM GUI**: Select RAID Level and disks	1. Click **Select RAID Level** and select **RAID 10**. 2. 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

Procedure 126. RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X5-2/Netra X5-2)

7. ☐	**ILOM GUI**: Create a volume	1. Click **Create Volume**.  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 2. Click **Create** to confirm creation. No name is needed.  Create Volume You may name the volume and choose stripe size. Volume Name: Stripe Size (KB): 64 3. Under Created Volumes, note the **Volume ID** and save this information for later. For example, in this case, the Volume ID is **sdb**.  Created Volumes Volume Name | Volume ID | RAID Level | Size (GB) | Number Of Disks | Volume State | Details/ Actions | sdb (c0r0) | 10 | 2233 | 4 | OK | Details
8. ☐	**ILOM GUI**: Exit OSA screen UI and Reboot	1. Click **Exit** in the OSA GUI.  2. Click **Reboot** on the warning screen.  To exit Oracle System Assistant, click Reboot or Shut Down. ***Note:*** Ignore the warning messages related to primary OS and storage not being available.

Procedure 127. RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2)

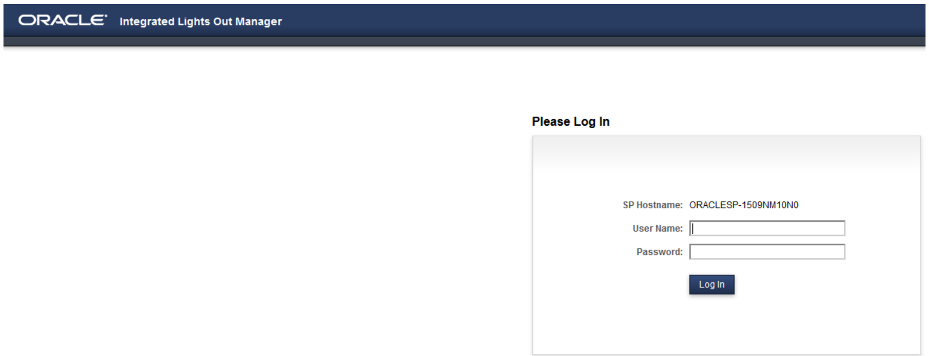
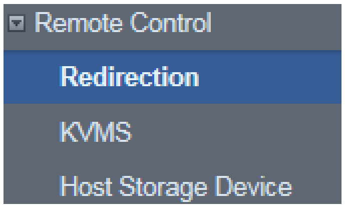
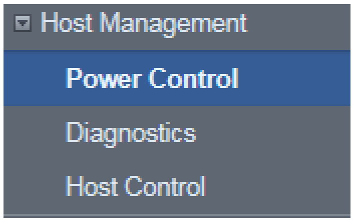
This procedure creates an HD RAID10 volume by combining multiple HDD on Oracle X6-2.

Prerequisites:

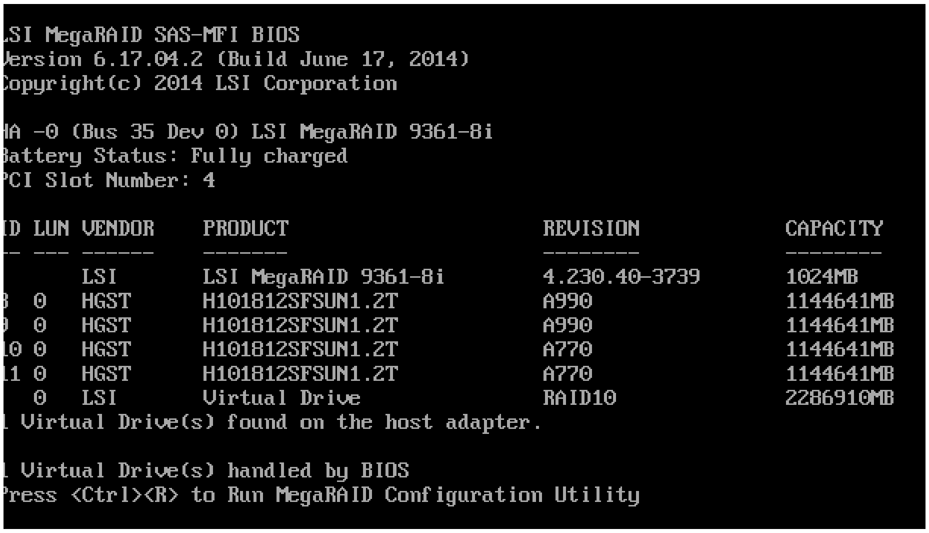
- Multiple HDD must be installed and configured on the target RMS.
- TVOE ISO USB must be inserted into USB socket.

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

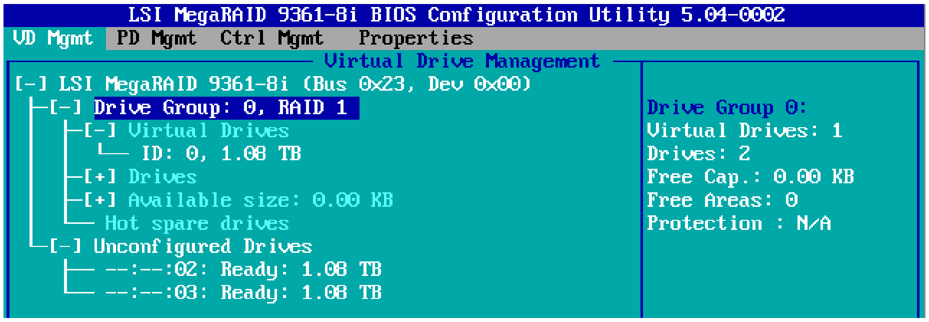
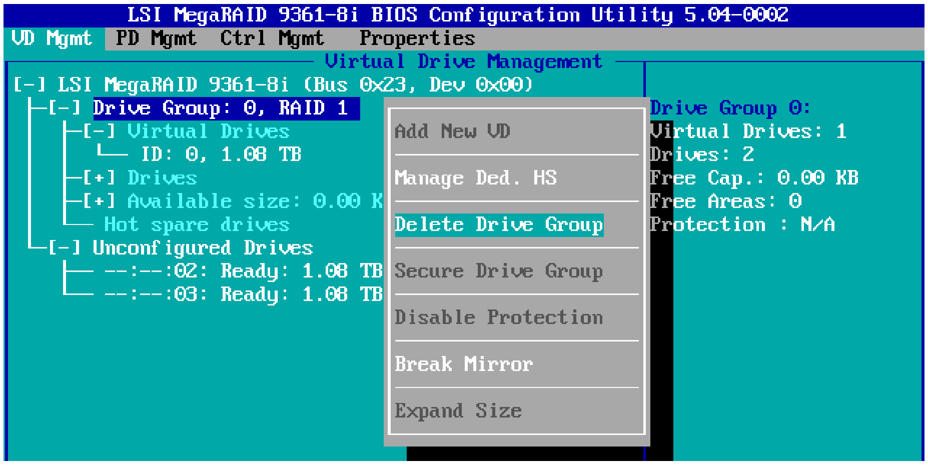
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**Oracle X6-2**: Login	Log into the Oracle rack mount server ILOM.  ORACLE Integrated Lights Out Manager Please Log In SP Hostname: ORACLESP-1509NM10N0 User Name: Password: Log In
2. ☐	**ILOM GUI**: Launch remote console	1. Navigate to Remote Control > **Redirection**.  Remote Control Redirection KVMS Host Storage Device 2. Click **Launch Remote Console**.
3. ☐	**ILOM GUI**: Power cycle server	1. Navigate to **Host Management > Power Control**.  Host Management Power Control Diagnostics Host Control 2. Select **Power Cycle** and **Save**.

Procedure 127. RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2)

4. ☐	**ILOM GUI**: Launch RAID BIOS configuration utility	Press **Ctrl+R** during the boot process to launch the BIOS Configuration Utility. The LSI MegaRAID BIOS Configuration Utility displays. 

```
SI MegaRAID SAS-MFI BIOS
ersion 6.17.04.2 (Build June 17, 2014)
opyright(c) 2014 LSI Corporation

HA -0 (Bus 35 Dev 0) LSI MegaRAID 9361-8i
attery Status: Fully charged
CI Slot Number: 4

ID LUN VENDOR    PRODUCT                      REVISION          CAPACITY
-- --- ------    --------                     --------          --------
       LSI       LSI MegaRAID 9361-8i         4.230.40-3739     1024MB
   0   HGST      H101812SFSUN1.2T             A990              1144641MB
   0   HGST      H101812SFSUN1.2T             A990              1144641MB
10 0   HGST      H101812SFSUN1.2T             A770              1144641MB
11 0   HGST      H101812SFSUN1.2T             A770              1144641MB
   0   LSI       Virtual Drive                RAID10            2286910MB
1 Virtual Drive(s) found on the host adapter.

1 Virtual Drive(s) handled by BIOS
ress <Ctrl><R> to Run MegaRAID Configuration Utility
```

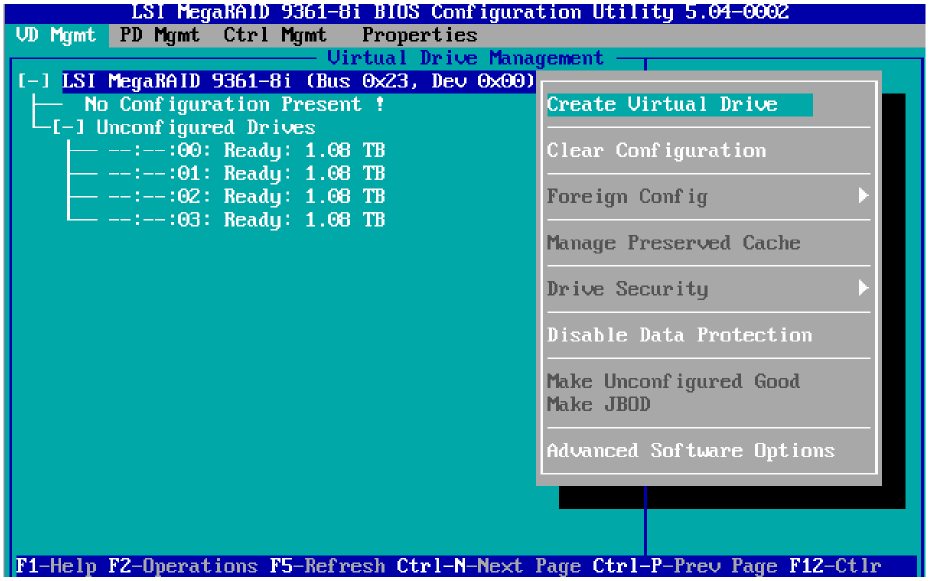
5. ☐	**ILOM GUI**: Delete the existing drive group, if it exists	1. Look under Drive Group. If there is a volume created that does not match the configuration you want, then complete this step.  2. Press **F2**. Select **Delete Drive Group**.  3. Click **Yes** to confirm.

LSI MegaRAID 9361-8i BIOS Configuration Utility 5.04-0002
VD Mgmt
PD Mgmt
Ctrl Mgmt
Properties
Virtual Drive Management

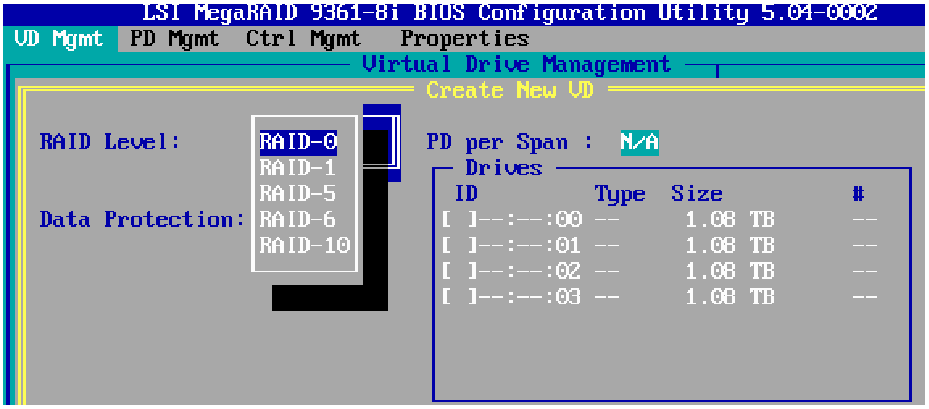
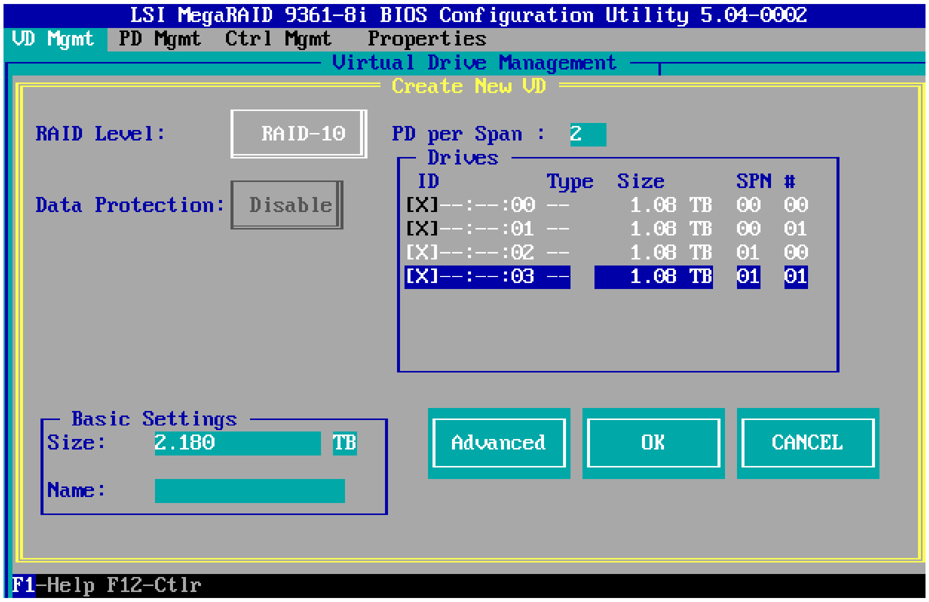
```
[-] LSI MegaRAID 9361-8i (Bus 0x23, Dev 0x00)
  ├[-] Drive Group: 0, RAID 1
  │  ├[-] Virtual Drives
  │  │   └── ID: 0, 1.08 TB
  │  ├[+] Drives
  │  ├[+] Available size: 0.00 KB
  │  └── Hot spare drives
  └[-] Unconfigured Drives
     ├── --:--:02: Ready: 1.08 TB
     └── --:--:03: Ready: 1.08 TB

Drive Group 0:
Virtual Drives: 1
Drives: 2
Free Cap.: 0.00 KB
Free Areas: 0
Protection : N/A
```

LSI MegaRAID 9361-8i BIOS Configuration Utility 5.04-0002
VD Mgmt
PD Mgmt
Ctrl Mgmt
Properties
Virtual Drive Management
Add New VD
Manage Ded. HS
Delete Drive Group
Secure Drive Group
Disable Protection
Break Mirror
Expand Size

Procedure 127. RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2)

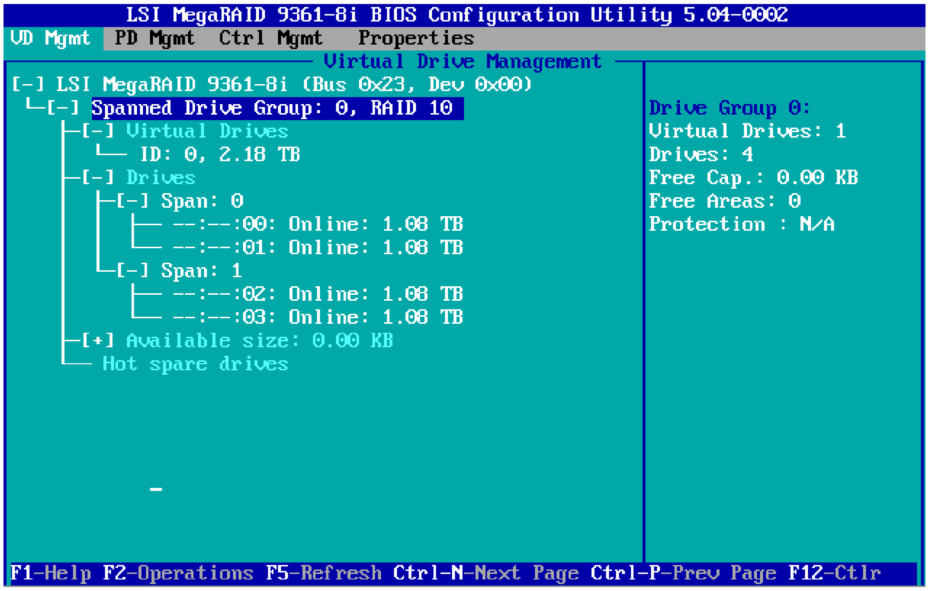
6. ☐	**ILOM GUI**: Create virtual drive	1. Select the MegaRAID item and press **F2**.  LSI MegaRAID 9361-8i BIOS Configuration Utility 5.04-0002 VD Mgmt PD Mgmt Ctrl Mgmt Properties Virtual Drive Management [-] LSI MegaRAID 9361-8i (Bus 0x23, Dev 0x00) No Configuration Present ! [-] Unconfigured Drives --:--:00: Ready: 1.08 TB --:--:01: Ready: 1.08 TB --:--:02: Ready: 1.08 TB --:--:03: Ready: 1.08 TB Create Virtual Drive Clear Configuration Foreign Config Manage Preserved Cache Drive Security Disable Data Protection Make Unconfigured Good Make JBOD Advanced Software Options F1-Help F2-Operations F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr 2. Select **Create Virtual Drive**.

Procedure 127. RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2)

7. ☐	**ILOM GUI**: Select RAID level and assign drives	1. Select **RAID-10** as the Raid Level.  LSI MegaRAID 9361-8i BIOS Configuration Utility 5.04-0002 VD Mgmt PD Mgmt Ctrl Mgmt Properties Virtual Drive Management Create New VD RAID-0 RAID-1 RAID-5 RAID-6 RAID-10 RAID Level: Data Protection: PD per Span : N/A Drives ID Type Size # [ ]--:--:00 -- 1.08 TB -- [ ]--:--:01 -- 1.08 TB -- [ ]--:--:02 -- 1.08 TB -- [ ]--:--:03 -- 1.08 TB -- 2. For each drive you want in the logical drive, navigate to the drive and press **Enter** in its ID field to display an X in the field.  LSI MegaRAID 9361-8i BIOS Configuration Utility 5.04-0002 VD Mgmt PD Mgmt Ctrl Mgmt Properties Virtual Drive Management Create New VD Advanced OK CANCEL F1-Help F12-Ctlr RAID Level: RAID-10 Data Protection: Disable PD per Span : 2 Drives ID Type Size SPN # [X]--:--:00 -- 1.08 TB 00 00 [X]--:--:01 -- 1.08 TB 00 01 [X]--:--:02 -- 1.08 TB 01 00 [X]--:--:03 -- 1.08 TB 01 01 Basic Settings Size: 2.180 TB Name: 3. Navigate to **OK**, press **Enter**, and click **OK**.

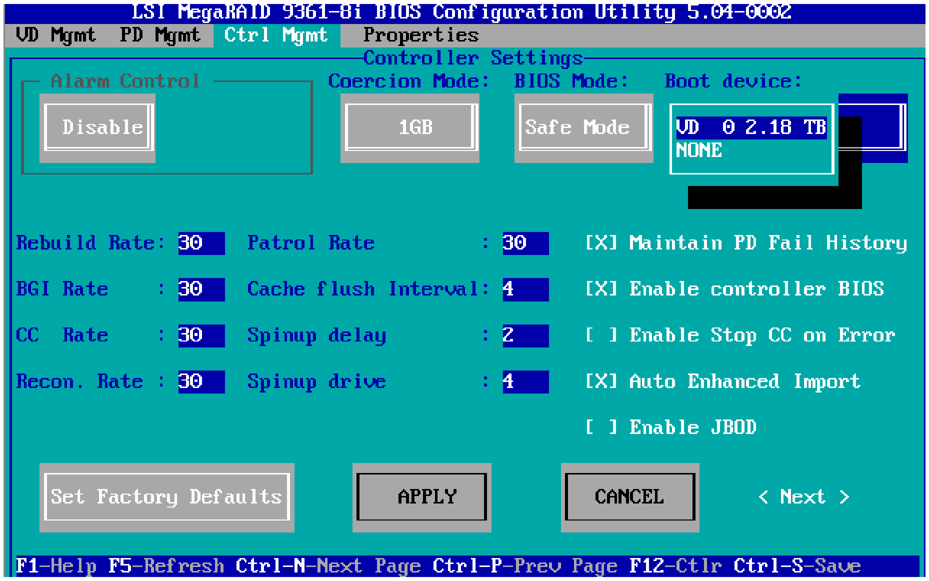
Procedure 127. RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2)

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 displayed on the page.



```
         LSI MegaRAID 9361-8i BIOS Configuration Utility 5.04-0002
VD Mgmt  PD Mgmt  Ctrl Mgmt   Properties
                      Virtual Drive Management
[-] LSI MegaRAID 9361-8i (Bus 0x23, Dev 0x00)
 └[-] Spanned Drive Group: 0, RAID 10                 Drive Group 0:
    ├[-] Virtual Drives                               Virtual Drives: 1
    │  └── ID: 0, 2.18 TB                             Drives: 4
    ├[-] Drives                                       Free Cap.: 0.00 KB
    │ ├[-] Span: 0                                    Free Areas: 0
    │ │  ├── --:--:00: Online: 1.08 TB                Protection : N/A
    │ │  └── --:--:01: Online: 1.08 TB
    │ └[-] Span: 1
    │    ├── --:--:02: Online: 1.08 TB
    │    └── --:--:03: Online: 1.08 TB
    ├[+] Available size: 0.00 KB
    └── Hot spare drives

            -

F1-Help F2-Operations F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr
```

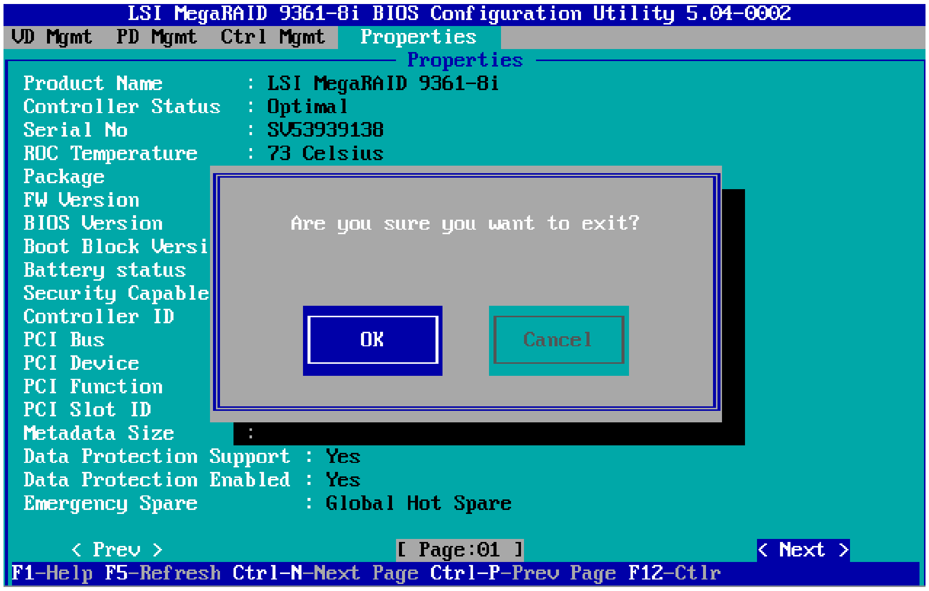
9. ☐	ILOM GUI: Make drive bootable	1. Press **Ctrl + N** twice to select Ctrl Mgmt. 2. Navigate to the **Boot device** and press **Enter**. 3. Select the drive to make it bootable.



```
         LSI MegaRAID 9361-8i BIOS Configuration Utility 5.04-0002
 VD Mgmt  PD Mgmt  Ctrl Mgmt  Properties
                       Controller Settings
  Alarm Control            Coercion Mode:  BIOS Mode:   Boot device:
   Disable                   1GB          Safe Mode    VD  0 2.18 TB
                                                       NONE

Rebuild Rate: 30   Patrol Rate         : 30   [X] Maintain PD Fail History
BGI Rate     : 30   Cache flush Interval: 4    [X] Enable controller BIOS
CC  Rate     : 30   Spinup delay        : 2    [ ] Enable Stop CC on Error
Recon. Rate  : 30   Spinup drive        : 4    [X] Auto Enhanced Import
                                               [ ] Enable JBOD

  Set Factory Defaults      APPLY        CANCEL       < Next >

F1-Help F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr Ctrl-S-Save
```

4. Navigate to **Apply** and press **Enter**.
5. Press **CTRL+S** to save the configuration.

Procedure 127. RAID10 Logical Volume Creation Spanning Multiple HDDs (Oracle X6-2)

10. ☐	**ILOM GUI**: Exit configuration	Press **Esc** and click **OK**. 

```
         LSI MegaRAID 9361-8i BIOS Configuration Utility 5.04-0002
VD Mgmt  PD Mgmt  Ctrl Mgmt  Properties
                                       Properties
 Product Name          : LSI MegaRAID 9361-8i
 Controller Status     : Optimal
 Serial No             : SV53939138
 ROC Temperature       : 73 Celsius
 Package
 FW Version
 BIOS Version                   Are you sure you want to exit?
 Boot Block Versi
 Battery status
 Security Capable
 Controller ID                     OK              Cancel
 PCI Bus
 PCI Device
 PCI Function
 PCI Slot ID
 Metadata Size      :
 Data Protection Support : Yes
 Data Protection Enabled : Yes
 Emergency Spare         : Global Hot Spare

      < Prev >                      [ Page:01 ]                    < Next >
F1-Help F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr
```

11. ☐	**ILOM GUI**: Reboot	Press **Ctl + Alt + Delete** to reboot. ***Note:*** Volume ID for X6-2 is: sda. This is used when installing TVOE.

Procedure 128. RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380)

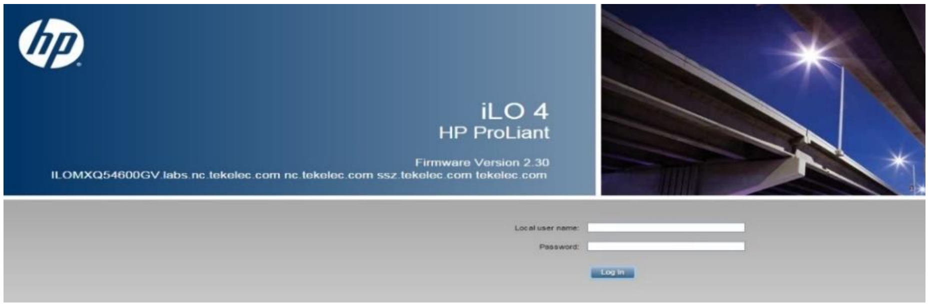
This procedure creates an HD RAID10 volume by combining multiple HDD on HP DL380 Gen 9.

Prerequisites:

- 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.

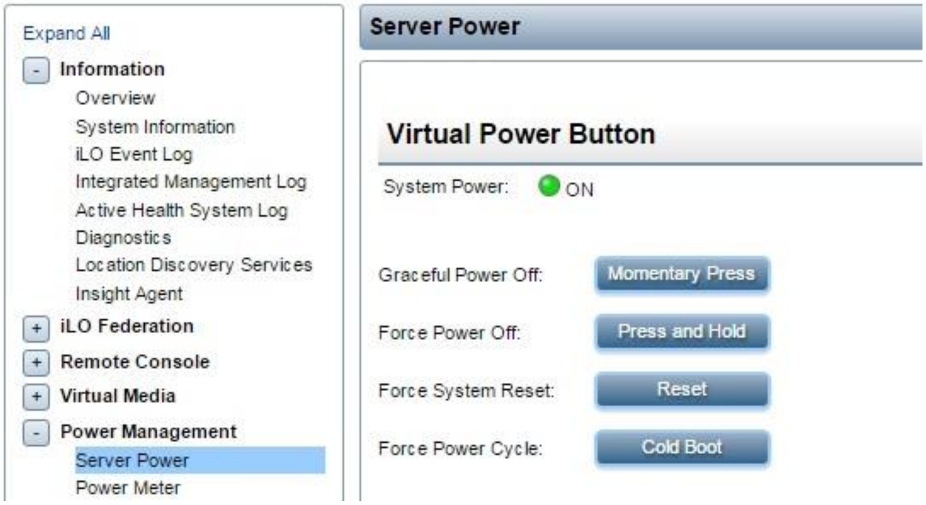
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. ☐	**HP Gen 9**: Log into the ILOM GUI	Log into the HP rack mount server ILOM. 

iLO 4
HP ProLiant
Firmware Version 2.30
ILOMXQ54600GV.labs.nc.tekelec.com nc.tekelec.com ssz.tekelec.com tekelec.com
Local user name:
Password:
Log In

Procedure 128. RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380)

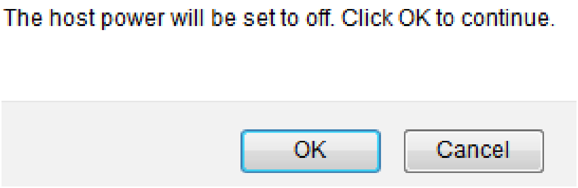
<table>
<tr>
<td>2.
☐</td>
<td>**ILOM GUI**: Turn off the power</td>
<td>
1. Navigate to **Power Management > Server Power**.


Expand All
Information
Overview
System Information
iLO Event Log
Integrated Management Log
Active Health System Log
Diagnostics
Location Discovery Services
Insight Agent
iLO Federation
Remote Console
Virtual Media
Power Management
Server Power
Power Meter
Server Power
Virtual Power Button
Graceful Power Off:
Momentary Press
Force Power Off:
Press and Hold
Force System Reset:
Reset
Force Power Cycle:
Cold Boot

System Power: ● ON

2. From the Virtual Power Button, click **Momentary Press** for graceful power off.

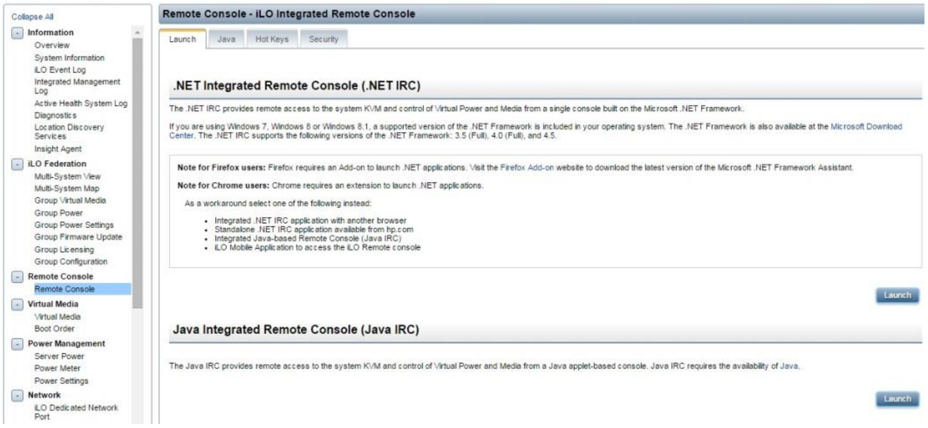
3. Click **OK** to confirm.



The host power will be set to off. Click OK to continue.

</td>
</tr>
<tr>
<td>3.
☐</td>
<td>**ILOM GUI**: Launch HP iLO Integrated Remote Console</td>
<td>
1. Navigate to **Remote Console > Remote Console**.

2. Click **Launch**.


Collapse All
Information
Overview
System Information
iLO Event Log
Integrated Management Log
Active Health System Log
Diagnostics
Location Discovery Services
Insight Agent
iLO Federation
Multi-System View
Multi-System Map
Group Virtual Media
Group Power
Group Power Settings
Group Firmware Update
Group Licensing
Group Configuration
Remote Console
Remote Console
Virtual Media
Virtual Media
Boot Order
Power Management
Server Power
Power Meter
Power Settings
Network
iLO Dedicated Network Port
Remote Console - iLO Integrated Remote Console
Launch
Java
Hot Keys
Security

.NET Integrated Remote Console (.NET IRC)

The .NET IRC provides remote access to the system KVM and control of Virtual Power and Media from a single console built on the Microsoft .NET Framework.

If you are using Windows 7, Windows 8 or Windows 8.1, a supported version of the .NET Framework is included in your operating system. The .NET Framework is also available at the Microsoft Download Center. The .NET IRC supports the following versions of the .NET Framework: 3.5 (Full), 4.0 (Full), and 4.5.

Note for Firefox users: Firefox requires an Add-on to launch .NET applications. Visit the Firefox Add-on website to download the latest version of the Microsoft .NET Framework Assistant.

Note for Chrome users: Chrome requires an extension to launch .NET applications.

As a workaround select one of the following instead:

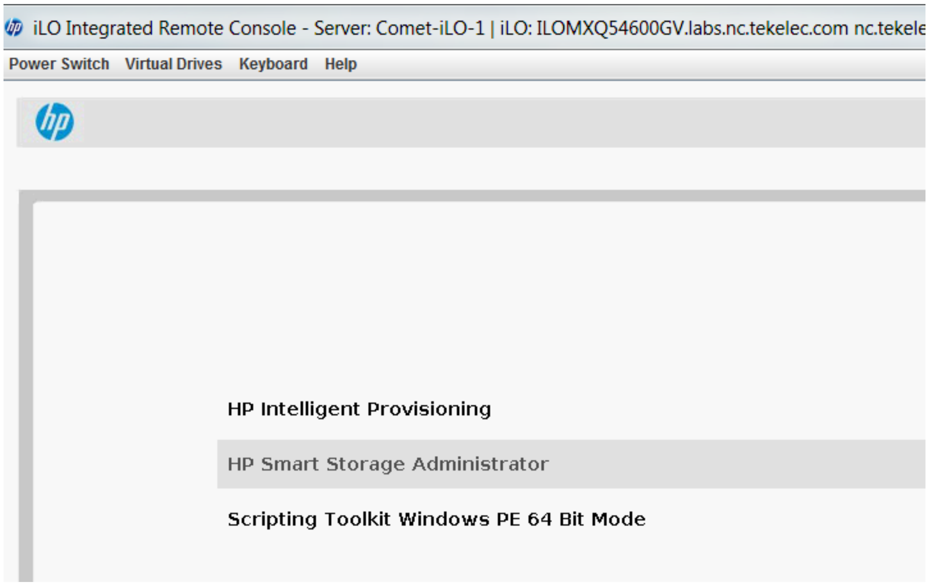
- Integrated .NET IRC application with another browser
- Standalone .NET IRC application available from hp.com
- Integrated Java-based Remote Console (Java IRC)
- iLO Mobile Application to access the iLO Remote console

Java Integrated Remote Console (Java IRC)

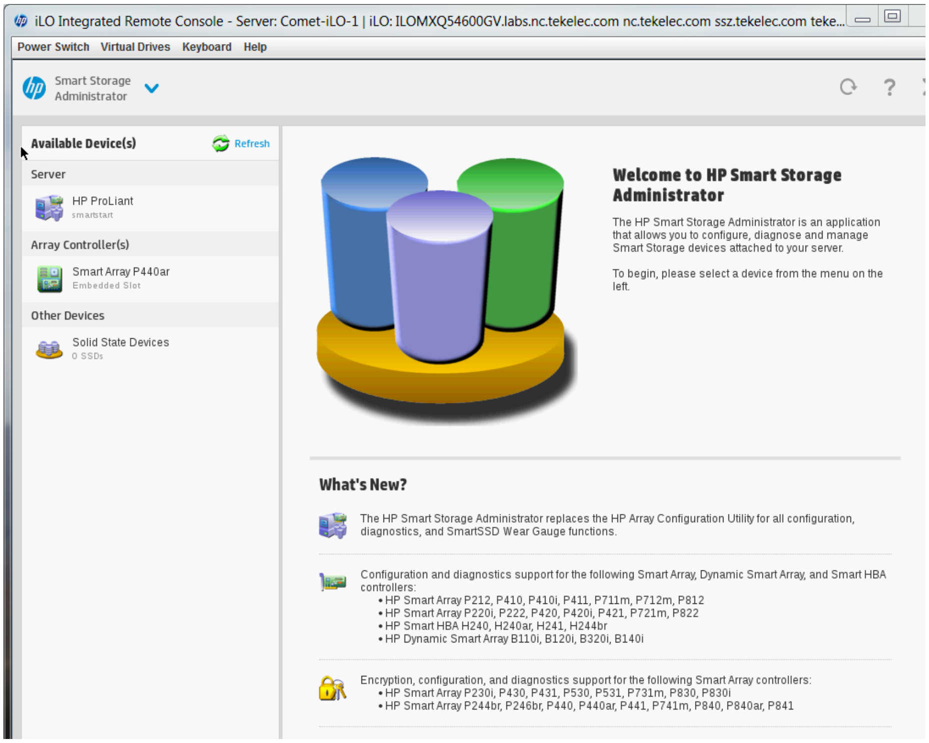
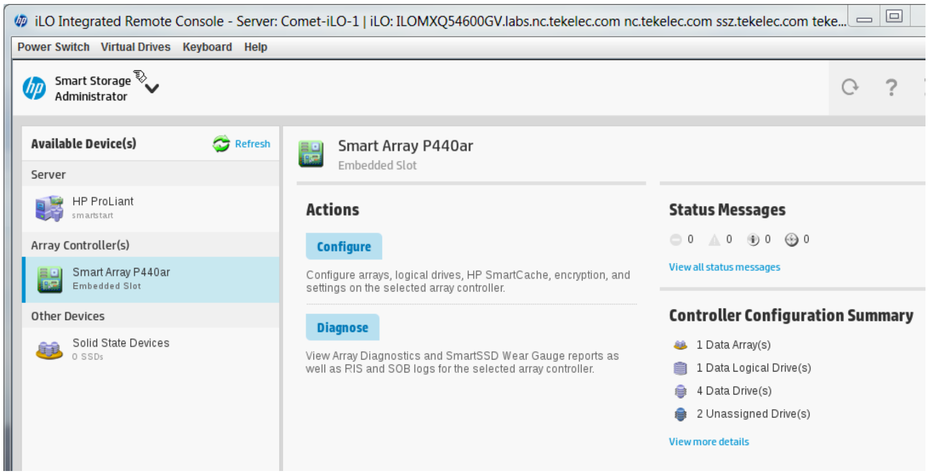
The Java IRC provides remote access to the system KVM and control of Virtual Power and Media from a Java applet-based console. Java IRC requires the availability of Java.

</td>
</tr>
</table>

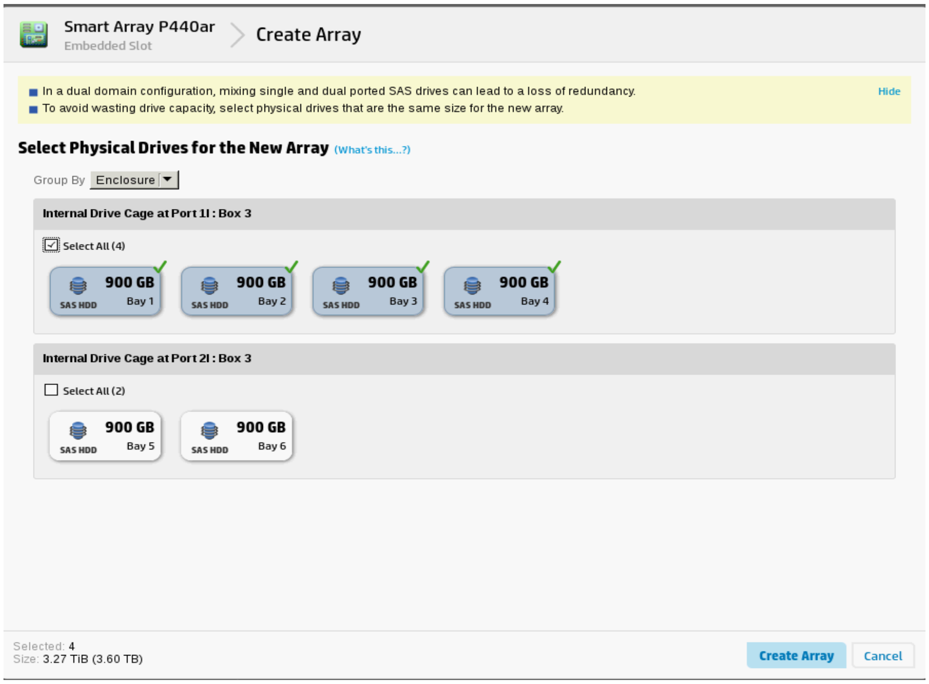
Procedure 128. RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380)

4. ☐	**ILOM GUI**: Access HP Intelligent Provisioning/ HP Smart Storage Administrator	1. Enter into the **HP Intelligent Provisioning** by pressing **F10** during boot up. 2. Enter **HP Smart Storage Administrator**.  iLO Integrated Remote Console - Server: Comet-iLO-1 | iLO: ILOMXQ54600GV.labs.nc.tekelec.com nc.tekele Power Switch Virtual Drives Keyboard Help HP Intelligent Provisioning HP Smart Storage Administrator Scripting Toolkit Windows PE 64 Bit Mode

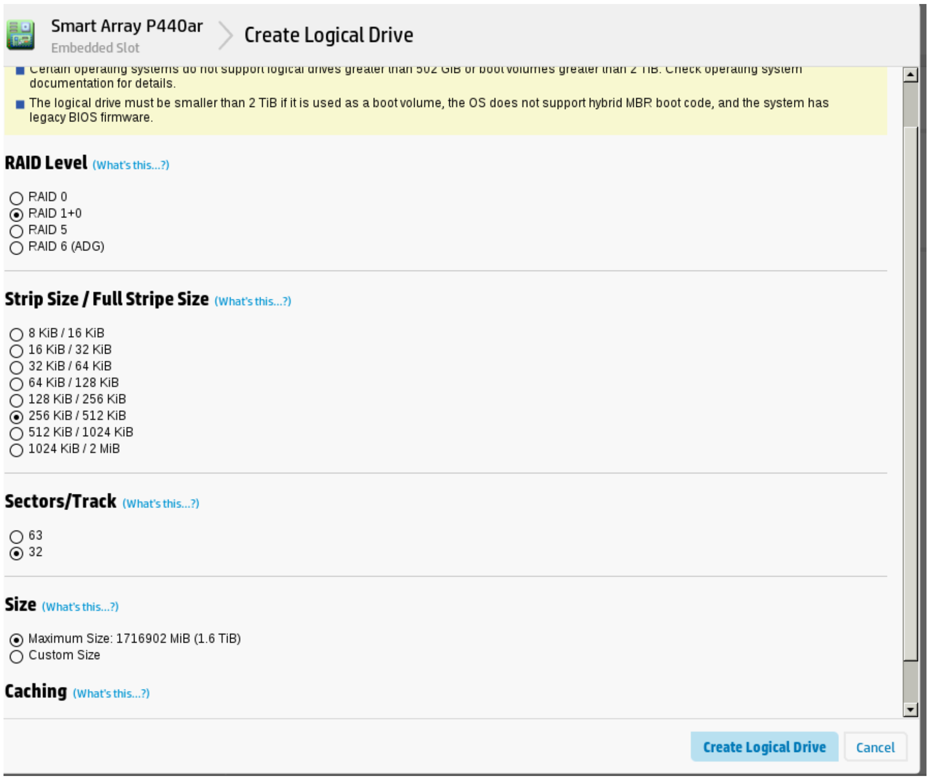
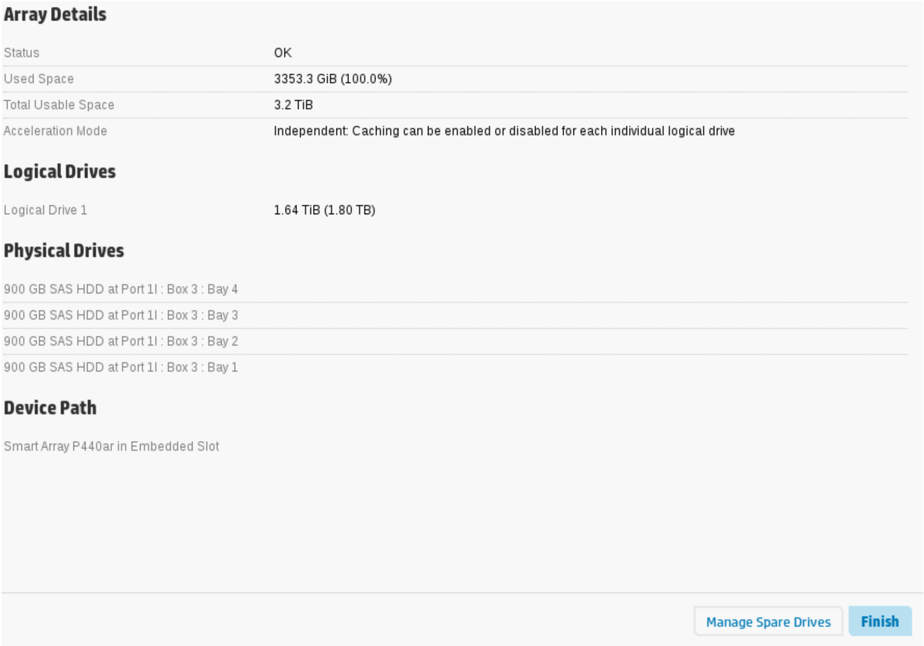
Procedure 128. RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380)

5. ☐	**ILOM GUI**: Configure array controllers	1. Click **Smart Array P440ar**. iLO Integrated Remote Console - Server: Comet-iLO-1 | iLO: ILOMXQ54600GV.labs.nc.tekelec.com nc.tekelec.com ssz.tekelec.com teke... Power Switch Virtual Drives Keyboard Help Smart Storage Administrator Available Device(s) Refresh Server HP ProLiant smartstart Array Controller(s) Smart Array P440ar Embedded Slot Other Devices Solid State Devices 0 SSDs Welcome to HP Smart Storage Administrator The HP Smart Storage Administrator is an application that allows you to configure, diagnose and manage Smart Storage devices attached to your server. To begin, please select a device from the menu on the left. What's New? The HP Smart Storage Administrator replaces the HP Array Configuration Utility for all configuration, diagnostics, and SmartSSD Wear Gauge functions. Configuration and diagnostics support for the following Smart Array, Dynamic Smart Array, and Smart HBA controllers: • HP Smart Array P212, P410, P410i, P411, P711m, P712m, P812 • HP Smart Array P220i, P222, P420, P420i, P421, P721m, P822 • HP Smart HBA H240, H240ar, H241, H244br • HP Dynamic Smart Array B110i, B120i, B320i, B140i Encryption, configuration, and diagnostics support for the following Smart Array controllers: • HP Smart Array P230i, P430, P431, P530, P531, P731m, P830, P830i • HP Smart Array P244br, P246br, P440, P440ar, P441, P741m, P840, P840ar, P841 2. Click **Configure**. iLO Integrated Remote Console - Server: Comet-iLO-1 | iLO: ILOMXQ54600GV.labs.nc.tekelec.com nc.tekelec.com ssz.tekelec.com teke... Power Switch Virtual Drives Keyboard Help Smart Storage Administrator Available Device(s) Refresh Server HP ProLiant smartstart Array Controller(s) Smart Array P440ar Embedded Slot Other Devices Solid State Devices 0 SSDs Smart Array P440ar Embedded Slot Actions Configure Configure arrays, logical drives, HP SmartCache, encryption, and settings on the selected array controller. Diagnose View Array Diagnostics and SmartSSD Wear Gauge reports as well as RIS and SOB logs for the selected array controller. Status Messages 0 0 0 0 View all status messages Controller Configuration Summary 1 Data Array(s) 1 Data Logical Drive(s) 4 Data Drive(s) 2 Unassigned Drive(s) View more details

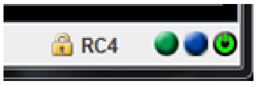
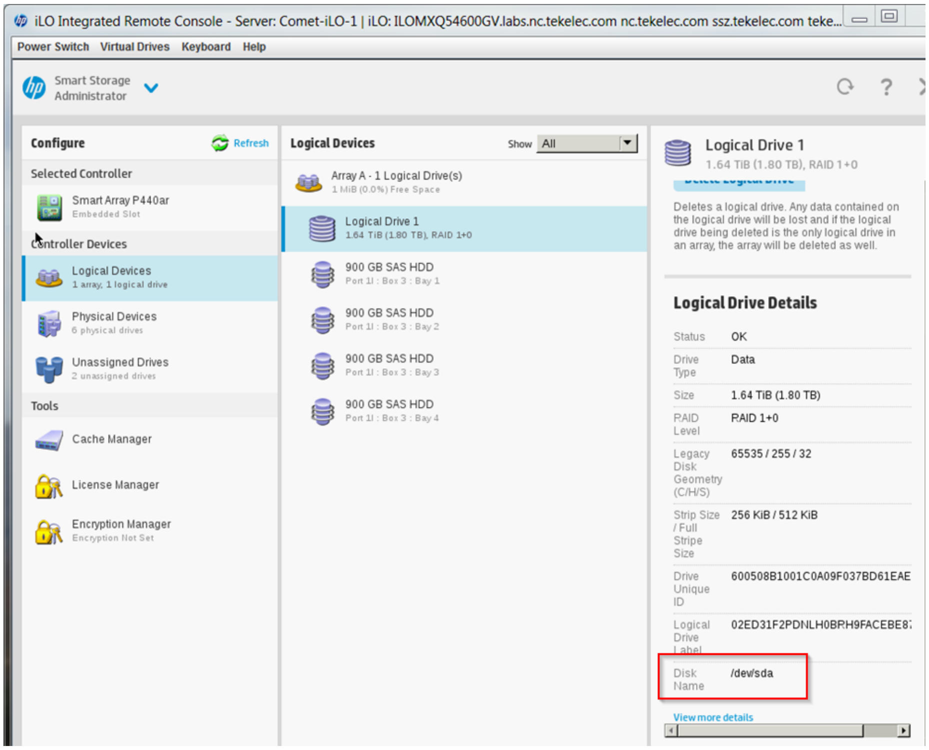
Procedure 128. RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380)

6. ☐	**ILOM GUI**: Create new array	Select 4 physical drives and click **Create Array**.  In a dual domain configuration, mixing single and dual ported SAS drives can lead to a loss of redundancy. To avoid wasting drive capacity, select physical drives that are the same size for the new array. Selected: 4 Size: 3.27 TiB (3.60 TB) Smart Array P440ar Embedded Slot Create Array Hide Select Physical Drives for the New Array (What's this...?) Group By Enclosure Internal Drive Cage at Port 1I : Box 3 ☑ Select All (4) 900 GB SAS HDD Bay 1 ✓ 900 GB SAS HDD Bay 2 ✓ 900 GB SAS HDD Bay 3 ✓ 900 GB SAS HDD Bay 4 ✓ Internal Drive Cage at Port 2I : Box 3 ☐ Select All (2) 900 GB SAS HDD Bay 5 900 GB SAS HDD Bay 6 Create Array Cancel

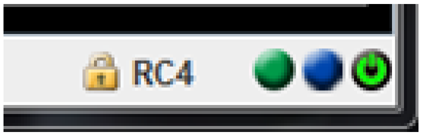
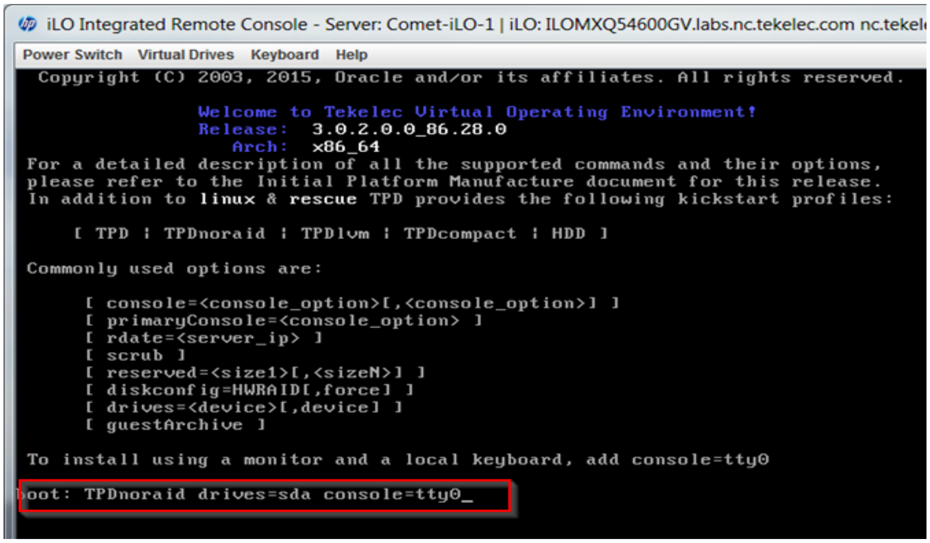
Procedure 128. RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380)

7. ☐	**ILOM GUI**: RAID 10 logical volume creation	1. Select RAID Level as **RAID1+0**, leave the rest as defaults, and click **Create Logical Drive**.  Smart Array P440ar Embedded Slot Create Logical Drive - Certain operating systems do not support logical drives greater than 502 GiB or boot volumes greater than 2 TiB. Check operating system documentation for details. - The logical drive must be smaller than 2 TiB if it is used as a boot volume, the OS does not support hybrid MBR boot code, and the system has legacy BIOS firmware. **RAID Level** (What's this...?) ○ RAID 0 ● RAID 1+0 ○ RAID 5 ○ RAID 6 (ADG) **Strip Size / Full Stripe Size** (What's this...?) ○ 8 KiB / 16 KiB ○ 16 KiB / 32 KiB ○ 32 KiB / 64 KiB ○ 64 KiB / 128 KiB ○ 128 KiB / 256 KiB ● 256 KiB / 512 KiB ○ 512 KiB / 1024 KiB ○ 1024 KiB / 2 MiB **Sectors/Track** (What's this...?) ○ 63 ● 32 **Size** (What's this...?) ● Maximum Size: 1716902 MiB (1.6 TiB) ○ Custom Size **Caching** (What's this...?) Create Logical Drive Cancel 2. Click **Finish**.  **Array Details** Status: OK Used Space: 3353.3 GiB (100.0%) Total Usable Space: 3.2 TiB Acceleration Mode: Independent: Caching can be enabled or disabled for each individual logical drive **Logical Drives** Logical Drive 1: 1.64 TiB (1.80 TB) **Physical Drives** 900 GB SAS HDD at Port 1I : Box 3 : Bay 4 900 GB SAS HDD at Port 1I : Box 3 : Bay 3 900 GB SAS HDD at Port 1I : Box 3 : Bay 2 900 GB SAS HDD at Port 1I : Box 3 : Bay 1 **Device Path** Smart Array P440ar in Embedded Slot Manage Spare Drives Finish

Procedure 128. RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380)

8. ☐	**ILOM GUI**: Restart the server	Restart the server by clicking the power button at the bottom right corner of the window. 
9. ☐	ILOM GUI	Repeat step 4. to get into the Smart Storage Administrator screen.
10. ☐	**ILOM GUI**: Select the created logical drive	1. Click on the **Logical Devices** under the Controller Devices and select **Logical Drive 1**. 2. Note the **Disk Name**. For example, **/dev/sda**. This is used in the next step.  iLO Integrated Remote Console - Server: Comet-iLO-1 | iLO: ILOMXQ54600GV.labs.nc.tekelec.com nc.tekelec.com ssz.tekelec.com teke... Logical Drive 1 1.64 TiB (1.80 TB), RAID 1+0 Deletes a logical drive. Any data contained on the logical drive will be lost and if the logical drive being deleted is the only logical drive in an array, the array will be deleted as well. Logical Drive Details Status OK Drive Type Data Size 1.64 TiB (1.80 TB) RAID Level RAID 1+0 Legacy Disk Geometry (C/H/S) 65535 / 255 / 32 Strip Size / Full Stripe Size 256 KiB / 512 KiB Drive Unique ID 600508B1001C0A09F037BD61EAE Logical Drive Label 02ED31F2PDNLH0BRH9FACEBE8 Disk Name /dev/sda Power Switch Virtual Drives Keyboard Help Smart Storage Administrator Configure Refresh Selected Controller Smart Array P440ar Embedded Slot Controller Devices Logical Devices 1 array, 1 logical drive Physical Devices 6 physical drives Unassigned Drives 2 unassigned drives Tools Cache Manager License Manager Encryption Manager Encryption Not Set Logical Devices Show All Array A - 1 Logical Drive(s) 1 MiB (0.0%) Free Space Logical Drive 1 1.64 TiB (1.80 TB), RAID 1+0 900 GB SAS HDD Port 1I : Box 3 : Bay 1 900 GB SAS HDD Port 1I : Box 3 : Bay 2 900 GB SAS HDD Port 1I : Box 3 : Bay 3 900 GB SAS HDD Port 1I : Box 3 : Bay 4 View more details

Procedure 128. RAID10 Logical Volume Creation Spanning Multiple HDDs (HP DL380)

11. ☐	**ILOM GUI**: Reboot the server	1. Reboot the server by clicking the power button icon at the bottom right hand corner.  2. When prompted, provide correct **Disk Name** (noted in step 10.) and press **Enter**.  iLO Integrated Remote Console - Server: Comet-iLO-1 | iLO: ILOMXQ54600GV.labs.nc.tekelec.com nc.tekel Power Switch Virtual Drives Keyboard Help

```
 Copyright (C) 2003, 2015, Oracle and/or its affiliates. All rights reserved.

                Welcome to Tekelec Virtual Operating Environment!
                Release:   3.0.2.0.0_86.28.0
                   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 | TPDnoraid | TPDlvm | 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

oot: TPDnoraid drives=sda console=tty0_
```

Appendix Q.2 Non-HA Lab Node PMAC Deployment

This section deploys PMAC, creates VMs, and provides CPU, RAM, and hard disk information to override the default values when importing a profile while creating a VM.

Procedure 129. PMAC Deployment: Deviation

This procedure deploys PMAC on the TVOE host. ***Prerequisites***: Completed first RMS network configuration (PMAC host). ***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 My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC TVOE iLO/iLOM**: Login and start the integrated remote console	Log into iLO/iLOM and follow Appendix D TVOE iLO/iLOM GUI Access to access the iLO/iLOM GUI. `https://<management_server_iLO_ip>`

Procedure 129. PMAC Deployment: Deviation

2. ☐	**TVOE iLO/iLOM**: Mount the PMAC media to the TVOE server	Use one of the following two options to mount the PMAC media:

Option 1:

1. If using a USB media, insert the PMAC USB into a USB port and execute this command to mount the ISO.

```
$ ls /media/*/*.iso
/media/sdd1/872-2586-101-5.7.0_57.3.0-PM&C-x86_64.iso
```

2. Use the output of the previous command to populate the next command.

```
$ sudo mount -o loop /media/sdd1/872-2586-101-
5.7.0_57.3.0-PM&C-x86_64.iso /mnt/upgrade
```

Option 2

1. If using an ISO image, run this to mount it.

```
$ sudo mount -o loop ISO_FILENAME.iso /mnt/upgrade
```

2. Validate the PMAC media.

```
$ cd /mnt/upgrade/upgrade
$ .validate/validate_cd
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
```

Note: If the media validation fails, the media is not valid and should not be used.

Procedure 129. PMAC Deployment: Deviation

3. ☐	**TVOE iLO/iLOM**: Deploy PMAC	1. Using the PMAC-deploy script, deploy the PMAC instance using the configuration captured during the site survey.

```
$ cd /mnt/upgrade/upgrade
```

2. If deploying PMAC without the NetBackup feature, run this command:

```
$ 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
```

If deploying PMAC with NetBackup feature, run the following command:

```
$ 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
```

The PMAC deploys and boots. The management and control network displays based on the settings provided to the PMAC-deploy script.

Note: This step takes between 5 and 10 minutes.

4. ☐	**TVOE iLO/iLOM**: Unmount the media	1. The media should auto-unmount, if it does not, unmount the media.

```
$ cd /
$ sudo /bin/umount /mnt/upgrade
```

2. Remove the media from the drive.

Procedure 129. PMAC Deployment: Deviation

5. ☐ **TVOE iLO/iLOM**: SSH into the management server

1. Using an SSH client such as putty, ssh to the TVOE host as **admusr**.
2. Login using **virsh** and wait until you see the login prompt.

```
$ sudo /usr/bin/virsh list
Id  Name  State
----------------------------------
2   PM&C  running
```

```
$ 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.
PM&Cdev7 login:
```

6. ☐ **Virtual PMAC**: Verify the PMAC is configured correctly on first boot

1. Establish an SSH session to the PMAC and login as **admusr**.
2. Run this command (there should be no output).

```
$ sudo /bin/ls /usr/TKLC/plat/etc/deployment.d/
```

7. ☐ **TVOE iLO/iLOM**: Error doing verification, if error is outputted

If an error displays, delete the PMAC guest and re-deploy the guest again:

```
$ sudo guestMgr --remove <PMAC_Name>
```

8. ☐ **Virtual PMAC**: Set the PMAC time zone

Note: Valid time zones can be found in Appendix J List of Frequently Used Time Zones.

1. Run:

```
$ sudo set_pmac_tz.pl <time zone>
```

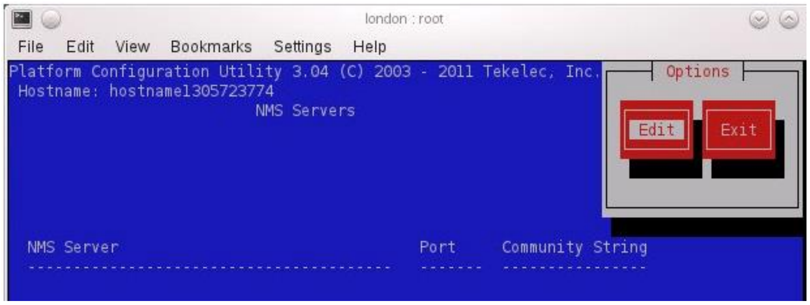
Example:

```
$ sudo set_pmac_tz.pl America/New_York
```

2. Verify the time zone has been updated.

```
$ sudo date
```

Procedure 129. PMAC Deployment: Deviation

9.
☐
	Virtual PMAC:
	Set SNMP
		1. Enter the platcfg menu.
		`$ sudo su – platcfg`
		2. Navigate to **Network Configuration > SNMP Configuration > NMS Configuration**.
		 london : root
		File Edit View Bookmarks Settings Help
		Options
		Edit
		Exit`Platform Configuration Utility 3.04 (C) 2003 - 2011 Tekelec, Inc.`
		`Hostname: hostname1305723774`
		`NMS Servers`
		`NMS Server                               Port     Community String`
		`-------------------------------------   -------  ---------------`
		3. Select **Edit** > **Add a New NMS Server**.
		4. Enter all the information to complete the form about the SNMP trap destination.
		Refer to Appendix H SNMP Configuration for more information.
		5. Click **OK** to finalize the configuration.
		6. Click **Exit**.
		7. Click **Yes** and wait until the Alarm Routing Service restarts.
		8. Exit out of platcfg by selecting **Exit**.

10. ☐	**Virtual PMAC**: Reboot the server	`$ sudo init 6`

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_SEESION_MEM="16384"	DSR_VIRT_SBR_SESSION_VDISK="71680"

CPU	**MEMORY**	**VDISK**
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

Procedure 130. iDIH Installation: Deviation

This procedure installs and configures iDIH.

Prerequisites: 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 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. through 4.

1. Add the application ISO images (Mediation, Application, and OracleGuest) to the PMAC using one of these methods:
   - Insert the CD containing the IDIH media into the removable media drive.
   - Attach the USB device containing the ISO to a USB port.
   - Copy the Application ISO file to the PMAC server into the **/var/TKLC/smac/image/isoimages/home/smacftpusr/** directory as pmacftpusr user:

     cd to the directory where your ISO image is located on the TVOE Host (not on the PMAC server).
2. Using sftp, connect to the PMAC server.

```
$ sftp pmacftpusr@<pmac_management_network_ip>
$ put <image>.iso
```

3. After the image transfer is 100% complete, close the connection.

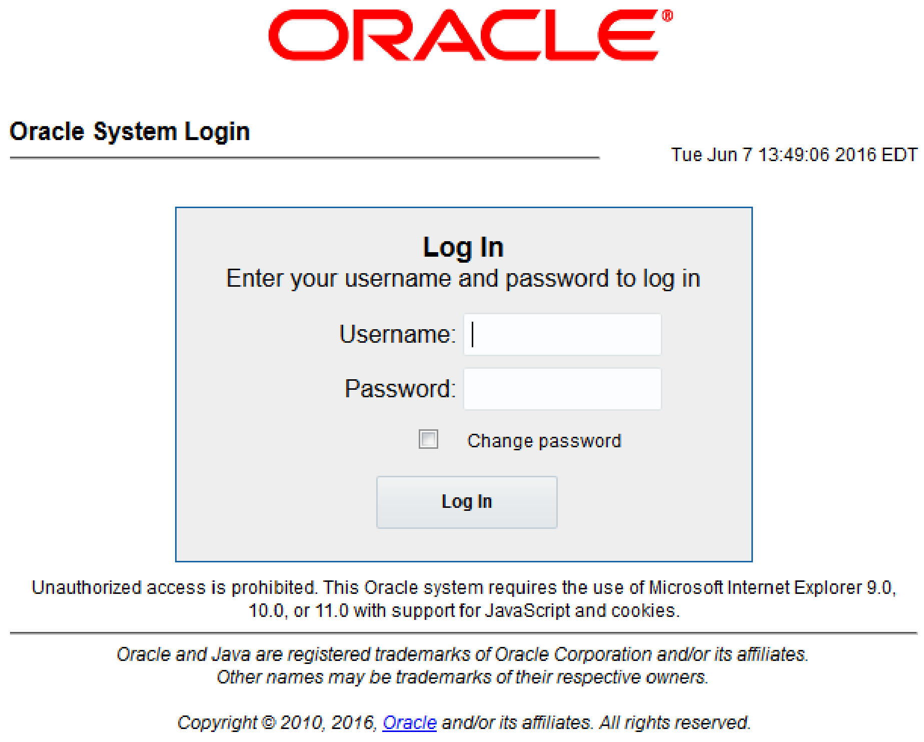
```
$ quit
```

Procedure 130. iDIH Installation: Deviation

<table>
<tr>
<td>2.
☐</td>
<td>PMAC GUI: Login</td>
<td>
1. Open the web browser and navigate to the PMAC GUI:

```
http://<PMAC_network_IP>
```

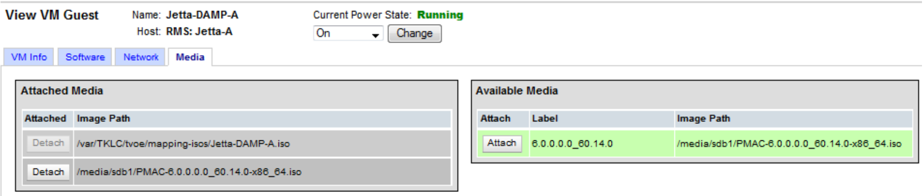
2. Login as the guiadmin user:



Oracle System Login
Tue Jun 7 13:49:06 2016 EDT
Log In
Enter your username and password to log in
Username:
Password:
☐ Change password
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.
<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>

</td>
</tr>
<tr>
<td>3.
☐</td>
<td>PMAC GUI: Attach the software image to the PMAC guest</td>
<td>
If the ISO image was transferred to PMAC using sftp (step 1.), 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.

1. In the PMAC GUI, navigate to VM Management. In the VM Entities list, select the PMAC guest. On the resulting View VM Guest screen, select the Media tab.
2. Under the Media tab, find the ISO image in the Available Media list and click its Attach button. After a pause, the image displays in the Attached Media list.



View VM Guest
Name: Jetta-DAMP-A
Host: RMS: Jetta-A
Current Power State: Running
On

Attached Media

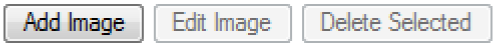
<table>
<tr><th>Attached</th><th>Image Path</th></tr>
<tr><td>Detach</td><td>/var/TKLC/tvoe/mapping-isos/Jetta-DAMP-A.iso</td></tr>
<tr><td>Detach</td><td>/media/sdb1/PMAC-6.0.0.0.0_60.14.0-x86_64.iso</td></tr>
</table>

Available Media

<table>
<tr><th>Attach</th><th>Label</th><th>Image Path</th></tr>
<tr><td>Attach</td><td>6.0.0.0.0_60.14.0</td><td>/media/sdb1/PMAC-6.0.0.0.0_60.14.0-x86_64.iso</td></tr>
</table>

</td>
</tr>
</table>

Procedure 130. iDIH Installation: Deviation

<table>
<tr>
<td>4.
☐</td>
<td>PMAC GUI: Add an application image</td>
<td>
1. Navigate to Software > Manage Software Images.
2. Click Add Image and select the image from the list of options.


If the image was supplied on a CD or a USB drive, it displays 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 on the second device, device://dev/sr1. If one or more CD or USB-based images were already on the management server before you started this procedure, select a correspondingly higher device number.
If the ISO image was transferred to PMAC using sftp (step 1.), it displays in the list as a local file in /var/TKLC/....
3. Select the appropriate path and click Add New Image.
4. Check the progress by clicking the Task Monitoring link.
5. Observe the green bar indicating success. Once the file has transferred, remove the IDIH media from the optical drive of the management server.
</td>
</tr>
<tr>
<td>5.
☐</td>
<td>PMAC: Establish terminal session</td>
<td>Establish an SSH session to the PMAC and login as admusr.</td>
</tr>
<tr>
<td>6.
☐</td>
<td>PMAC: Copy the vedsr_idih.xml.template XML file to the PMAC guest-dropin directory</td>
<td>
<pre>
$ sudo cp /usr/TKLC/pmac/html/TPD/mediation-7.1.0.0.0_x.x.x.x/vedsr_idih.xml.template /var/TKLC/smac/guest-dropin
$ cd /var/TKLC/smac/guest-dropin/
$ mv vedsr_idih.xml.template <idih_fdc_file_name>.xml
</pre>
</td>
</tr>
</table>

Procedure 130. iDIH Installation: Deviation

7. ☐	**PMAC**: Configure the fdc.cfg file	Configure the <idih_fdc_file_name>.xml template file. See Appendix M Configure IDIH Fast Deployment 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:

IDIH	**Profile Parameters (No. of CPU, RAM, Virtual Disk)**	**XML Stanzas to Modify**

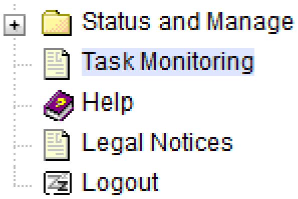
IDIH-Mediation	No. of CPUs: 2
	Memory (MBs): 8192 MB
	Virtual Disks: 65536 MB
		`<cpus>2</cpus>`
		`<memory>8192</memory>`
		
		`<vdisk>`
		`<hostvolname>MED.img</hostvolname>`
		`<hostpool>vgguests</hostpool>`
		`<size>65536</size>`
		`<primary>yes</primary>`
		`<guestdevname>PRIMARY</guestdevname>`
		`</vdisk>`

IDIH-Application	No. of CPUs: 2
	Memory (MBs): 8192 MB
	Virtual Disks: 65536 MB
		`<cpus>2</cpus>`
		`<memory>8192</memory>`
		
		`<vdisk>`
		`<hostvolname>APP.img</hostvolname>`
		`<hostpool>vgguests</hostpool>`
		`<size>65536</size>`
		`<primary>yes</primary>`
		`<guestdevname>PRIMARY</guestdevname>`
		`</vdisk>`

IDIH-Database	No. of CPUs: 4
	Memory (MBs): 8192 MB
	Virtual Disks: 166926 MB (102400 MB for ORA_SDB and 65536 MB for ORA)
		`<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>`

Procedure 130. iDIH Installation: Deviation

8.
☐
	PMAC: Run the fdconfig	`$ screen`
		`$ sudo fdconfig config --file=<idih_fdc_file_name>.xml`
		Example:
		`$ sudo fdconfig config --file=tvoe-ferbrms4_01-22-15.xml`
		Note: This is a long duration command (45-90 minutes). If the screen command was run before executing fdconfig, perform a **screen -dr** to resume the screen session in the event of a terminal timeout, etc.

9. ☐	**PMAC GUI**: Monitor the configuration	1. If not already done so, establish a GUI session on the PMAC server. 2. Navigate to **Task Monitoring**.  Status and Manage Task Monitoring Help Legal Notices Logout 3. 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 in Table 6.

Table 6. VM Automation Profile Values

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="14"	DSR_VIRT_SBR_SEESION_MEM="32768"	DSR_VIRT_SBR_SESSION_VDISK="71680"
DSR BINDING SBR		
DSR_VIRT_SBR_BINDING_CPU="12"	DSR_VIRT_SBR_BINDING_MEM="25600"	DSR_VIRT_SBR_BINDING_VDISK="71680"

CPU	MEMORY	VDISK
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="10240"	SDS_VIRT_DP_VDISK="71680"
SDS QUERY SERVER		
SDS_VIRT_QS_CPU="4"	SDS_VIRT_QS_MEM="16384"	SDS_VIRT_QS_VDISK="102400"

Appendix S. VM Placement in HP DL380 Gen 8/Gen 9 (Onboard 1Gbps NICs)

HP DL380 Gen 8 and HP DL380 Gen 9 rack mount server solutions should place VMs in one of these deployment scenarios:

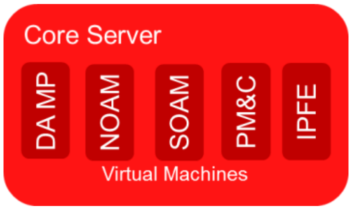

Core Server
DA MP
NOAM
SOAM
PM&C
IPFE
Virtual Machines

Figure 4. HP DL380 Gen 8/Gen 9 (1Gbps) VM Placement Non-HA LAB Deployment

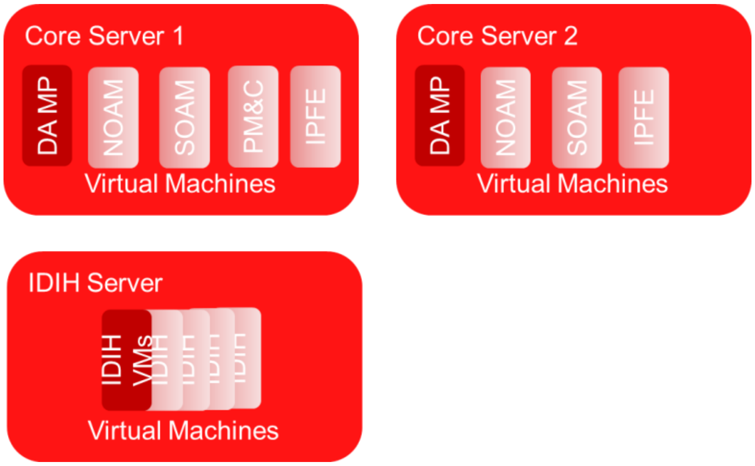

Core Server 1
DA MP
NOAM
SOAM
PM&C
IPFE
Virtual Machines
Core Server 2
DA MP
NOAM
SOAM
IPFE
Virtual Machines
IDIH Server
IDIH VMs
IDIH
IDIH
IDIH
IDIH
Virtual Machines

Figure 5. HP DL380 Gen 8/Gen 9 (1Gbps) VM Placement Small Production DSR with IDIH

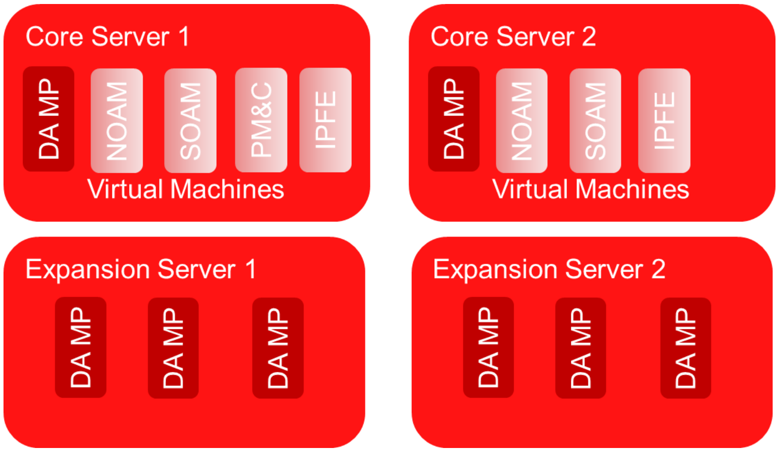

Core Server 1
DA MP
NOAM
SOAM
PM&C
IPFE
Virtual Machines
Core Server 2
DA MP
NOAM
SOAM
IPFE
Virtual Machines
Expansion Server 1
DA MP
DA MP
DA MP
Expansion Server 2
DA MP
DA MP
DA MP

Figure 6. HP DL380 Gen 8/Gen 9 (1Gbps) VM Placement Scaled DSR

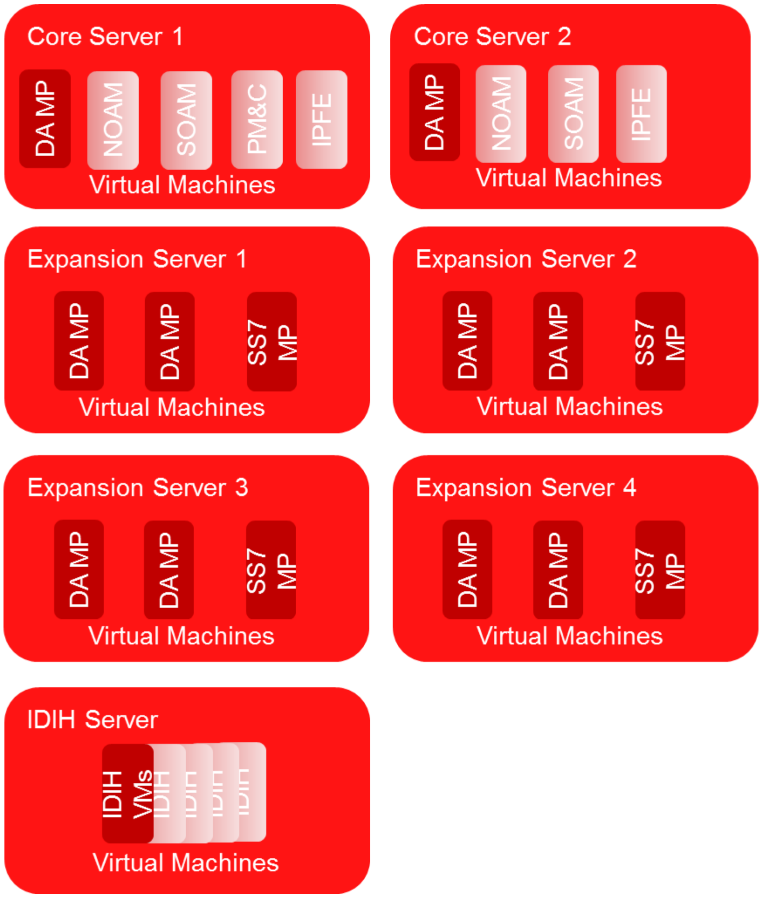

Core Server 1
DA MP
NOAM
SOAM
PM&C
IPFE
Virtual Machines
Core Server 2
DA MP
NOAM
SOAM
IPFE
Virtual Machines
Expansion Server 1
DA MP
DA MP
SS7 MP
Virtual Machines
Expansion Server 2
DA MP
DA MP
SS7 MP
Virtual Machines
Expansion Server 3
DA MP
DA MP
SS7 MP
Virtual Machines
Expansion Server 4
DA MP
DA MP
SS7 MP
Virtual Machines
IDIH Server
IDIH VMs
IDIH
Virtual Machines

Figure 7. HP DL380 Gen 9 (1Gbps) VM Placement Scaled DSR with SS7 MPs and IDIH

Appendix T. Restore SNMP Configuration to SNMPv3 (Optional)

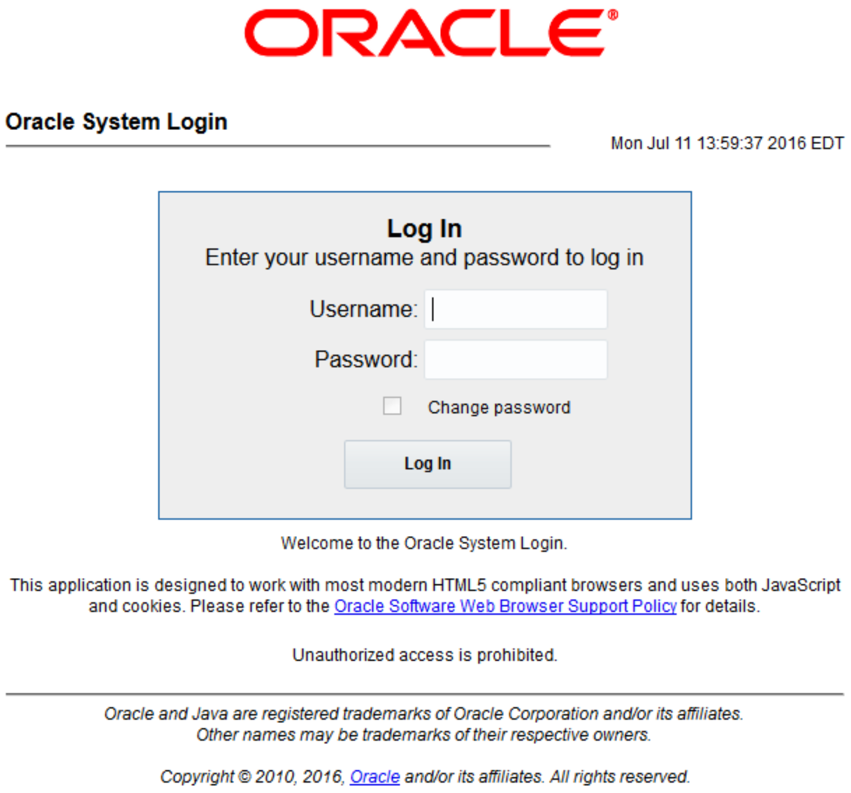
Procedure 131. Restore SNMP Configuration to SNMP v3

This procedure restores SNMP configuration to SNMPv3 for forwarding of SNMP traps from each individual server.

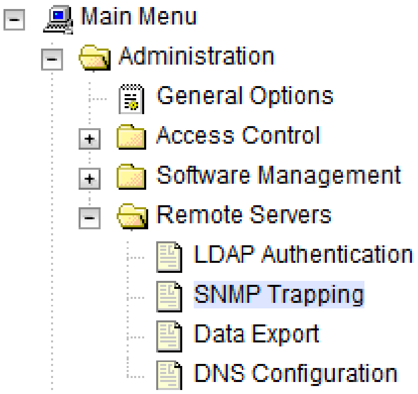
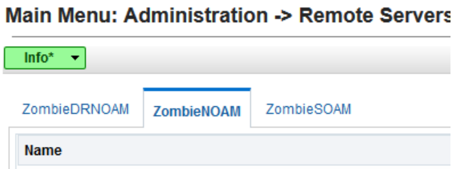
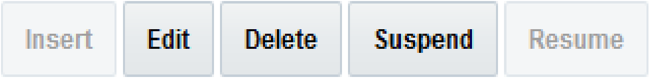
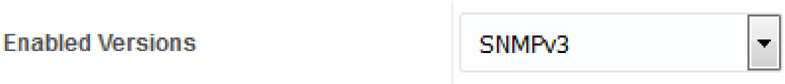
Note: If SNMP is configured with SNMPv2c and SNMPv3 as enabled versions as a workaround step (Procedure 37 Configure SNMP Trap Receivers, steps 4. through 8.) and the SNMPv3 is required to be configured.

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

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

1. ☐	(Workaround) **Primary NOAM VIP GUI**: Login	***Note:*** This workaround should be performed only if SNMP is configured with SNMPv2c and SNMPv3 as enabled versions as a workaround (Procedure 37 Configure SNMP Trap Receivers, steps 4. through 8.) and the SNMPv3 is required to be configured. 1. Establish a GUI session on the NOAM server by using the XMI VIP IP address. Open the web browser and enter a URL of: `https://<NOAM_XMI_VIP_IP_Address>` 2. Login as the **guiadmin** user.  ORACLE 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 131. Restore SNMP Configuration to SNMP v3

2. ☐	**NOAM VIP GUI**: Configure system-wide SNMP Trap receiver(s)	1. Navigate to **Administration > Remote Servers > SNMP Trapping**.  Main Menu Administration General Options Access Control Software Management Remote Servers LDAP Authentication SNMP Trapping Data Export DNS Configuration 2. Select the Server Group tab for SNMP trap configuration. The server group that is configured for SNMPv2c and SNMPv3 as a workaround:  Main Menu: Administration -> Remote Servers Info* ZombieDRNOAM ZombieNOAM ZombieSOAM Name 3. Click Edit.  Insert Edit Delete Suspend Resume 4. Update the Enabled Versions as SNMPv3: Enabled Versions SNMPv3 5. Click OK.

Appendix U. CPU Pinning in HP DL380 Gen 9 (Onboard 1Gbps NICs)

The following tables contain information about HP DL380 Gen 9 (1Gbps) CPU Pinning with and without SS7MPs:

Table 7. HP DL380 Gen 9 (1Gbps) CPU Pinning without SS7MPs

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 8. HP DL380 Gen 9 (1Gbps) CPU Pinning with 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													

Refer 3.13 CPU Pinning to perform the pinning.

Appendix V. netConfig backupConfiguration/restoreConfiguration/upgradeFirmware with TPD Cipher Change

Beginning with TPD 7.6.0.0.0_88.50.0, the cipher list is restricted to allow only a limited number of ciphers for ssh access to the servers. As a result, netConfig backup and restore operations are not functional with Cisco switches (3020, 4948s) since these switches use other ciphers. Executing these commands with the restricted ciphers would fail as shown here:

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

Command failed: backupConfiguration

Error saving to SSH service

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

To avoid this issue while maintaining a focus on improved security, the Procedure 132 must be executed before and after netConfig backup and restore operations.

Procedure 132. Turn Off Cipher List Before backupConfiguation/restoreConfiguration/upgradeFirmware Command

Step #	Procedure	Description
This procedure prepares the PMAC to avoid the cipher mismatch issue with Cisco switches. This is performed before the netConfig backup or restore operations. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1.
☐
	Turn off cipher list	1. From the PMAC shell enter:
		`sudo vi /etc/ssh/sshd_config`
		2. Add # in the beginning of the following three lines to comment them out, the result is:
		`#Ciphers aes256-ctr,aes192-ctr,aes128-ctr`
		`#MaxAuthTries 4`
		`#LoginGraceTime 1m`

Step #	Procedure	Description
2. ☐	Restart sshd	`sudo service sshd restart`

3.
☐
	Run the netConfig backupConfiguation/restoreConfiguration/upgradeFirmware command	For a backup operation:
		`[admusr@pmac ~]$ sudo /usr/TKLC/plat/bin/netConfig backupConfiguration --device=<switch_name> service=<ssh_service> filename=<switch_name>-backup`
		For a restore operation:
		`[admusr@pmac ~]$ sudo /usr/TKLC/plat/bin/netConfig restoreConfiguration --device=<switch_name> service=<ssh_service> filename=<switch_name>-backup`
		For a upgrade operation:
		`[admusr@pmac ~]$ sudo /usr/TKLC/plat/bin/netConfig upgradeFirmware --device=<switch_name> service=<ssh_service> filename=<Cisco IOS>`

Procedure 133. Resume Cipher List After backupConfiguation/restoreConfiguration/upgradeFirmware Command

Step #	Procedure	Description
This procedure restores the PMAC restricted cipher list after perform the netConfig backup and restore operations. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1.
☐
	Resume the cipher list	1. From the PMAC shell enter:
		`sudo vi /etc/ssh/sshd_config`
		2. Uncomment the three lines:
		`Ciphers aes256-ctr,aes192-ctr,aes128-ctr`
		`MaxAuthTries 4`
		`LoginGraceTime 1m`

2. ☐	Restart sshd	`sudo service sshd restart`

Appendix W. My Oracle Support (MOS)

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

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

1. Select **2** for **New Service Request**.

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

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

Emergency Response

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

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

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

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

Locate Product Documentation on the Oracle Help Center

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

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